
Model-based Management of Cyber Resiliency for Healthcare Systems

Thesis report submitted in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

by

Myrsini Athinaiou

Under the supervision of

Haralambos Mouratidis

Michalis Pavlidis

Theo Fotis



University of Brighton

School of Architecture, Technology and Engineering

University of Brighton

January 19, 2022

Acknowledgments

It is impossible to face the challenge of researching without being inspired, influenced and supported by others. Those that have crossed my path are numerous, and thus I will not be able to address them all.

Haris, Theo and Michalis, after all the ideas we have shared and interchanged, I seem to be at a loss regarding how to adequately express my appreciation and gratitude for all you do and are to me. We started out having a strict work relationship, and somewhere along the line, you became my cherished mentors and voice of reason in my head when it all just seemed too complicated. Vaggeli, Vaso, Kwsta, Shaun, Oresti, Daniel, and Duaa, thank you for welcoming me to our research group. Kosta, Luca, Mohamed and Rama, thank you for bringing back the excitement of a new start in our group and I wish you a productive completion. I also feel compelled to thank Sandra, Myrsini, Lujain, and Panagiota, who, after attending one workshop together, we remained together throughout our diverse research projects.

Dearest grandmother, it is surreal that you will not be able to see me complete this project, as you have always supported me and encouraged me to be creative and share ideas. I feel you watching me from above. Thank you for letting me be your granddaughter. I love you, and I miss you.

Mom, Dad, we are fortunate to share so much love among us. Thank you for all your struggles, patience and care.

Billie, Mel and Robin, thank you for being always friendly and understanding. Thank you for your kindness, generosity and hospitality. Trish and John, I am grateful for your guidance. Beena, Tasha, Amy, Kat, Linda, Laura, Sophie, Tash, Hina, thank you for being my mates. Thank you for the repeated suggestions, arguments and fun times. Liv, Nick, Ludo, Julia, Daniel and Paul, I will treasure our shared experiences forever. Thank you for being yourselves and accepting me as myself. A big thank you to all my rugby teammates for being inclusive and my table tennis family for supporting everyone and our local community.

To the opposition, thank you very much for your input. May our argumentation be fruitful.

Brighton
January 19, 2022

Myrsini Athinaiou

Contents

Acknowledgments	i
List of Tables	viii
List of Figures	x
Abstract	xv
1 Narrative	2
1.1 Motivation	2
1.1.1 The Healthcare Environment	2
1.1.2 Healthcare Cybersecurity	3
1.1.3 Medical Devices and Cybersecurity	4
1.2 Terminology	8
1.3 Background and Research Objectives and Assumptions	10
1.3.1 Requirements engineering	11
1.3.2 The important role of RE in the BINA context	12
1.3.3 Model-based approaches	13
1.3.4 Research assumptions	13
1.4 Research scope	14
1.4.1 Cybersecurity	14
1.4.2 Healthcare	14
1.4.3 Resiliency	15
1.5 Research Methodology	16
1.5.1 Design Science	17
1.6 Design Problems and Knowledge Questions	17
1.7 Document Structure	17

2	Problem Investigation	20
2.1	Stakeholders and Goal Analysis	20
2.2	Systematic Review	21
2.2.1	Search questions	22
2.2.2	Search strategy	23
2.2.3	Search reliability	24
2.2.4	Inclusion and exclusion criteria	24
2.2.5	Data quality assessment	25
2.2.6	Data extraction and synthesis	25
2.2.7	Search limitations	26
2.3	Systematic Review Results	26
2.3.1	General characteristics	26
2.3.2	Aggregation based on incident response phases	28
2.3.3	Aggregation based on context	31
2.4	Stakeholders Challenges and Goals	34
2.5	Discussion and Closing Remarks	36
3	Requirements Specification and Existing Treatments	37
3.1	Requirements Specification	37
3.2	Requirements Contribution to Goals	38
3.3	Available Treatments	38
3.3.1	Operationalisation using existing treatments set	39
3.3.2	Search of healthcare cybersecurity reviews	44
3.3.3	Search for cybersecurity resilience treatments	45
3.3.4	Data extraction and synthesis	46
3.3.5	Search limitations	49
3.4	Systematic Review Results	50
3.5	Discussion and Closing Remarks	51
4	Cybersecurity Resiliency Domain Model	56
4.1	Research approach	56
4.2	Literature review	58
4.3	BINA construct association	60

4.3.1	Constructs to study	60
4.3.2	Constructs analysis	60
4.3.3	Association table of BINA constructs	63
4.3.4	Elicitation of relationships between BINA constructs	67
4.3.5	Overall remarks about construct association and relationship extraction	69
4.4	The BINA conceptual model	69
4.4.1	Names of the constructs	69
4.4.2	Constructs definitions	69
4.4.3	Relationships and multiplicities of the BINA domain model	72
4.4.4	Validation of the BINA	74
4.5	Benefits and Limitations of the BINA	75
4.5.1	Benefits of the conceptual model	75
4.5.2	Limitations of the conceptual model	76
4.6	Discussion and Closing Remarks	77
5	Delineation of the Cyber Resiliency Management Metrics	78
5.1	Research method	79
5.2	Theory	80
5.2.1	Introduction to risk evaluation	80
5.2.2	The GQM approach	81
5.2.3	On the definition of ROSI	83
5.3	Use of the GQM framework on the BINA domain	83
5.4	Examination of BINA approaches for metrics validation	85
5.4.1	Cyber resiliency standards	86
5.4.2	Cyber resiliency frameworks	88
5.5	Enhancement of the BINA conceptual model with metrics	89
5.6	Summing-up the BINA metric elicitation	91
5.7	Discussion and Closing Remarks	92
6	Assessment of the BINA by using Security and Incident Response Modelling Languages	93
6.1	Research method	94
6.1.1	Running Example	95

6.1.2	Generic security requirements process	95
6.1.3	An overview of Security and Incident Response Modelling Languages	98
6.2	Evaluation of BINA by KAOS	100
6.2.1	Modelling BINA with KAOS	100
6.2.2	Association of KAOS with BINA domain model	101
6.2.3	Discussion	104
6.3	Evaluation of BINA by Misuse Cases	106
6.3.1	Modelling BINA with Misuse cases	106
6.3.2	Association of Misuse cases with BINA domain model	108
6.3.3	Discussion	110
6.4	Evaluation of BINA by Secure Tropos	111
6.4.1	Modelling BINA with Secure Tropos	111
6.4.2	Association of Secure Tropos with BINA domain model	113
6.4.3	Discussion	114
6.5	Summary of language association	115
6.6	A cyber resiliency-aware Secure Tropos	116
6.6.1	Concrete syntax extensions	116
6.6.2	Abstract syntax extensions	119
6.6.3	Application of resiliency-aware Secure Tropos	122
6.6.4	Theoretical evaluation	124
6.7	Summing-up the Assessment of BINA	126
6.7.1	Research method	126
6.7.2	Assessment of BINA support by security-oriented languages	126
6.7.3	Review of language association	127
6.7.4	A cyber resiliency-aware Secure Tropos	127
6.7.5	Discussion and Closing Remarks	127
7	BINA Process and Tool	129
7.1	Overview of the BINA process	129
7.1.1	Activity 1: Organisational modelling	130
7.1.2	Activity 2: Incident modelling	131
7.1.3	Activity 3: Holistic resiliency modelling	133
7.1.4	Activity 4: Resiliency analysis	134

7.2	Tool description	135
7.2.1	Constructs graphical notation	136
7.2.2	BINA tool functionality	137
7.3	Discussion and Closing Remarks	144
8	Evaluation of BINA methodology by case study research in the health care domain	146
8.1	Proof of Concept for BINA by case study research in the health care domain . . .	147
8.2	Case study design	148
8.2.1	Case study objectives	148
8.2.2	Case selection/context	149
8.2.3	Unit of analysis	149
8.2.4	Data collection and analysis methods	150
8.2.5	Case study validity	150
8.3	Brain-Computer Interfaces	152
8.4	Teleoperated Robotic Systems	167
8.5	Evaluation of BINA methodology by case study research in the health care domain	184
8.5.1	Activity 1: Organisational modelling	184
8.5.2	Activity 2: Incident modelling	186
8.5.3	Activity 3: Holistic resiliency modelling	188
8.5.4	Activity 4: Resiliency analysis	194
8.6	Discussion and Closing Remarks	202
9	Evaluation of BINA methodology by interviews and a survey research	203
9.1	Survey design	204
9.1.1	Survey objectives	204
9.1.2	Subjects	204
9.1.3	Ethics approval	205
9.1.4	Tools	205
9.1.5	Training	205
9.1.6	Tasks	206
9.1.7	Data collection methods	206
9.1.8	Data analysis methods	207
9.1.9	Study validity	208

9.2	Data collection	208
9.3	Data analysis	208
9.4	Discussion and Closing Remarks	212
10	Conclusions and Future Work	214
10.1	Review of research questions	214
10.2	Research contributions	214
10.3	Research limitations	216
10.4	Future work	217
10.5	Publications in relation to this thesis	218
	Bibliography	219
A	Literature extracted definitions for healthcare cyber resiliency constructs	235
A.0.1	Cyber resiliency standards	235
A.0.2	Cybersecurity standards	235
A.0.3	Health-related standards	238
A.0.4	Cyber resiliency frameworks	239
B	Alignment table of cyber resiliency concepts	243
C	Survey constructs	257
C.1	Invitation for participation	257
C.2	Participation Information Sheet	257
C.3	Consent Form	259
C.4	Questionnaire	259

List of Tables

1.1	Examples of Cyber-Physical Systems (CPSs) in Healthcare Critical Infrastructures (HCCIs) (based on [1, 2, 3])	10
2.1	Characteristics of selected papers shorted by publication year	27
2.2	Aggregation of selected papers based on incident response phases by NIST SP 800-61r2 [4]	29
2.3	Aggregation of papers context	32
3.1	Operationalisation of existing set of treatments	39
3.2	Aggregation of treatments by publication year	53
4.1	Association table for cyber resiliency standards.	64
4.2	Association table for cybersecurity standards.	65
4.3	Association table for health-related standards.	66
4.4	Association table for cyber resiliency frameworks.	66
4.5	Name of the constructs included in the BINA.	70
5.1	Example of qualitative scale (based on [5]).	81
5.2	Example of semi-quantitative scale (based on [5]).	81
5.3	Example of semi-quantitative scale (based on [5]).	82
5.4	Metrics analysis table for NIST SP 800-184 [6, p. 20]).	86
5.5	Metrics analysis table for NIST SP 800-61r2 [4, p. 40-41]).	87
5.6	Metrics analysis table for MTR140499R1 [7]).	88
5.7	Metrics analysis table for MTR110237 [8]).	89
6.1	Construct alignment between KAOS and the BINA domain model.	102
6.2	Construct alignment between Misuse cases and the BINA domain model.	109
6.3	Construct alignment between Secure Tropos and the BINA domain model.	113
6.4	Examination of BINA support by security-oriented modelling languages.	115

6.5	Domain-related constructs.	117
6.6	Offensive-related constructs.	118
6.7	Defensive-related constructs.	120
10.1	Summary of research questions and proposed treatments	215
B.1	Aggregation of treatments by publication year (continuation)	244
B.2	Aggregation of treatments by publication year (continuation)	254

List of Figures

1.1	Healthcare infrastructures relations in the context of medical devices.	5
1.2	Medical device manufacturers current attentiveness to cybersecurity.	5
1.3	A suggestion about how to make more cybersecurity attentive the medical device manufacturers.	6
1.4	Regulations based healthcare model.	7
1.5	Cybersecurity risks terminology clarifications.	8
1.6	Business/IT alignment at the level of resilient cybersecurity.	12
1.7	Research scope.	14
1.8	Frameworks and standards within the research scope.	15
1.9	Relevant activities in the engineering cycle.	16
1.10	Outline of the thesis structure based on research approach and research questions.	19
2.1	Research areas that cyber resiliency covers.	22
2.2	Selection process stages.	23
3.1	Selection process stages of second systematic review.	46
4.1	The research approach used for the design of the BINA domain model.	57
4.2	The BINA domain model.	73
5.1	Research method for the BINA metrics determination.	80
5.2	Generic structure of a GQM model.	82
5.3	GQM model for the first aim.	84
5.4	GQM model for the second aim.	85
5.5	The BINA domain model enhanced with the metrics proposed by NIST SP 800-184	87
5.6	BINA domain model enhanced with metrics	90
6.1	Research method applied for the assessment of BINA support by security modelling languages	94

6.2	Security requirements elicitation and analysis process	96
6.3	Partial goal model for the Pharma Invent	101
6.4	Partial operation model for the Pharma Invent	102
6.5	Partial antigoal model for the Pharma Invent	103
6.6	Partial antigoal operational model for the Pharma Invent	104
6.7	Security requirements and controls modelling in KAOS	105
6.8	KAOS pattern for BINA event	106
6.9	Asset modelling in Misuse cases	107
6.10	Modelling Risk in Misuse cases	108
6.11	Modelling Security constraints in Misuse cases	108
6.12	Example of the Misuse cases template	110
6.13	Actor and goal models of Secure Tropos for assets modelling.	111
6.14	112
6.15	Actor and security models of Secure Tropos for risk modelling.	112
6.16	Security constraints modelling in Secure Tropos.	113
6.17	Enhanced BINA domain-related constructs.	117
6.18	Enhanced BINA offensive-related constructs.	119
6.19	Enhanced BINA defensive-related constructs.	119
6.20	Secure Tropos abstract syntax [9]	121
6.21	Organisational view of Pharma Invent	123
6.22	Security incident view of Pharma Invent	123
6.23	Resiliency requirements view of Pharm Invent	124
7.1	BINA process.	130
7.2	Organisational modelling activity.	131
7.3	Incident modelling activity.	133
7.4	Holistic resiliency modelling activity.	134
7.5	Holistic resiliency modelling activity.	135
7.6	Constructs notation.	137
7.7	Constructs properties.	138
7.8	Relations among constructs.	139
7.9	Implementational metamodel.	140
7.10	Assessment of implementation of recovery objectives from CIRPs.	141

7.11	Assessment of implementation of security constraints from CIRPs.	141
7.12	Assessment of protection of assets from CIRPs.	142
7.13	Assessment of security controls aggregation to CIRPs.	142
7.14	Analysis of CIRPs effects on threat objectives.	143
7.15	Analysis of effects among different CIRPs.	143
8.1	Validation approach.	147
8.2	Case study acquisition methods.	150
8.3	A simple Brain-Computer Interface.	152
8.4	Partial BCI system goal-dependency model.	153
8.5	Partial BCI system organisational model.	155
8.6	An incident scenario against a Brain-Computer Interface.	156
8.7	A partial resiliency model for BCI.	157
8.8	CIRP properties determination.	158
8.9	Holistic resilience model for BCI.	160
8.10	Potential interactions between BCI's CIRPs.	161
8.11	CIRPs implementing BCI objectives.	162
8.12	Analysis of the CIRPs effects on objectives for the BCI system.	163
8.13	Structural security constraints implementation through CIRPs for the BCI system.	164
8.14	BCI security controls that aggregate to CIRPs.	164
8.15	Strategic security constraints that restrict BCI objectives.	165
8.16	Decomposition of strategic objectives to structural objectives.	166
8.17	Threats and malicious objectives.	166
8.18	A typical interaction between a surgeon and a Teleoperated Robotic Systems.	167
8.19	Partial TRS organisational model.	168
8.20	An incident scenario against a surgical TRS.	170
8.21	Holistic resilience model for a surgical TRS.	173
8.22	TRS Properties determination.	176
8.23	System resiliency before and after the resiliency analysis.	177
8.24	Potential interactions between TRS's CIRPs.	177
8.25	CIRPs implementing TRS objectives.	178
8.26	Analysis of the CIRPs effects on malicious objectives for the TRS.	179
8.27	Structural security constraints implementation through CIRPs for the TRS.	180

8.28	TRS security controls that aggregate to CIRPs.	181
8.29	Strategic security constraints that restrict TRS objectives.	182
8.30	Decomposition of strategic constraints to structural constraints.	183
8.31	Threats and malicious objectives.	183
8.32	A typical interaction between a hospital's home nursing team and a smart glasses system.	184
8.33	Partial telemedicine system organisational model.	185
8.34	Partial telemedicine system incident model.	187
8.35	Partial holistic resilience model for smart glasses.	190
8.36	Dependency level (D) as generated from the BINA tool for the CIRP 'Diversity'.	191
8.37	Property section for CIRPs in BINA tool.	191
8.38	Properties of the CIRP 'Diversity' in BINA tool.	191
8.39	Property section for CIRPs in BINA tool.	191
8.40	Properties of the CIRP 'local storage' in BINA tool.	192
8.41	System Resiliency as generated from the BINA tool.	192
8.42	Properties of the construct 'Event'.	193
8.43	Properties of the construct 'Incident'.	193
8.44	Properties of the construct 'Risk'.	194
8.45	Smart glasses system resiliency after the resiliency analysis.	194
8.46	High-level CIRPs implementing smart glasses system objectives.	195
8.47	Potential interactions between smart glasses system CIRPs.	195
8.48	Potential interactions between new and old smart glasses system CIRPs.	196
8.49	CIRPs implementing smart glasses system objectives.	197
8.50	Analysis of the CIRPs effects on malicious objectives against the smart glasses system.	198
8.51	Structural security constraints implementation through CIRPs for the smart glasses system.	199
8.52	Smart glasses system security controls that aggregate to CIRPs.	199
8.53	Strategic security constraints that restrict smart glasses system's objectives.	200
8.54	Decomposition of strategic constraints to structural constraints for the smart glasses system.	201
8.55	Threats and malicious objectives against the smart glasses system.	201
9.1	survey approach.	204

9.2	Survey data collection and analysis methods.	207
9.3	Survey results concerning the BINA modelling language.	209
9.4	Survey results concerning the BINA tool.	210
9.5	Survey results concerning the BINA methodology.	211

Abstract

Ad hoc cyber resiliency can introduce delays and further vulnerabilities resulting in increased threats, impacts and costs. Within the healthcare context, these delays can cause physical harm to patients. Research has shown that a priori evaluation of cyber resiliency plans can reduce or avoid such delays. However, the absence of an approved catalogue of cyber resiliency requirements and the lack of semantic interoperability among the available cyber resiliency standards and frameworks leave healthcare infrastructures puzzled. This study aims to determine how current domain knowledge can assist healthcare systems to be more cyber resilient by design. Building on existing cyber resiliency work, it asks how a socio-technical a priori analysis approach could help healthcare systems become more cyber resilient by design. In this context, cyber resiliency is defined as the ability to analyse resiliency capabilities at a cyber security requirements level, to maintain a set of security constraints by reducing the impact and likelihood of adverse occurrences that violate security constraints.

Based on a literature review and specification of stakeholders as individuals or/and organisations affected by the proposed treatment, we designed a domain model that semantically aligns concepts and their relations. In this way, we were able to describe the entities of the problem domain space. To manage these entities, we needed to search for ways to measure them. Using the existing literature and combining it with the metrics of relevance to how we defined cyber resiliency, utilising the Goal, Question, Metrics (GQM) approach, we enhanced the attributes of the domain model with resiliency metrics.

To examine if the existing cyber security languages express cyber resiliency concerns, we used a case study to apply them and compare them. That resulted in association tables among their semantic and syntactic capabilities. It also allowed us to identify Secure Tropos as a modelling language that had the most expressivity. Hence, we extended Secure Tropos to cover the cyber resiliency domain entities as expressed in the domain model. To allow stakeholders to use our methodology, we designed a process based on observed patterns in the literature. We also tried ourselves in small case studies to identify a meaningful analysis path. This endeavour led us to the design of a relevant process using SPEM 2.0. Furthermore, to support the reasoning using the modelled metrics, we designed algorithms that automated some aspects of cyber resiliency analysis. We developed a software tool to demonstrate and test the above components of our approach that we named Built-In resiliency Analysis (BINA).

To evaluate our treatment (BINA), we used two case studies from the health care domain. In this way, we were able to demonstrate the applicability and benefits of applying the BINA approach. Then we interviewed Chief Technology/Information Officers working for medical device manufacturers and hospitals and Software Engineers with more than 15 years of experience. The interviews involved a brief presentation of the BINA approach, which they implemented in a small case study. Subsequently, they filled in a questionnaire that asked for their feedback regarding the modelling language, the process, the automation and the tool. We also had the opportunity to apply BINA to an actual case study in an ongoing Brighton and

Hove living lab project. This allowed us to analyse the cyber resiliency of a healthcare system under development. The combination of the different evaluation methods contributed to the reduction of biases and threats against validity.

Chapter 1

Narrative

1.1 Motivation

NIST SP 800-160 v.2 defines 'cyber resiliency' as *"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources"* [10, p. xiv]. Cyber resiliency decision making tends to be more routine, a process that occurs without thinking, rather than an actual decision-making process [11]. However, good organisational habits can lead to success, and cyber resiliency can become the "keystone habit" for healthcare infrastructures. A keystone habit means that by focusing on becoming more cyber resilient, healthcare infrastructures can improve their overall performance and even financial position.

This thesis is considering cyber resiliency within a health care context. Therefore by way of introduction, it is necessary first to consider the health context and then discuss its cyber resiliency challenges intertwined with the broader context of cybersecurity.

1.1.1 The Healthcare Environment

Healthcare moves increasingly closer to the patient's location. In the past, the delivery of some healthcare services was possible only in hospitals. With technological advances, healthcare services can now be provided remotely (e.g., telesurgery, insulin pumps, implantable cardioverter-defibrillators). Healthcare service provision ranges from low to high acuity as a patient's needs increase.

Hospitals are still an essential part of the healthcare environment, especially when acute care is required. However, their ownership is not necessarily governmental. Hospital owners can be private organisations (for-profit or non-profit), and even though rarely, individuals can own them.

The healthcare environment does not include only hospitals. It also includes other healthcare-related facilities, such as pharmacies, hearing centres, dental clinics, home care programs, community health centres, hospices, and medical equipment suppliers. These organisations are also essential for the provision of healthcare services.

As a consequence, a broad range of stakeholders characterises the healthcare environment. Their broad range can be understood from a simple example, that of a patient. A patient can be from a newborn infant to advanced age or a physician that has fallen ill. Patients are especially

susceptible to threats. Their conditions render them less able to secure themselves. Cybersecurity bears the responsibility to protect them from cyber threats and attacks. However, each patient type yields unique security challenges, needs and concerns that resilient security plans need to consider.

The provider of healthcare services bears the responsibility to provide a cyber-secure healthcare environment for all patients. It has the same duty when it comes to their healthcare staff too. Here, the range is broad again and can include physicians and technical caregivers to support staff, facilities management, and biomedical equipment repair personnel.

From a cybersecurity perspective, a security practitioner is another important stakeholder. The healthcare environment has many context limitations related to the patient's condition, healthcare operations, state and availability, and legal and financial considerations. A healthcare cybersecurity plan needs to take into account such aspects. These aspects require cybersecurity professionals to protect and respond to threats and attacks against healthcare systems.

In general, a system is a set of components that cooperate in some way. The World Health Organisation (WHO) defines a *healthcare system* as "(i) all the activities whose primary purpose is to promote, restore and/or maintain health; (ii) the people, institutions and resources, arranged together in accordance with established policies, to improve the health of the population they serve, while responding to people's legitimate expectations and protecting them against the cost of ill-health through a variety of activities whose primary intent is to improve health." [12, p. 9]. *Complex adaptive systems* address structures that change based on their environment to survive. *Systems thinking* is a holistic approach that analyses the change and complexity of a system as an interconnected whole, rather than components in isolation.

1.1.2 Healthcare Cybersecurity

The term healthcare cybersecurity is quite vague. It can be given a different meaning in different settings. In particular, within the context of healthcare systems, *cybersecurity* can be generally defined as a system of safeguards designed to protect, respond and recover from threats and attacks to achieve relative security for all people interacting within the healthcare system and its environment.

This definition, of course, leaves the problem of defining relative security. It is well understood in the cyber context that what is secure today may not be secure tomorrow or even later today. In practice, cybersecurity is intended to reduce the occurrence and impact of detrimental incidents. It does not aim, though, to do so for all systems and their components. Cybersecurity, then, is related to the criticality of the entity to be protected (e.g., process, goal, asset), and it cannot be static. In other words, it needs to be responsive to incidents. As incidents, systems, and environmental conditions change, so does cybersecurity design. This phenomenon requires systems' cybersecurity to be designed to force their engagement in responsive behaviours to produce desirable effects. This requirement also applies in the healthcare environment.

Effective healthcare cybersecurity needs to be aligned with the goals of the healthcare system and the organisation in which it operates. Still, in practice, many security systems are designed having as a primary concern their legal compliance or security standards (e.g., ISO 27001/13). Of course, legal restrictions affect the cybersecurity of a healthcare system, but cybersecurity is fundamentally a business function. As such, it needs to be tailored to a specific healthcare system's needs.

A system-specific by-design cybersecurity development is essential because it will protect

the healthcare system's interests while complying with legal requirements. However, it still leaves the ability to the healthcare organisation to decide the most beneficial cybersecurity course of action, given the specific circumstances of an incident.

Cybersecurity is essential for the provision of healthcare services for a variety of reasons:

- Secure cyber healthcare is a moral responsibility for the common good.
- Cybersecurity-focused on healthcare connects and complies to sector-specific legal accreditation and regulatory concerns.
- Cybersecurity affects the provision of patient care given restricted resources.
- Cybersecurity contributes to maintaining good relations with the general public, the local community and the healthcare personnel that feel that they can trust the healthcare system to at least not harm them.

Healthcare systems have to consider cybersecurity as they bear the responsibility of managing healthcare services provided to patients. In the case of occurrences of cyber incidents, they might be held responsible for cybersecurity corporate negligence. In other words, if healthcare organisations provide services in a manner that fails to meet standard healthcare cybersecurity practices and this causes harm, they will be penalised.

1.1.3 Medical Devices and Cybersecurity

Medical Device Manufacturers (MDMs) tend to come from infrastructures that, after the industrial revolution, adjusted to market changes. It seems that the majority of the MDMs have their routes to fine mechanics (e.g., in the past, they were manufacturing watches), pharmaceuticals (they tend to expand to medical device manufacturing) and machinery, materials and biomaterials. A medical device has two main components: the machine and the application. In other words, a physical (hardware) component and a cyber (software) component. Depending on the past orientation of the MDM, more commonly, hardware/machinery requirements are prioritised over software/application requirements.

Consequently, MDMs design and develop new medical devices based on past habits, rather than assessing the current context in which these devices operate (cf. Fig. 1.1). At the top left of Fig. 1.1 are the suppliers of medical device manufacturers. At the bottom right are the healthcare facilities (e.g., clinics, hospitals, blood banks) that MDMs provide medical devices. This illustration shows how healthcare infrastructures interconnect in the context of medical devices. Furthermore, this view reveals that the cybersecurity habits of one type of healthcare infrastructure affect others.

Admittedly there are no infrastructures, including MDMs, without institutional habits. When it comes to cybersecurity¹, there are only MDMs where the design of cybersecurity is deliberate and MDMs where cybersecurity happens without forethought. Usually, in the second case, that means that it grows from rivalries and fear among departments. It is common knowledge that requirements often get political. For example, a typical collision occurs between the marketing and the research and development departments of medical device manufacturers. The marketing department tends to focus on user needs, whereas the research and development department tends to be more concerned with functional and safety aspects. Neither of

¹Here, we exclude cyber resiliency as after we talked with two medical device manufacturers, they made clear that at this point in time as well as in the past, they do not focus on cyber security let alone cyber resiliency.

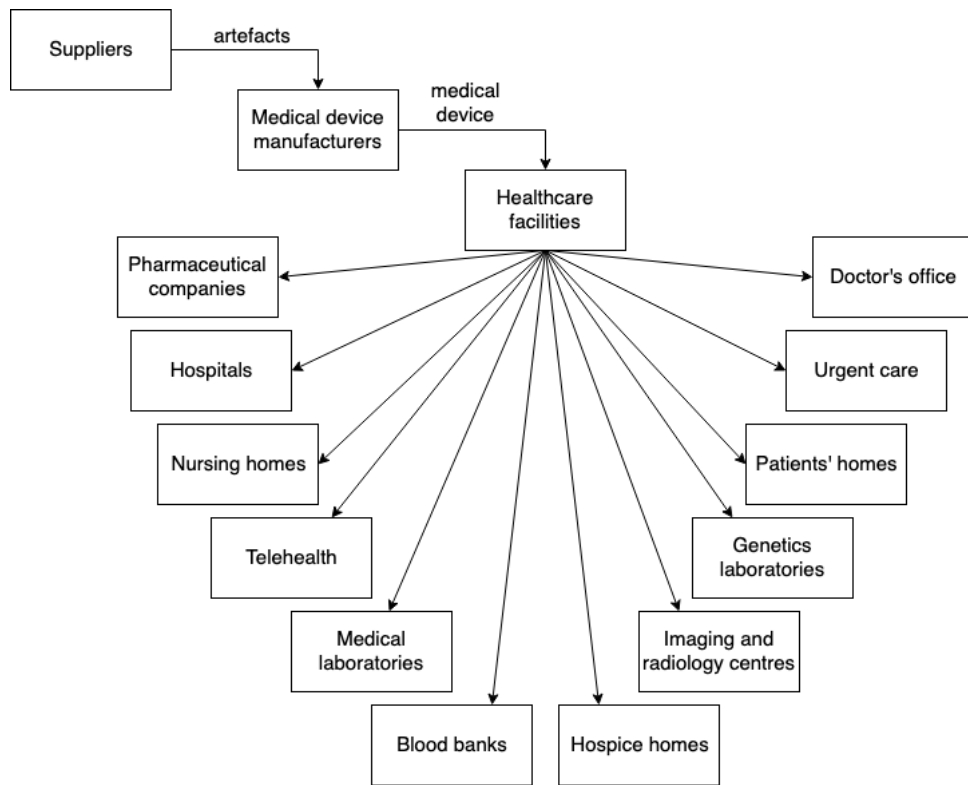


Figure 1.1: Healthcare infrastructures relations in the context of medical devices.

them, though, is interested in supporting cybersecurity requirements, let alone cyber resiliency ones.

Based on Nelson and Winter [13], corporate behaviour reflects the general habits of the employees and strategic operations coming from a MDM's past. Here their finding suggests that a MDM's cybersecurity attentiveness reflects organisational habits and past practices (e.g., cybersecurity is an IT issue). This finding further implicates that cybersecurity decisions are not, in many cases, the results of a detailed survey of an incident and the available assets, people and processes, but somewhat distant branches of the decision tree. In other words, MDMs' choices should be based on deliberate decision making, but that is not what happens in practice. Those MDMs that realise the necessity of cybersecurity, at least because of legislative requirements, tend to seek expertise from the banking sector. Fig 1.2 shows how the relations between healthcare infrastructures and the stakeholders involved in a generic procurement process.

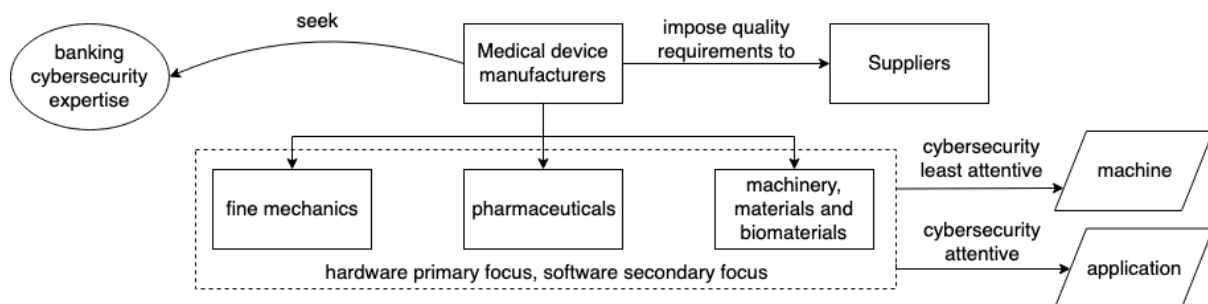


Figure 1.2: Medical device manufacturers current attentiveness to cybersecurity.

Manufacturers are increasingly developing networked medical devices. As a consequence,

the cybersecurity and cybersecurity risks have increased too. Focusing on cybersecurity risks, suppliers, manufacturers and customers share the cybersecurity responsibility throughout the procurement process and before or after the occurrence of cyber incidents. The number of cyber incidents is rising as the sophistication of offenders is swiftly growing. Unfortunately, many manufacturers do not take sufficient account of this as they are more focused on the hardware aspects of their products. A potential reason for the negligence of cybersecurity in medical devices manufacturing might stem from the lack of collective pressure coming from healthcare facilities. If healthcare facilities require cybersecurity from medical device manufacturers, then this will move to their suppliers too. Ideally, that will drive all the participants in the chain of medical devices to be more attentive to the cybersecurity requirements associated with hardware and software, too (cf. Fig. 1.3).

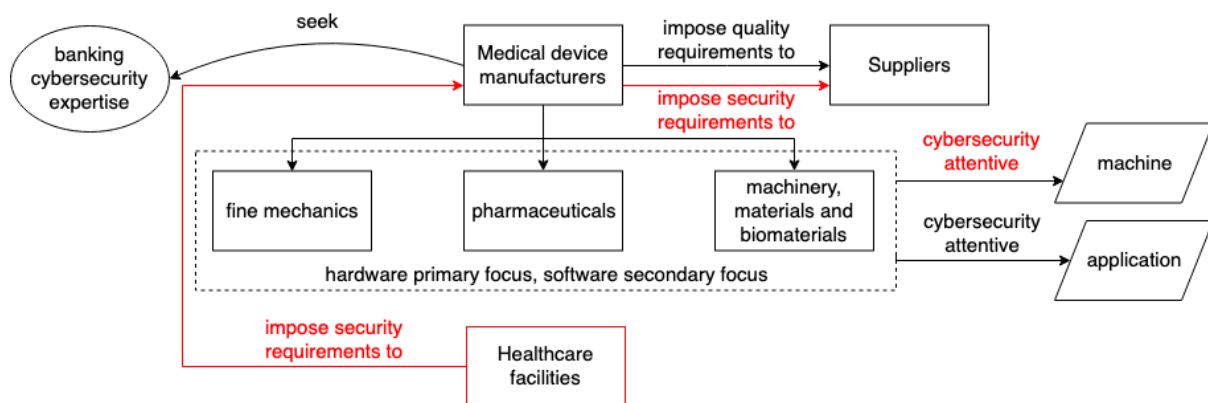


Figure 1.3: A suggestion about how to make more cybersecurity attentive the medical device manufacturers.

The EU regulations (MDR, IVDR) explicitly demand cybersecurity for both generic medical devices and in vitro diagnostic medical devices (IVDs). These regulations (for medical devices (MDR) and in vitro diagnostic medical devices (IVDR)) entered into force in 2017, and after a transition period of three (2020) and five (2022) years, respectively, they will be fully implemented. The importance of these regulations lies in the establishment of requirements. However, before examining these requirements, the provision of the terminology used from MDR and IVDR is also essential.

Based on Article 2(1) of the MDR a medical device is *"any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings"* [14]. Similarly, Article 2(2) of the IVDR defines an IVD as *"medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body"* [15].

MDR and IVDR classify medical devices based on their risk class. As the risk increases, the MDMs have to carry out conformity assessments. The assessments demonstrate that the medical device meets the requirements of the two regulations (MDR, IVDR). The only categories of devices that are considered low risk are the class I MDs and the class A IVDs. These classes conjure with the assurance levels of the cybersecurity act [16], according to which the cybersecurity risk has three assurance levels (basic, substantial, high). A product, service or process takes a cybersecurity risk characterisation based on the probability and impact of an incident. For example, a pacemaker with a high assurance level means that the certified medical device has been subject to the highest security tests.

In the MDR [14] security is addressed in six instances. At the very beginning (39), it necessitates patient awareness regarding the security information of an implanted device. Annex I (17.2) and (17.4) refers to programmable electronic systems such as software, cybersecurity is considered part of a manufacturer’s responsibility for the devices’ life cycle and risk management. Annex I (23.4, ab) refers to the instructions of use again concerning devices that incorporate programmable electronic systems; it is important to include requirements, not only for hardware and networking capabilities but also for IT security mechanisms. Annex VI (6.5.3) concerns the unique identification of devices at the level of software; minor revisions do not include security patches. This exclusion implies that security configurations can affect a device’s performance, the safety of use and data analysis. For the confidentiality of personal data, Annex XV (4.5) states the implementational necessity of security mechanisms suitable to tackle data breaches.

In the IVDR [16] security is addressed in five instances, very similar to MDR. First, in Annex I (16.2) and (16.4), programmable electronic systems and the need for their cybersecurity is stated. Second, in Annex I (20.4.1, ah), the establishment of security requirements becomes explicit. Third, in Annex VI (6.2.3), concerning the unique identification of devices at the level of software, minor revisions do not include security patches. Finally, Annex XIV (4.5) sets out the demands for security mechanisms to undertake cases of data breaches.

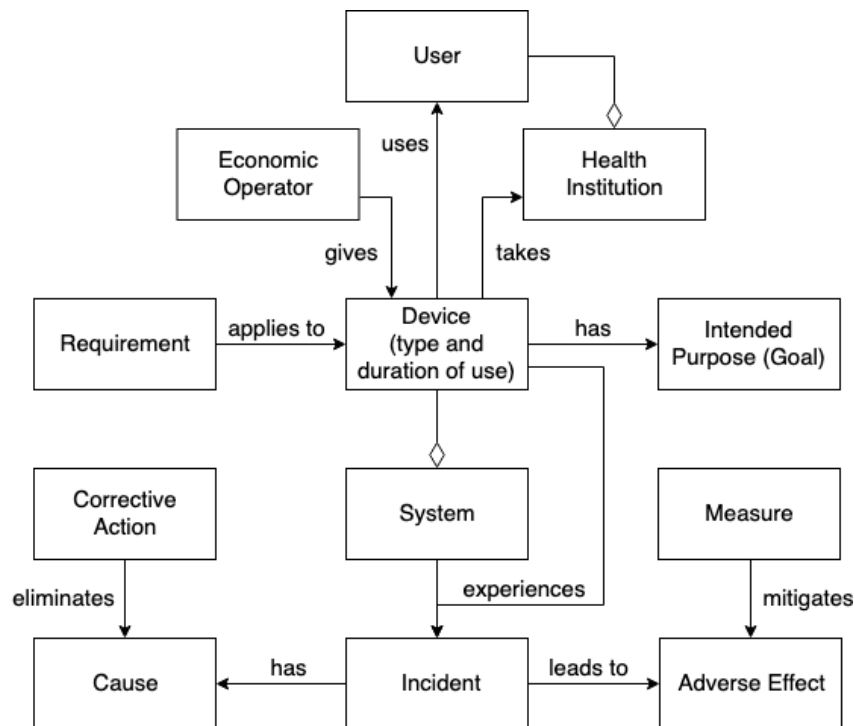


Figure 1.4: Regulations based healthcare model.

These two regulations define the healthcare context of cybersecurity as abstracted in Fig. 1.4. An economic operator can be "a manufacturer, an authorised representative, an importer, a distributor or a person". As such, he/she give devices to healthcare institutions. The user of a device can be an actor with or without medical knowledge. A healthcare institution is an establishment that provides care or treatment of patients/public health. A device (following the definition given above) can be part of a system. A system stands for interconnected assets that aim to achieve an intended medical purpose synergistically. An intended purpose stands for the purpose that the manufacturer of a device designated. Devices and systems experience incidents. Incidents, according to MDR and IVDR are any breakdowns, bugs of a device that can lead to adverse effects. In particular, the regulations define the adverse effects of serious

incidents relating them to the general public's and individuals' loss of lives and/or deterioration of their health state. Corrective actions are taken to eradicate the cause of an incident, whereas mitigative measures reduce the adverse effects that an incident can cause.

To connect medical devices with cybersecurity, using the definitions given from the European Union in Regulation (EU) 2019/881 [16] and Directive (EU) 2016/1148 [17] relevant to cybersecurity, we constructed Fig. 1.5 that depicts how the key terms used in the domain relate to each other. A *network and information system* can be an electronic communications network, a device or group of interconnected devices or data. *Cyber threats* are occurrences that can adversely affect a network and information system and/or its related actors. The defence of network and information systems and the various types of actors that interact with them (e.g., users, operators, technicians) from cyber threats requires *cybersecurity activities*. The two cybersecurity directives use the term *risk* as an overarching word that covers both cyber threats and incidents. *Incidents* stand for an occurrence that negatively affects the cybersecurity of network and information systems. In contrast, cyber threats negatively affect network and information systems, not their cybersecurity. Respectively, *incident handling* deals with every plan that assists the detection, analysis, containment, eradication and response of an incident.

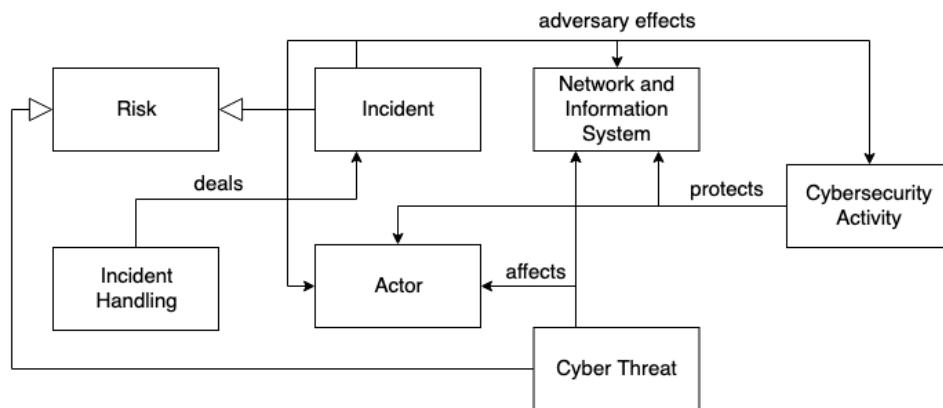


Figure 1.5: Cybersecurity risks terminology clarifications.

From the above, it becomes clear that cybersecurity risk analysis needs to go past the examination of use case scenarios. Instead, cybersecurity needs to cover cases outside the expected use (e.g., misuse and abuse cases). Therefore, the concept of anticipated misuse must be investigated more accurately because the MDM now has to examine all technical possibilities of invasion into the networked MDs. Moreover, in contrast to most other essential MDs's requirements, there are no harmonised standards on cybersecurity and consequently cyber resiliency. Therefore, there is no approved catalogue of requirements that are recognised as reflecting the required state of the art.

1.2 Terminology

This section offers a clarification of the meaning of some standard terms used throughout this document. The terms relating to the design and investigating research activities conducted, meaning either the artefact or the healthcare context with which it interacts. With the term *design*, we refer to decisions made about treatment, whereas *specifications* stand for the documentation of a treatment's desired properties (internal and external).

In design activities, the term *artefact* stands for any entity designed from people with a specific purpose. An artefact can relate to the whole life-cycle of a healthcare system or one

or more particular phases. The users of an artefact are people that are part of the context with which it interacts. Regularly this document uses the term *treatment* and initially the similar in meaning term of *treatment-to-be*. Overall a *treatment* refers to the design of artefacts. These designers are referred to as *treatments* because their contribution to their purpose is subject to validation, and that implies that design is not necessarily a solution but rather an attempt to be tested.

The *validation* of treatment examines how a proposed treatment (i.e., the Build-In ResilieNcy Analysis (BINA) framework and its components) are contributing to the satisfaction of stakeholders goals. Researchers conduct validation within controlled environments where they expose an artefact to models of the context to predict how it interacts. The term *model* is used within this research to refer to *analogic models*. Analogic models represent entities of interest in a way that allows answering relevant questions about them. *Targets* is another way to refer to these entities of interest. For example, in this project, a BINA instance represents resiliency requirements and allows their analysis for a specific healthcare system by design.

This document, in the context of investigation activities, refers to Critical Infrastructures (CIs). There are thirteen officially recognised categories of CIs in the UK; those are chemicals, nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water [18]. The focus of this study is on the CIs identified as critical and entitled 'Health' in the UK. However, there are considerations if the 'Emergency Services' and, more precisely, the sub-sector 'Ambulance' must be included. Nevertheless, the lead organisations regarding the CIs of 'Health' and the Sub-Sector of 'Emergency Services', 'Ambulance' are shared, and we refer to both of them under the term *Healthcare Critical Infrastructures (HCCIs)*.

HCCIs are increasingly dependent on CPSs as is the case with other types of CIs. CPSs merge digital capabilities of communication, monitoring and control with physical functions that take place in the kinetic world of CIs. These systems consist of multiple components, commonly including sensors, actuators, control processing units, and communication devices [19]. CPSs form grids that communicate through networks that make them susceptible to cyber attacks [20]. There is a wide range of CPSs that support the operations of HCCIs. Table 1.1 lists some relevant examples.

The term *Medical Cyber-Physical Systems (MCPSs)* refer more precisely to systems of Medical Devices (MDs) and their components that are critical for life, aware of their operational context and networked [21]. Recognisably, the size and complexity of MCPSs is increasing, making their development a laborious and error prompt process [21]. Lee et al. have categorised them based on their primary functions to monitoring and delivery devices, that collaborate with administrative and decision-support systems[21]. HCCIs incorporate also other forms of CPSs and in particular to what is in this document referred as Medical Facilitys (MFs) [22]. MFs stand for other CPSs used in the same environment as Medical Devices (MDs) and interacting with them (e.g., Building Controls Systems (BCSs) monitors and environmental equipment like boilers, chillers and air conditions).

Cybersecurity studies of HCCIs, like hospitals, also investigate their organisational aspect [23]. In other words, there is research that studies HCCIs as organisations that each one has its unique system characteristics, interactions, dependencies and entities. The term *healthcare system* integrates these three aspects of HCCIs, namely the MDs, the MFs and their organisational characteristics.

Cybersecurity challenges characterise such environments. From threats against medical data to attackers' capabilities to monitor, degrade, destruct, command and control, and deny the operation of a MCPS. In other words, these technologies hold the potentials to be turned

Table 1.1: Examples of Cyber-Physical Systems (CPSs) in Healthcare Critical Infrastructures (HCCIs) (based on [1, 2, 3])

Name	Acronym
Strategic Information Systems	SIS
Management Information Systems	MIS
Operational Information Systems	OIS
Clinical Health Information Systems	CHIS
Administrative Health Information Systems	AHIS
Financial Health Information Systems	FHIS
Business Management Systems	BMS
Care Administration Systems	CADS
Clinical Management Systems	CMAS
Medical Devices and Equipment	MDE
Health Applications	HA
Building Control Systems	BCS
Utility Management Control Systems	UMCS
Energy Management Control Systems	EMCS
Computerised Maintenance Management Systems	CMMS
Computer-Aided Facility Management Systems	CAFMS
Electronic HealthCare Record	EHCR
Decision Support Systems	DSS
Robotic Systems	RS
Simulation Training Systems	STS
Health Telematics Systems	HTS
Health Decisions Computer Simulation Systems	HDCSS

against their original design purpose and inflict harm directly to patients, healthcare personnel and indirectly to society as a whole.

1.3 Background and Research Objectives and Assumptions

Build-In Resiliency Analysis (BINA) is paramount because it helps companies adopt resiliency plans that will not cause further harm. As we have discussed in the previous sections, cyber resiliency needs to support the overall organisational goals. However, the type and amount of incidents that can occur are numerous. Healthcare organisations cannot act on all of them because (i) every resiliency approach has a cost (not only in monetary terms), and (ii) organisations have limited resources. Hence, HCCIs want to make sure that they adopt only resiliency plans that are beneficial or at least not harmful for the specific circumstances of an incident. For example, a software update to a laparoscopic laser during an operation is not about the cyber aspect but also the medical impact on patients and everyone in the operating theatre. Hence a BINA needs to consider incidents not just as a technological issue but also context related.

We have seen that MDMs deal with cybersecurity based on past habits rather than their current context of information. By comparing different responses within the context of a HCCI (e.g., the cost of a healthcare service due to a successful cyber attack), BINA plays a vital role in the alignment of a MDM's business with its cyber resiliency strategy (which at present is

not explicitly consider, but only as part of cybersecurity). However, cybersecurity has a more preventative and protective focus than cyber resiliency that wants to mitigate the impact, eradicate an attack and recover the organisational functions back to their regular operations. In healthcare, we have also observed the absence of harmonised requirements standards on cybersecurity and, consequently, cyber resiliency. Therefore, there is no approved catalogue of requirements recognised as reflecting the required state of the art. HCCI need the means to elicit such requirements as they need to comply with regulations. They need a systematic approach that will offer them traceability and justification of their decisions, and it will contribute to clear communication among diverse stakeholders.

Hence, the results of this research work shall help to reach four different research objectives:

- to deliver resilient ISs (generally in terms of dependence to other response plans and their importance for a specific system);
- to create a link between business cyber resiliency needs and system resiliency measures, provided by risk-based approaches, to obtain a suitable for the system resiliency;
- to perform a priori resiliency analysis (i.e. before the design of a IS), as opposed to a posteriori;
- to produce deliverables under the form of models as proof of cyber resiliency management.

1.3.1 Requirements engineering

Requirements Engineering (RE) takes place during the early phases of the development of an IS. For this work, we adopt the following definition for RE: *"Requirements engineering is the branch of software engineering concerned with the real-world goals for, functions of, and constraints on software systems. It is also concerned with the relationship of these factors to precise specifications of software behaviour and their evolution over time and across software families"* [24]. Although this is subject to debate, researchers often differentiate between early and late RE [25]. Early requirements analysis emphasised understanding the whys of the system-to-be rather than what it should do. What the system should do is addressed during late requirements analysis. We argue that IS development should address security and, consequently, resiliency from early RE. In this context, we define a requirement as *"a condition over the phenomena of the environment that we wish to make true by installing the machine"* [26].

Requirements are further distinguished to functional that focus on what the system should do [27, 28] as opposed to non-functional requirements. There is no clear consensus on what precisely is a non-functional requirement [27], and many different definitions have already been proposed [28, 29]. In this research, we perceive a non-functional requirement as a property, or quality, that the product must have [28]. The literature considers security requirements as non-functional requirements like usability, performance and resiliency. However, regarding security-resiliency requirements, they can be sometimes functional requirements. For example, as depicted in [27] there are security requirements that are functional as focus on what the system should do under certain circumstances. For example, a database should grant access to personal data only to users with an authorised user name and password. Nevertheless, most of the time, security is considered a non-functional requirement [30, 28, 29, 31]. In the context of this thesis, and mainly because most of the security-oriented modelling languages we study consider security requirements as non-functional requirements [32, 33], we adopt this convention.

1.3.2 The important role of RE in the BINA context

The role of RE with regards to Build-In Resiliency Analysis (BINA) can be highlighted, as illustrated in Fig. 1.6. BINA is a specific case of the general business/IT alignment challenge [34]. ISs consist of IT infrastructure, here healthcare-related, and human-based tasks that support the realisation of the business strategy and its associated value scheme. This value scheme consists of knowledge and services planned and managed through processes, assembling organisational competencies [35, 36]. The alignment challenge stems from the IT risks that impact business functions. In healthcare, that could mean that medical devices vulnerabilities can negatively impact the provision of health and even lead to death. Thus, relevant research needs to find ways to mitigate the misalignment of business and technology. Even though a business can have mitigations in the form of controls and countermeasures to protect its technological infrastructure, preventative and protective measures can fail.

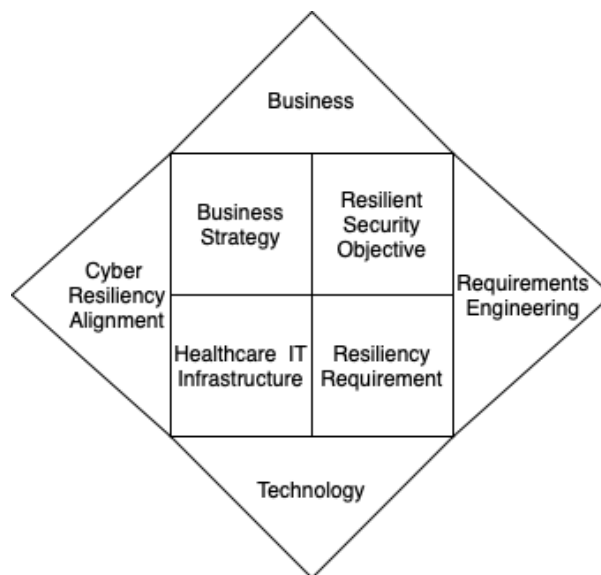


Figure 1.6: Business/IT alignment at the level of resilient cybersecurity.

Nevertheless, critical business operations need to continue. RE and, more particularly, Goal-Oriented Requirement Engineering (GORE) approaches can contribute to that by focusing on the resiliency of cybersecurity [37, 38, 39]. GORE approaches in the literature seem to be valuable and effective for the management of requirements. At the same time, GORE approaches vary in the granularity of analysis and their use in the decision-making process.

More precisely, as depicted in Fig. 1.6, an IT system designer can use GORE: (i) at the business level to understand the resiliency objectives associated with the cybersecurity business strategy; (ii) at the technology level, to express the requirements associated with the resiliency requirements in place to respond, recover and return to normal operations mitigating the impact on the healthcare infrastructure. Requirements will express the expected properties of these resiliency plans in terms of their impact on the negative incidents. (iii) at the business/IT alignment level, the progressive refinement of business resiliency objectives are supported by the IS cybersecurity resiliency requirements. Using GORE approaches, a security engineer can systematically investigate the different alternatives regarding the fulfilment of cybersecurity resiliency goals by resiliency requirements.

1.3.3 Model-based approaches

In software engineering, the classical approach adopted for a long time is to produce maps of the software product before starting the development. This approach is mainly driven by the generalised use of the UML standard [40]. However, when planning for cybersecurity incidents, the introduction of a model-based approach is motivated by several factors, related first to the efficiency of the BINA process, and second to the relevance of the product resulting from the performed process.

Models are structures that help us understand a particular issue of interest. Models can be simplifications of the world, mathematical analogies or exploratory/artificial constructs. When a model's primary purpose is realism, it removes any redundant attributes. Analogical models aim to capture a process, system or phenomenon. Instead of capturing or representing reality, models that represent an alternative reality aim to operate as an analytic and computational tool in which the user can explore possibilities and try new ideas. This type of models allows users to explore scenarios outside what is currently the state of the world.

The three main characteristics that are common among models are simplicity, precision and erroneousness. (i) Models are simple as they remove unnecessary details. (ii) Models make precise definitions. By simplification and precision, they create spaces within which reasoning can generate a hypothesis, design solutions and analyse data. However, (iii) all models are wrong because they simplify through omission [41]. This last characteristic justifies the existence of different models used to analyse the same phenomena.

Independently of its form, a model needs to be tractable. In other words, it must be simple enough to assist reasoning. Model rigour assures rational coherence. That reasoning can then be grounded in evidence by taking models to test, consecutively leading to refinement and improvement. We need models to make sense of the streams of data that we collect. They help us to clarify assumptions and think logically. We can use them to adjust, calibrate and test causal and correlative claims. In other words, reasoning through models is the association of conditions and deduction of rational assumptions.

Apart from reasoning support, models also explain in the form of testable hypothesis phenomena. By relating knowledge and understanding, they facilitate communication and allow exploration of possibilities and occurrences. In addition, models are helpful for predictions and conceptualisation of the unknown. Thus, in many instances, they guide decision making and support strategic, tactical and operational planning and implementational activities.

Overall, models from data lead to intellectual power. Data is raw, uncoded occurrences, experiences or phenomena. Example data within the healthcare setting are heart rate, blood pressure, births and deaths. These data named and partitioned turn into information. For example, hospital inpatients' records and radiographic images. When we organise information, commonly in the form of models, it forms knowledge, such as psychological, biological and bio-socio-psychological models. Finally, intellectual power derives from identifying and applying relevant knowledge, for instance, to know how to apply the biological model to treat a patient.

1.3.4 Research assumptions

Consequently, this research work relies on three main assumptions:

- Considering resiliency during the early phases of cyber-secure IS development is bet-

ter than later in the development process or once the IT healthcare system is already designed;

- Using a GORE approach provides beneficial results to define the resiliency requirements of cyber-secure healthcare ISs;
- To have a model-based approach supporting the Build-In Resiliency Analysis (BINA) process improves the design and final product coming from the various resiliency analysis steps.

1.4 Research scope

This research work is standing in the Healthcare System Cybersecurity Resiliency domain. In this section, we define the different concepts and the boundaries of this research project, summarised in Fig. 1.7.



Figure 1.7: Research scope.

1.4.1 Cybersecurity

The glossary of the Committee on National Security Systems (CNSS) defines 'cybersecurity' as *"the ability to protect or defend the use of cyberspace from cyber-attacks."* [42]. Currently, the literature recognises 'kinetic cyber-attacks'. These attacks are cyber-physical attacks that intend to cause physical damage in the real world to people, buildings, equipment, infrastructure or a nation's way of life. They go beyond virtual attacks and theft of data. Cyber-physical attacks can target systems and unintentionally harm human lives. Thus, the notion of security that we adopt in this work is associated with the CNSS-4009 definition and extends to the physical impact that kinetic cyber-attacks can have. In this sense, 'cybersecurity' protects and defends against kinetic cyber-attacks initiated from cyberspace.

1.4.2 Healthcare

According to NIST SP 800-66 a 'healthcare provider' is *"a provider of services ..., a provider of medical or health services ..., and any other person or organisation who furnishes, bills, or is paid for healthcare in the normal course of business."* [43]. The same standard also refers to 'covered healthcare providers' referring to *"any provider of medical or other health services, or supplies, who transmits any health information in electronic form ..."* [43]. Within this context, the same SP defines as 'health information' *"any information, whether oral or recorded in any form or medium,*

that: (1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.” [43].

CNSSI-4009 defines a ‘critical infrastructure’ as a “system and assets, whether physical or virtual, so vital to (a nation) ... that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” [42]. As we have seen, Healthcare Critical Infrastructures (HCCIs) in the UK need protection from cyber-attacks and kinetic cyber-attacks. An emergency stands for a sudden, unexpected event requiring immediate response due to a possible threat to health and safety or the environment. The concept of emergency connects with resiliency within the healthcare context and the need for HCCIs to be cyber secure. Thus, here we consider cyber and physical aspects of healthcare IS and network beyond healthcare as mere data. This broader definition derives from our perspective that healthcare organisations are Healthcare Critical Infrastructures (HCCIs).

1.4.3 Resiliency

NIST SP 800-34 define ‘resilience’ as “the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.” [44]. Resilience has also taken more specific definitions based on its application to a system or network. More specifically, NIST SP 800-30 defines ‘information system resilience’ as “the ability of a ... system to (1) continue to operate under stress, even if in a degraded condition while maintaining essential ... operational capabilities; and (2) recover effectively and quickly.” [45]. Whereas ‘network resilience’ can be understood as “the ability of a ... system network to (1) provide continuous operation (i.e., highly resistant to cyber-attack and able to operate in a degraded mode if damaged); (2) recover effectively if a cyber-attack does occur; and (3) scale to meet rapid or unpredictable demands.” [46]. This thesis focuses on the generic definition of resilience that we refer to as ‘resiliency’ that includes the more specific definitions of resilient ISs and networks, specifically associated with healthcare organisations.

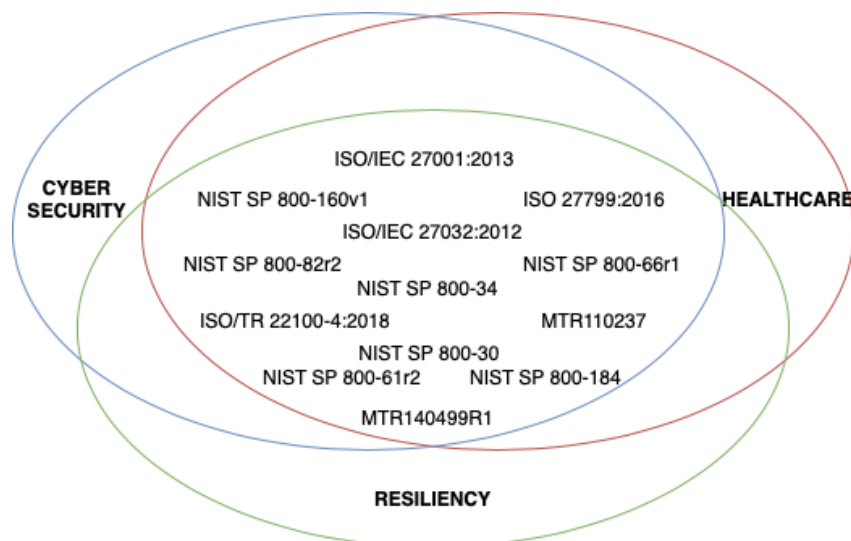


Figure 1.8: Frameworks and standards within the research scope.

1.5 Research Methodology

The choice of a research approach is an essential project decision. Wieringa et al. [47] observed that in the requirements engineering community, research tangles with design [47]. In the cybersecurity context, this observation is critical, especially in regards to security requirements engineering research. The design activity proposes an approach for a specific purpose and results in an artefact. On the other hand, the research activity investigates a topic systematically and results in new knowledge. Design and research activities have differences, but they can be combined within the engineering context. Fig. 1.9 shows three engineering activities that relate to this research project.

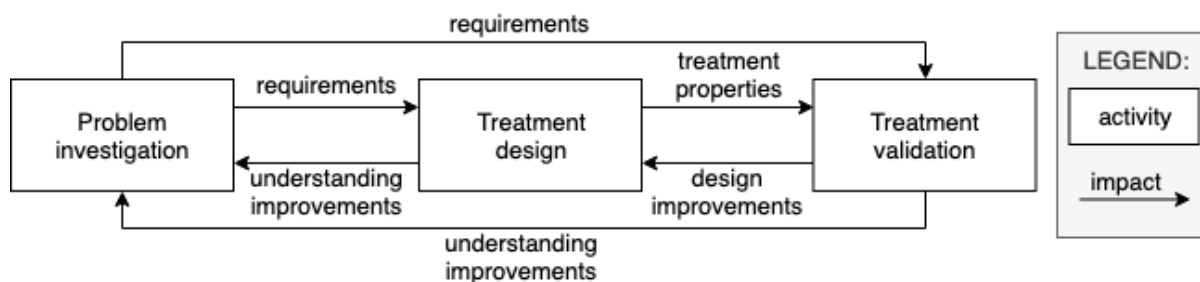


Figure 1.9: Relevant activities in the engineering cycle.

It is common in cybersecurity, including software and security engineering, the engineering cycle to be considered the structure that guides engineering. In Fig. 1.9, we focus on the three activities that are related to this project, namely problem investigation, treatment design and treatment validation. *Problem investigation* examines the current circumstances. *treatment design* proposes a treatment to the current circumstances. Lastly, *treatment validation* investigates the proposed treatment properties. To justify that a design solves a problem, the designer should investigate the problem. To justify selecting one solution rather than another, the designer should refer to the different properties of the solutions as uncovered by solution validations. To justify an implementation, the designer should refer to the solution design that had been chosen.

The excluded activities are the treatment selection, the treatment implementation and the implementation evaluation. We decided to exclude these activities mainly because they require closer collaboration with existing healthcare infrastructures willing to implement the proposed treatment. This project, having predefined and limited time and resources, could be feasible by pursuing three out of the six activities. This part of the engineering cycle is the *design cycle*. It represents a set of activities. These activities do not have to follow a particular order, and experienced designers seem to work with all of them in tandem [48].

Based on the research project's intended outcomes, we used the design cycle to investigate cybersecurity resilience in the requirements engineering practice, propose a treatment and validate its properties before its implementation. Each one of these activities uses different methods, has other types of outcomes and various evaluation criteria. For example, in problem investigation, the focus is on the clarity of the problem, its properties, the method soundness and the significance of its knowledge claim. In treatment design, key aspects are the clarity of the problem to be treated, the novelty of the treatment, the treatment description, and if it can be validated and the discussion of existing competitive treatments. Finally, in the treatment validation, essential is the description of the technique, its properties and soundness, its clarity and contribution to knowledge.

1.5.1 Design Science

Design science is the design and investigation of artefacts in context [49]. We study artefacts designed to interact with a problem context to improve something in that context. To do a design science project, we must understand its significant components: its object of study and its two major activities. The study object is an artefact in context, and its two major activities are designing and investigating this artefact in context [49]. For the design activity, it is vital to know the social context of stakeholders and the project's goals, as this is the source of the research budget and the destination of research results (cf. Section 2.1). The investigative activity requires knowledge of the project's context of the project. We use this knowledge and also contribute to it. The two primary activities and the two contexts form a framework for design science, and this is the framework this project uses. The formation of research question deviated to design problems, and knowledge questions illustrate the two significant activities of design and investigation, respectively.

1.6 Design Problems and Knowledge Questions

Our contribution aims at proposing a model-based approach to support BINA, mainly for early phases of RE, but also applicable in general. This thesis focuses on the modelling language part of such an approach, the methodological part, and the tool support. More specifically, the research questions are as follows:

- **RQ1:** What concepts should be present in a modelling language supporting (build in resiliency analysis) Build-In ResilieNcy Analysis (BINA) for cyber-secure ISs?
- **RQ2:** What metrics are relevant to perform (build in resiliency analysis) Build-In ResilieNcy Analysis (BINA) and reason for cyber resiliency?
- **RQ3:** What is the Build-In ResilieNcy Analysis (BINA) support provided by security-oriented modelling languages, and how it can be improved?
- **RQ4:** How well the proposed methodology supports modelling and reasoning about cyber resiliency requirements modelling and analysis?

1.7 Document Structure

We organised this thesis into nine chapters (cf. Fig. 1.10). The first two chapters investigate state of the art.

- In Chapter 2 we investigate the improvement problem of the way resiliency by design is part of cybersecurity engineering in healthcare systems. More specifically, we identify the main stakeholders for this research project, and we investigate cybersecurity and resiliency challenges within the context of HCCIs.
- In Chapter 3 we investigate the existing literature and elicit the requirements as the desired properties of the treatment-to-be before its actual design. We also review available treatments and compare relevant terminology.

Then we start the design process of a Build-In Resiliency Analysis (BINA) modelling framework, which consists of the definition of the BINA domain model, its metrics, and its comparison with existing security-oriented modelling languages, a process and a tool.

- In Chapter 4 we introduce the domain model of BINA. The research method applied for its construction and how we performed the different steps.
- In Chapter 5 we enrich the BINA domain model with metrics. We present a research method for identifying and eliciting relevant metrics, and we demonstrate its application, combining two complementary approaches.
- In Chapter 6 we assess BINA and how it supports cyber resiliency, comparing it with existing security-oriented modelling languages. The languages compared are KAOS extended to security [50], Misuse cases [32] and Secure Tropos [33]. For Secure Tropos, we propose an adaptation that aims to improve the coverage of the BINA domain.
- In Chapter 7 we introduce a process for applying the BINA domain model and a tool that assists the implementation of this process. The process outlines the types of analysis supported to perform semi-automated resiliency reasoning and the role of the software tool.

Following the design activities, we show how the produced artefacts can be used in concrete experiments.

- In Chapter 8 we present a proof of concept for the BINA methodology using two healthcare case studies. We also evaluate the BINA methodology and tool by survey research and apply it in a real healthcare system under development.

Finally, we summarise the significant findings and discuss future work.

- In Chapter 10 we summarise conclusions and future work related to the research problem of this thesis. We state the claimed contribution of this work and identify limitations that give ideas for future research projects.

The document ends with the Bibliography, which recapitulates all the references used and cited throughout the thesis. Finally, the appendices present some research material used in this research work.

- Appendix A gathers definitions used for the concept alignment of Chapter 4.
- Appendix B is a table summarising the concept alignment.
- Appendix C contains the survey constructs used in Chapter 8.

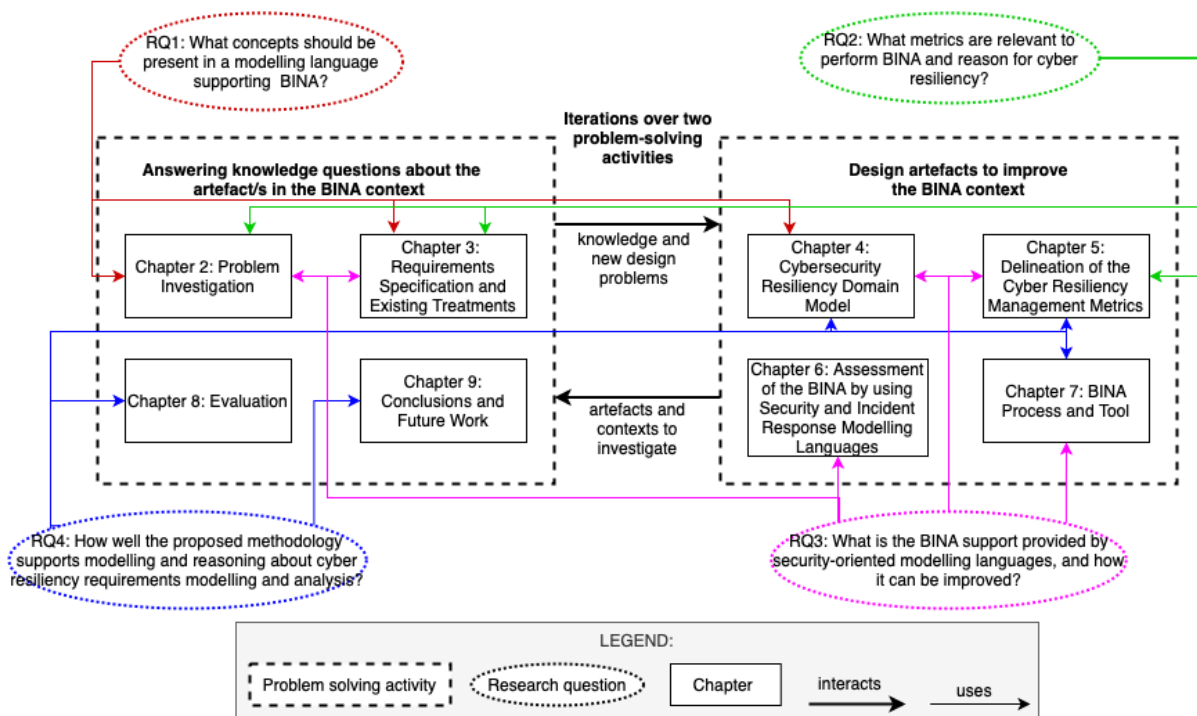


Figure 1.10: Outline of the thesis structure based on research approach and research questions.

Chapter 2

Problem Investigation

The research goal here is to investigate the improvement problem of how resiliency is introduced by design as part of cybersecurity engineering in healthcare systems. This quest precedes the design of an artefact as well as the identification of requirements for the artefact. In other words, the design cycle starts with the study of the problem itself. More specifically, after identifying the main stakeholders for this research project, we investigate cybersecurity and resiliency challenges within the context of HCCIs. The main interest at this stage is in the cyber-physical security phenomena and how they affect stakeholders goals. (cf. RQ1 in Section 1.6)

2.1 Stakeholders and Goal Analysis

The *stakeholders* of a design problem include any individual, group of people or institution affected by the proposed treatment. The definition of stakeholders, actual or potential, is very important for two main reasons. Firstly, stakeholders introduce goals and constraints that affect the treatment. Secondly, different stakeholders can be affected in different ways by the same treatment. For example, security engineers might be better off with a treatment for the problem of cyber resiliency, whereas attackers may be worse off when healthcare systems are cyber resilient by design. For simplicity, here, stakeholders are categorised using roles. A *role* is a class of stakeholder with a different relationship to the treatment under design. For example, both Physician and Nurse are roles within the 'Healthcare Professionals' slot in a hospital. Stakeholders can play more than one roles, such as when a physician is also a patient.

The main stakeholders of this research project are the EPSRC (sponsor), security engineers (end users) and security practitioners (functional beneficiaries). However, this research also has negative stakeholders, namely malicious actors, that will be worse off when healthcare systems are cyber resilient by design. Moreover, threat agents are stakeholders; however, their goals are to use a resiliency design to cause harm. Threat agents are one or more malicious actors that attack the cyber resiliency design instead of attacking the infrastructure. Hence, a treatment will benefit in some respects some of the stakeholders (i.e., EPSRC, security engineers and security practitioners in the context of HCCIs), but will trouble others (i.e., malicious actors as negative stakeholders and threat agents).

More specifically, the stakeholders that benefit from this research introduce goals and constraints that affect the treatment. The *sponsor* is a governmental organisation that has committed budget to design an approach that will improve the current healthcare cybersecurity

practices, having a more holistic than only technical approach. In general, the role of *security engineers* is responsible for establishing and implementing security for infrastructure and its assets. For this research project, security engineers have not committed to using the proposed approach, but there is an increasing interest in a structured approach for the development of resilient by design operational security in HCCIs. It is also essential to take into consideration that healthcare systems have long life cycles and are expensive. Consequently, their change is financially challenging. Moreover, healthcare systems interconnect increasingly with other systems and are software dependent. *Security practitioners* working for HCCIs, for example, Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) will benefit from the output of the treatment as they will manage systems, internally and externally respectively, that have cyber resiliency by-design and not just protective capabilities, in their incident response practices.

Above, we mention for the EPSRC the goal that they pursue and for which they have committed resources to this research project. For the other two stakeholders, namely, security engineers and security practitioners, their desires have been stated above. Desires can be any element of the context, like goals, but stakeholders do not necessarily budget to pursue them. Pursuing the goals and desires of the three main stakeholders, the designer needs to consider potential conflicts among them. This importance stems from the fact that conflict among goals and desires can be a reason to cancel a design project or to change its goals.

The preceding goals and desires yield two main conflicts. Firstly, there is a *financial conflict*. It is possible to form a structured approach for cybersecurity incident response with the current technical means. However, this conflicts with the long life cycles and costly equipment found in healthcare make replacements and configurations challenging to implement as it exceeds the available budget of the stakeholder. Secondly, a *technical conflict* exists, where it would be possible to secure healthcare systems and also to secure their connections with other systems by design covering not only prevention but also response and recovery from incidents. However, currently, we have no technical means to achieve this.

2.2 Systematic Review

Cybersecurity in healthcare is an increasing topic of interest to the research community. Mackey and Nayyar conducted a review in 2013 concerning cybersecurity challenges stemming from illicit pharmaceutical websites [51]. In 2017 Kruse et al. conducted a systematic review in regards to cybersecurity threats and trends in healthcare [52]. The same year Watzlaft et al. examined the cybersecurity practices of healthcare providers, separating security from privacy [53]. Interviews were also used from Jalali and Kaiser in 2018 to investigate from an organisational perspective the cybersecurity capabilities and internal dynamics of hospitals [23]. Jalali et al. also conducted a mapping study collecting and analysing healthcare and cybersecurity-related articles [54]. Coventry and Branley presented a narrative review of cybersecurity issues and gaps for further research, mainly for the healthcare sector [55]. A scoping review of Argaw et al. on attacks and best cyber practices for hospitals argues that more research is necessary for the unique aspects of healthcare, particularly where they interject with cybersecurity recommendations and guidelines [56]. They argue that they need to be more related to the specific needs of the healthcare sector [56].

The particular needs and challenges of different healthcare systems have also been the subject of systematic reviews. For example, Al-Janabi et al. collected cybersecurity problems of healthcare applications using wireless area networks [57]. Camara, Peris-Lopez and Tapiador [58] conducted similar research but specifically for implementable medical devices. Ben

Ida, Jemai and Loukil researched issues eHealth and clouds that are specific to the Internet of Things (IoT) [59]. These reviews address specific aspects of cybersecurity in healthcare, focusing on challenges.

Therefore, it seems that cybersecurity in healthcare is an important area of research that has been the subject of many primary studies that resulted in secondary studies like those presented above. Hence, it seems appropriate to search further within the same context of the primary research, especially in order to (i) gather knowledge about resiliency within the field of HCCIs cybersecurity and (ii) identify the primary methodologies and research techniques used in related projects. Thus, we undertook a systematic review of papers that discuss problems and propose solutions in regards to HCCIs cybersecurity focusing beyond prevention to resiliency and response. In conducting the systematic review, we used the approaches presented in the work of Kitchenham, Budgen and Brereton [60].

Section 2.2.1 discusses the aims of our research, reports related research and identifies the specific research questions we address. Section 2.2.2 reports the search and paper selection process we adopted. Section 2.2.3 reports on the search reliability and section 2.2.4 states the inclusion and exclusion criteria. Section 2.2.5 discusses the research data quality assessment. Section 2.2.6 presents our extraction and synthesis of information from the papers we included in the study. Last but not least, section 2.2.7 discusses the limitations that arose during our study.

2.2.1 Search questions

This review aims to assess whether we need to amend cybersecurity practices in healthcare to reflect the results of cyber resiliency investigations undertaken by cybersecurity engineering researchers. In order to do this, we undertook a systematic review of papers reporting experiences of using the cybersecurity practices in healthcare or investigating cyber resiliency as part of healthcare cybersecurity engineering. We use this information to assess whether cybersecurity has delivered the expected benefits to HCCIs, to identify attacks/threats found by cybersecurity engineering researchers when undertaking incident handling activities, and to elicit and assess proposals aimed at addressing perceived problems with the current practices.

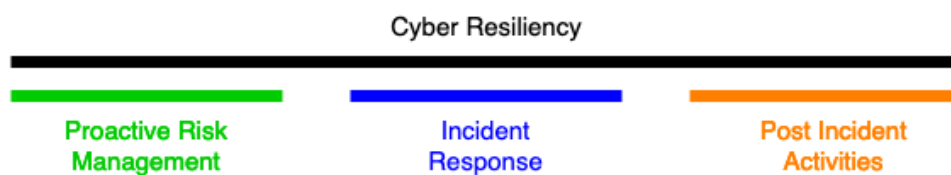


Figure 2.1: Research areas that cyber resiliency covers.

To the best of our knowledge, there has been one relevant study regarding cyber resiliency in healthcare. Cyber Resiliency consists of three main parts: proactive risk management, incident response and post-incident activities, as shown in Fig. 2.1 (cf. Section 2.2.1). Jalali et al. conducted a systematic review of journal articles that focused on cyber incident response in healthcare [61]. As a result, they identified the need to evaluate and improve incident response strategies. Consequently, this review will be valuable by using a wider range of resources than the existing systematic review [61], utilising a different search strategy. It will also provide aggregation and synthesis of results that will aim to identify gaps concerning cyber resiliency of HCCIs. Based on the above, the survey research questions are:

- What papers report experiences of using cybersecurity methodology or investigate cyber

resiliency process HCCIs?

- What problems have been observed by cybersecurity researchers when undertaking cyber resiliency activities within the context of Healthcare Critical Infrastructures (HCCIs)?
- What existing approaches propose related to cyber resiliency tasks, and what is the strength of the evidence supporting them?

2.2.2 Search strategy

We present an overview of the search strategy in Fig. 2.2. This strategy plays a vital role in the planning stage of the systematic review, providing a framework within which we made and documented the necessary study design decisions. In this way, we attempt to minimise bias by defining in advance the steps we follow and the criteria against which we make decisions during the systematic review.

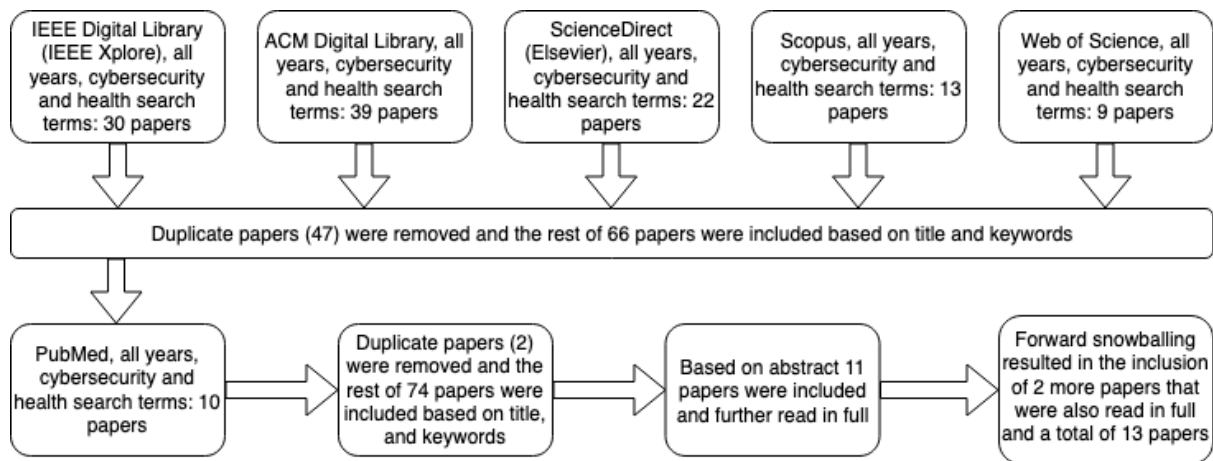


Figure 2.2: Selection process stages.

More specifically, initially, we undertook an informal *manual search* to identify journals and conference proceedings where cybersecurity and incident response intersect within the healthcare context. Instead, we found conferences and journals that connect mainly cyber systems with healthcare (the Studies in Health Technology and Information Systems Journal, the HIPAA Journal, the eHealth security ENISA conference, the International Conference on Biomedical and Health Informatics). Because we had limited access to the context and most of the articles did not cover cyber resiliency issues, we decided instead of collecting papers from specific journals and conferences to expand our sources and move to automated search. Moreover, from the manual search, we realised that there is quite a different terminology used in these domains, and the identification of such keywords could benefit the automated search.

In our *automated search* we used electronic resources such as digital libraries and indexing systems to search for relevant papers. Two essential publisher-specific resources used were the IEEE Digital Library (IEEE Xplore) and the ACM Digital Library, which cover the most critical computing journals and conference proceedings. We also decided to use ScienceDirect (Elsevier) to cover a broader spectrum for this systematic review. Finally, we utilised Scopus and Web of Science also to acquire Wiley and Springer publications. The only drawback for these last two was the expected duplication as they index IEEE, ACM and Elsevier papers but sometimes exclude more recent publications.

Initially, we evaluated each paper for inclusion in relevant papers based on its title and

abstract. We were inclined to include papers at this stage unless they were irrelevant to cybersecurity and/or healthcare. We were also including papers that were focusing only on privacy in healthcare. These resources also allowed us to determine an initial set of keywords useful for further search. The 113 papers identified from the different sources spread as follows:

- IEEE Digital Library (IEEE Xplore): 30 papers.
- ACM Digital Library: 39 papers.
- ScienceDirect (Elsevier): 22 papers.
- Scopus: 13 papers.
- Web of Science: 9 papers.

After removing duplicates, to support the automated search and expand the number of resources that combine the three search criteria (cybersecurity, healthcare and cyber resiliency related terms), we conducted further an automated search using PubMed and a backward snowballing by checking papers cited in the papers identified from the second automated search. To choose the sources of the second automated search, we reviewed the resources identified in the first automated search for journals that appear more commonly as we were planning for a manual search. Because we could not find any patterns, we finally decided to conduct a second automated search focusing on the PubMed database that concentrates on life sciences and biomedical topics. That search resulted in the extraction of 10 additional papers and an overall of 74 papers, having removed 2 duplicates that we had already from Scopus and Web of Science. All the collected papers were further filtered based on their abstracts, resulting in 11 resources. Given the access inclusion/exclusion criteria (cf. Section 2.2.4) and relevance of the papers to the three search criteria (cybersecurity, healthcare and cyber resiliency related terms), after the backward snowballing, we ended up with 13 papers. More precisely, the final decision for the inclusion or exclusion of each paper took place after reading the full papers and assessing their quality (cf. Section 2.2.5).

2.2.3 Search reliability

Regarding the search reliability, the resources identified by the manual search and the backwards snowballing search were compared with the set of papers from the automated search to assess the completeness of the manual and backwards snowballing search. If these searches were sound and the selection process, only the papers published in other sources than those searched systematically should be missed. If the automated search were reliable, then only the papers either not yet published or not indexed should be missed.

2.2.4 Inclusion and exclusion criteria

We defined the inclusion and exclusion criteria before the review of articles. The attempt to answer the review questions ideally is broad in terms of coverage. However, by its very nature, it is limited by some researcher-based characteristics. Hence, we could use sources available to the public and written in English or Greek language. Besides, there are also certain limitations specific to digital sources. As no search engine operates in real-time, the indexes were searched and not the pages themselves; thus, the latest data might be within a monthly interval, or greater [62]. Additionally, we found electronic sources on the web (Web 2.0). The reasons were

that the web offers a plethora of updated resources, has limited costs and good quality. Also, cybersecurity has a robust online presence as offenders and defenders use it to share updates. The inclusion criteria are outlined below:

- The publication is in English.
- Studies about cybersecurity, healthcare, or cyber resiliency.
- Available freely or through the University subscription.
- Present in the web (Web 2.0).
- Public access allowed.

2.2.5 Data quality assessment

Regarding the quality of resources, the processed data-sets contain mainly publications from high impact factor scientific journals and conferences. In the systematic literature review, this quality was the benchmark. We should note that none of the articles in the review process was excluded based on the quality assessment criteria.

Nevertheless, as a reality check, updates were observed from WikiLeaks and blog and tweeter accounts of white hat hackers in the health care sector, such as but not limited to Bruce Schneier and Brian Krebs mainly for cybersecurity issues, Avi Rubin, Sergey Lozhkin and Luis Ayala for hospitals, Billy Rios, Kevin Fu, and Jay Radcliff for medical devices. Also in the list should be mentioned the late Barnaby Jack.

Unofficial or not verifiable sources in security must be accepted and tolerated as denial and deception are a common occurrence in the field. As not officially peer-reviewed, these types of sources have not been included in the results of the systematic search but are considered fundamental. Thus, a part of the research tends to look in 'the wild' but treats only peer-reviewed data as quality sources. We decided to do that here too. Include only verifiable resources but correlate their relation with unverifiable sources, closer related to the field practitioners.

2.2.6 Data extraction and synthesis

We further reviewed resources that met the inclusion criteria to determine research issues and proposed treatments. Each article was reviewed individually, noted and categorised. More specifically, we extracted the identifiers for each resource (title, author, year, journal or conference). Subsequently, we collected from the relevant papers their type (problem investigation (PI) and/or treatment design (TD) or experience/opinion/discussion paper (EP)), the method used and if it performs evaluation/ validation.

We integrated the results from our synthesis with the suggestions we found in the individual papers. The resources were grouped into sets of studies addressing similar cyber resiliency aspects, based on its broad categories as suggested in NIST SP 800-61r2 [4], namely: preparation; detection and analysis; containment, eradication and recovery; and post-incident activity. After the initial aggregation, we looked for any general trends that had not been previously discussed and could indicate a yet unaddressed issue suitable for future research. We then used these suggestions to specify areas where more research is required.

2.2.7 Search limitations

We base this search on digital source and papers that the University of Brighton has access to. Since we conducted an automated search, general indexing systems that supported such analysis were another restriction. To reduce any bias introduced by using specific digital indexing sources, we performed a manual search of essential sources and undertook backwards snowballing. We also tried to avoid personal bias, but we understand that there will be instances where the researchers cannot identify their logical fallacies. Nevertheless, we extracted resources and used predefined criteria to assess the inclusion or exclusion of the resources, tending towards inclusion in cases of doubt. Additionally, as we conducted a systematic review, the set of collected papers represents the knowledge available at a certain point in time. If and when more primary studies become available, a later extended systematic review may well be able to refine and revise the original findings.

Moreover, we restricted our automated search to papers that combined a set of terms from three domains that, for each one independently, has been the focus of excellent depth research (cybersecurity, healthcare, cyber resiliency). Consequently, there might be papers that we have missed, and we could find them with a broader search. The reason for our restriction was beyond time and resources in general, related to the focus of this research itself. We wanted to avoid collecting papers with a broader scope, meaning outside the intersection of the three domains. The main reason was that we had attempted reviews with that logic, but we could not aggregate their results effectively to justify such an endeavour's difficulty. Secondly, they did not always offer information that was meaningful when the domains intersect. To double-check our extracted set of papers, we compared it with a similar systematic review from Jalali et al. [61] since an independent group of researchers collected their set.

2.3 Systematic Review Results

This section discusses each of the papers we included in our study in the context of papers with similar characteristics. More specifically, Section 2.3.1 presents the aggregation results of the 16 articles that met this review's inclusion criteria. Subsequently, in Section 2.3.2 we group and analyse the resources into sets of studies addressing similar incident handling phases, based on the categories of NIST SP 800-61r2 [4] (preparation; detection and analysis; containment, eradication and recovery; and post-incident activity). Finally, we collect and aggregate the conceptual characteristics of their context in Section 2.3.3.

2.3.1 General characteristics

The general characteristics of the collected set of resources included in this review are presented in Table 2.1. There were sixteen (16) resources selected that had been conducted between 2005 and 2021 - the publication venues were diverse, and we could not observe any form of concentration among them. Standard research methods used by the collected body of knowledge seem to be literature reviews, case studies and designs (i.e., machine learning systems and algorithms and conceptual frameworks and architectures - all of them constitute different artefacts that address similar problem contexts). Eleven (11) studies were conducting problem investigation (PI); from them, nine (9) were also proposing a treatment design (TD). Four (4) of the papers presented experiences, opinions, or discussing authors' opinions and issues (EP). From the nine (9) papers that proposed treatments, six (6) of them have conducted some form of validation.

Table 2.1: Characteristics of selected papers shorted by publication year

Citation No.	Year	Publication venue	Research method	Type	Evaluation/ Validation
Information security policy's impact on reporting security incidents [63]	2005	Comp and Sec	Literature Review and Questionnaire	PI	No
Organizational Repertoires and Rites in Health Information Security [64]	2008	Cambridge Quart Heal Eth	Case Study	EP	No
Cyber Resilience in Medical Practice Security Achievable? [65]	2010	Int Cyber Res conf	N/A	PI	No
Incident Response Plan for a Small to Medium Sized Hospital [66]	2013	IJNSA	Redesign of Incident Command System	PI and TD	No
Case study: An academic medical center's response to widespread computer failure [67]	2013	Am J Disaster Med	Case Study	EP	No
Towards Realizing a Self-Protecting Healthcare Information System [68]	2016	IEEE 40th An Comp Sw App Conf	Design Science Research	PI and TD	No
Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks [69]	2016	Appl Clin Inform	Conceptual Approach	TD	No
A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures [70]	2017	IML'17	Machine Learning and Visualisation	PI and TD	Yes
Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization [71]	2017	Inform Health Soc Care	Case Study, Semi-structured Interviews, Questionnaires	EP	No
The challenges of cybersecurity in health care: the UK National Health Service as a case study [72]	2019	Lancet J	N/A	EP	No
ML-based cyber incident detection for Electronic Medical Record (EMR) systems[73]	2019	Smart Health J	Machine Learning, Anomaly detection	PI and TD	Yes
EARS to cyber incidents in health care [61]	2019	JAMIA	Systematic Review	PI and TD	Yes
Healthcare Data Breaches: Implications for Digital Forensic Readiness[74]	2019	J Med Syst	Review and Conceptual Architecture	PI and TD	No
Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem [75]	2020	JCDE	Literature Review, Bayesian network	PI and TD	Yes
A quantitative bow-tie cyber risk classification and assessment framework [76]	2021	J Risk Research	HEMP risk evaluation method	PI and TD	Yes
Towards an organizationally-relevant quantification of cyber resilience [77]	2021	54th HICSS	Design Science Research	PI and TD	Yes

2.3.2 Aggregation based on incident response phases

The set of the collected resources was decomposed and categorised based on the by NIST SP 800-61r2 [4] incident handling phases. The relevant results are presented in Table 2.2. A first observation is that even from the resources that address cyber response, the focus seems to remain in the phases of preparation, detection and post-incident activity. Hence, there seems to be a lack of research in quantity and quality regarding containment, eradication and recovery. That coincides with the categorisation of resources to pre- and post-incident actions in the work of Jalali et al. [54].

Furthermore, it seems that there is no consistent definition of what is the plan that entails incident response. Terms like contingency, emergency, crisis management and incident response seem to be considered interconnected, and their distinction is as important as their coordinating implementation. Another observation relevant to terminology is that response is used interchangeably with the terms 'resilience' or 'resiliency' and 'readiness'.

Preparation

From a simple reference to Table 2.2, it can be seen that many resources aggregate similar knowledge. More particularly, it is repetitively addressed the need for resources referring not only to financial but also to other types such as human availability and systems' redundancies [63, 64, 66, 77]. They also address that the existence and understanding of a security policy is an integral part of incident anticipation [63, 66, 74]. Another important preparation activity seems to be the identification of critical information, systems, actors and the dependencies among them [63, 65, 69, 76]. *Adaptability* appears as an essential characteristic of incident handling and relates to organisational culture, incident characteristics, resources and plans [64, 66].

Stress testing, maintenance and inspections of systems, plans, humans and other resources is essential for cyber resiliency [64, 65, 67, 72, 61, 74, 75]. Communication among individuals and teams, external and internal parties is also addressed in current studies and is further associated with collaboration and continuous training [64, 66, 71, 61]. Cyber resiliency is analysed following either what we call here a top-down or a bottom-up approach. A top-down approach means that resiliency is considered at a critical infrastructures level and usually involves governmental participation [63, 64, 66, 74]. In a bottom-up approach, resiliency is analysed at a healthcare organisation (e.g., hospital) level and involves heterogeneous internal and external participants [65].

Detection and analysis

Independently from preparedness and preventive security mechanisms, incidents can still occur. When that happens a Root Cause Analysis (RCA) should be conducted at this phase [64, 68] to guide incident categorisation [66, 67, 71]. In the phase of an incident, healthcare organisations need to have and maintain communication with internal and external parties that they will use for compliance with legally required notifications [64, 66, 67, 72, 61]. Forensic analysis is initiated at this phase and supports incident classification, prioritisation and damage assessment of the affected entities [66, 61, 74].

In correspondence with an *adaptive* incident response plan, data monitoring needs to be as close as possible to real-time and continuous [67, 68, 69]. This approach of data collections supports forensic activities and further requires their secure storage [61]. A logging system

Table 2.2: Aggregation of selected papers based on incident response phases by NIST SP 800-61r2 [4]

Citation No.	Preparation	Detection and analysis	Containment, eradication and recovery	Post-incident activity
Information security policy's impact on reporting security incidents [63]	+ Security policy (deterrent) + Identification of critical information + Budgetary support	+ Limited effectiveness of security policies	N/A	+ Policy for reporting incidents (occurrence and 'seriousness')
Organizational Repertoires and Rites in Health Information Security [64]	+ Organisational ethics + Stock of resources + Concern for member well-being + Commitment to open business practices + Standardised communication process + Adaptive corporate culture + Stress testing prior to development + Support self-sufficiently complex and multi-vendor applications + Build trust between teams	+ Seemingly independent ques + Compartmentalised sense making + Root cause analyses + Effective internal organisational communication + Notification (legal support)	+ Different people and processes with different goals and priorities + Ad hoc approach + Sustain communication + Mobilisation of technical experts + Legal support counselling	+ Documentation + Procedural problems identification/ Assessments + Recommendations/ Lessons learned
Is Cyber Resilience in Medical Practice Security Achievable? [65]	+ Build, understand and test a business continuity plan + Secure information exchange for the national e-health system + Understand and act on organisational resilience + Understand dependencies and the importance of end-points + Strategy that includes recovery (responsibility and coordination) + National level security for e-health system	N/A	N/A	+ National impact (non-operational healthcare services)
Incident Response Plan for a Small to Medium Sized Hospital [66]	+ Have adequate Cyber Incident Response Team + Reporting requirements to individuals and regulatory agencies + Prevention security systems + Trained personnel (responsibilities and limits) + Security policies + Adjustable plan and resources to incident-specific characteristics	+ Forensic analysis + Identification of effected entities + Violation categorisation + Notification/ Incident reporting + Classification and incidents' prioritisation	+ Eliminate further damage (short and long term goals and actions) + Forensic evidence preservation	+ Lessons learned + Documentation
Case study. An academic medical center's response to widespread computer failure [67]	+ Maintenance and testing of active IT disaster recovery program	+ Data collection (ongoing) + Categorisation of incident + Establishment of emergency operations command centre + Selection of suitable response + Communication with external parties (for support and collaboration)	+ Activation of downtime procedures for services provision and logging activities + Prioritisation of restorations	+ Debriefing and draft of AAR + Demobilisation of emergency operations command centre
Towards Realizing a Self-Protecting Healthcare Information System [68]	+ Monitor and anticipate attacks + Assess security risk (impact and likelihood) + Characterise systems + Establish baseline security controls + Real-time monitoring	+ Determine attacks + Early warning based on historical data and real-time data feeds + Real-time event analysis + Use of Intrusion Detection Systems	+ Assessment and implementation of optimal responses + Control mechanisms for neutralisation of attacks + Use of Intrusion Response Systems	N/A
A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks [69]	+ Correct installation and configuration of computers and networks + User-focused defensive strategies	+ Continuous monitoring of computer and application usage	+ Timely response and recovery	+ Take actions to prevent recurrence
A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures [70]	N/A	+ Machine learning and visualisation for patterns identification	N/A	N/A
Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization [71]	+ Internal communications	+ Need for electronic incident logging system + Incident severity level determination	N/A	+ Have a structured way to gather and redistribute incident knowledge + Identify policies and processes that undermine existing defences + Identify any weaknesses in staff competency
The challenges of cybersecurity in health care: the UK National Health Service as a case study [72]	+ Systems upgrade	+ Cyber incidents are required to be reported and registered in the NHS	N/A	+ Need for governmental oversight of digital transformation
ML-based cyber incident detection for Electronic Medical Record (EMR) systems [73]	N/A	+ Machine learning for anomaly detection	N/A	N/A

Citation No.	Preparation	Detection and analysis	Containment, eradication and recovery	Post-incident activity
EARS to cyber incidents in health care [61]	<ul style="list-style-type: none"> + Establishment of IRP + Notification of key actors (including law enforcement and legal counsel) + Employee disciplinary actions plan + Construction of contingency plan + Mock testing of recovery plans + Network segmentation + Devices inspections 	<ul style="list-style-type: none"> + Forensic incident investigation + Initiation of corrective action plan and notification methods + Evidence secured and documented + Damage assessment 	<ul style="list-style-type: none"> + Vulnerabilities patching + Based on system criticality disconnection of compromised systems + Algorithmic recovery support 	<ul style="list-style-type: none"> + Incident documentation + Documentation of incident response (and chain of custody) + Dissemination of knowledge and lessons learned
Healthcare Data Breaches: Implications for Digital Forensic Readiness [74]	<ul style="list-style-type: none"> + Clear understanding of what constitutes health information + Establish operational and infrastructure readiness 	<ul style="list-style-type: none"> + Digital investigation (forensic audit logging) 	N/A	N/A
Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem [75]	<ul style="list-style-type: none"> + Predictive inference reasoning and sensitivity analysis + Identification of potential factors that are responsible for the disruption 	N/A	N/A	<ul style="list-style-type: none"> + Update of the proposed cyber risk assessment tool
A quantitative bow-tie cyber risk classification and assessment framework [76]	<ul style="list-style-type: none"> + Assess risks + Visualise areas of concern + Understand the risk posed by individual threats 	N/A	N/A	<ul style="list-style-type: none"> + Record the effectiveness of implementing control barriers + Guide insurance product development + Understand consequences or risks to different industry sectors
Towards an organizationally-relevant quantification of cyber resilience [77]	<ul style="list-style-type: none"> + Simulator + Resilience exploration + Quantification of cyber resilience 	N/A	<ul style="list-style-type: none"> + Redundancy + Deception 	N/A

can also support this collection and storage of pieces of evidence [71, 72, 74]. The literature, to ensure appropriate actions will follow the detection of an incident, supports the establishment of an emergency operations command centre that, based on data, will select and initiate a suitable incident response plan [67, 61].

Containment, eradication and recovery

Incident Response Teams (IRTs) in order to contain an incident, they need to have the technical and legal expertise and sustain communication with all the necessary parties [64]. At this phase IRTs want to eliminate any further damage [66]. They can achieve that through a diverse set of control mechanisms to initially neutralise an attack, using, for example, incident response systems; segmentation of networks; redundancy; deception; disconnection of affected devices and algorithmic recovery support [68, 61, 77]. These are all relevant with downtime procedures, vulnerabilities patching, and forensic evidence preservation [66, 61]. For the implementation of these controls and activities, what seems to be essential is the way with which IRTs prioritise restoration activities [67].

This prioritisation seems in case studies to be an essential capability, and current ad hoc practices seem to indicate that [64]. However, within healthcare organisations, there are various people, processes and technologies that are prioritised differently under different circumstances [64, 66]. Thus an ad hoc mentality is not optimal as attacks are complex, and they can introduce delays and further vulnerabilities that can allow more attacks, more significant impact or increased costs [64, 68].

Post-incident activity

After the demobilisation of the emergency operations command centre, healthcare organisations need to take actions to prevent an incident's recurrence [67, 69]. In addition, regulatory oversight might be necessary in cases of health sector-wide digital changes following an incident [72]. To list and initiate the necessary changes and determine how wide they need to be, identifying what went wrong is necessary. After debriefing takes place based on re-

ports of incident occurrence and severity resulting from the previous phases, assessments take place [63, 64].

These assessments have as their goal to identify procedural problems and conflicts with existing defences, weaknesses in human resources competencies and assess the social implication collecting data also from external organisations [64, 71, 65]. All of these assessments take place based on specific plans for gathering the relevant evidence [71, 76]. After the collection of this knowledge, its redistribution back to the healthcare organisation occurs [71, 61]. Essential part of this process is the documentation of the recommendations and lessons learned that commonly take the form of a After Action Report (AAR) [64, 66, 67, 61, 75].

2.3.3 Aggregation based on context

Terminology

We were interested in identifying the extent to which the way the key terminology of the selected papers had the same meaning. The common terms identified were: *healthcare*, *incident*, *response* and *security* and they are examined based on the context they cover for each paper (cf. Tab 2.3).

Healthcare overall appeared to have five different meanings. In 3 papers coincides with the term hospital [63, 66, 67], in 9 papers with a form of a system, including Medical Cyber-Physical Systems (MCPSs), Electronic Medical Record (EMR) systems and healthcare information systems [64, 65, 68, 69, 70, 73, 75, 76, 77], in 3 papers as a Healthcare Critical Infrastructure (HCCI) or a particular type (e.g. National Healthcare Service (NHS)) [65, 70, 72], in 2 papers addressed healthcare organisations in general [71, 61] and 1 was focusing on healthcare information [74]. The majority of the above papers interpret the term healthcare as a type of healthcare system. It is important here to clarify that the number of papers corresponding to meanings (18) is greater than the set of papers collected (16) is that in some papers, the same term is used but is given multiple meanings. The same holds for the rest of the terms and the corresponding number of papers with similar interpretations.

The set of collected papers interprets the term *incident* in four different ways. The majority of papers (10) consider an event such as updates, hardware failures, emergencies, human errors, natural disasters, misuse and abuse cases as occurrences of incidents [63, 64, 65, 67, 71, 73, 74, 75, 76, 77]. In four (4) papers an incident is interpreted as a cybersecurity attacks like hacking, ransomware and Advanced Persistent Threats (APTs) [68, 69, 70, 74]. Two (2) papers use the NIST SP 8000-61 definition either explicitly or implicitly [66, 61] and one (1) paper focuses on the effects of an occurrence on systems functions and society as an incident [72]. Here, an incident definition exists, and each study chooses to focus on an aspect of an incident. Other studies seem to choose a wider scope, that of event that also includes incidents and subsequently cybersecurity incidents.

When it comes to *response*, four (4) papers address specific aspects/phases like detection, forensics and post-incident activities [70, 71, 73, 74], three (3) papers refer to all the phases of incident response [64, 66, 69], three (3) papers analyse response overarching manner ranging from reactive on the one end and on the other to proactive adaptable responses to incident characteristics [63, 68, 75], in three (3) papers response is studied within the planning context in the form of an Incident Response Plan (IRP) along with other types of plans like emergency plan and business continuity plan [67, 61, 77]. Response is also considered closely associated

Table 2.3: Aggregation of papers context

Citation No.	Healthcare	Incident	Response	Security	Stakeholders	Challenges
[63]	Hospital	Computer abuse (violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices)	Risk analysis, reactive	Medical information, insider threat, defence (deterrents and preventives)	Health care industry, federal and state legislators, and researchers	Enforcement practices, detection capabilities, human controls, security planning and evaluations, ethical framework for computer use, absence of proactive response, how computer abuse is documented in hospitals? the effectiveness of security policies in the seriousness of computer abuse incidents
[64]	Patient Portal	Ongoing events (cascading errors, accidents, and breaches), unexpected and nonsensical situations	All life-cycle phases information	Organisation wide	Heterogeneous internal teams and healthcare organisations	Rich incident response organisational repertoire (culture, people, processes, and technology integrated with reliability and ethos development)
[65]	Healthcare National Infrastructure, interdependent system, primary care	Emergency (no consideration of deliberate attacks)	Resilience as ability to recover, returning to an original state, after some disruptive event	Medical information, malleable but not breakable, interdependence and resilience in security, inherent vulnerabilities in its construction and use	Healthcare providers	Lack of knowledge and acceptance of cyber risk, limited time and resources, disaster recovery plans focused on individual practice recovery only, outsourced policies/procedures, no consideration for the security of end-points and access points, security and resilience are not considered as a whole, resilience undefined and even unconsidered in e-health, diverse and privately owned systems, lack of responsibility understanding, need for a coordinated approach to resiliency
[66]	Hospital (small or medium sized)	NIST SP 800-61 and any illegal activity involving Hospital computers, data or both	All life-cycle phases, adjustment of Incident Command System for fires	Patient information, similar to safety from natural disasters	Heterogeneous incident command teams and actors, management of small and medium sized hospitals	Absence of security capabilities in small and medium sized companies, evolution of threat landscape
[67]	Hospital	Erroneous anti-virus update resulting to hospital-wide downtime	Emergency planning, business continuity, coordinated inter-departmental	Organisation wide scope	Healthcare organisations, research community	Security guidelines created for enterprises that do not provide healthcare, quantitative disaster contextualisation
[68]	Healthcare information systems	Known and unknown attacks	Proactive self-protection heal and self-protect within the organisational context	Proactively self-configure, self-optimize, self-	Healthcare organisations	Limited financial resources, scarcity of cyber security professionals, evolving threats, and complex network infrastructure, need to reduce human involvement, different communication standards that need to be secure and resilient, sophisticated cyber attacks
[69]	Hospital's computing infrastructure	Ransomware attacks	All life-cycle phases	Socio-technical problem	IT professionals, health care organisations, and end-users	Need for centralised learning system for incidents, need for similar approaches for other security challenges
[70]	Healthcare infrastructures, MCPs	Large scale attacks, APTs,	Detection based on data behaviours and users' profiles	Cyber-physical approach, machine learning system	Information security officers	Insecure medical devices, legacy systems, bespoke software, user-behaviour analysis, larger data-sets, consideration of the specific hospital's context
[71]	Healthcare organisations	Hardware failures, human errors and policy violations	Method to improve the aspect of incident learning	Medical records	Healthcare and IT professionals	Organisational practices limited to technical processes, limited practice of post-incident learning activities, lack of willingness to share lessons learned with other organisations, ineffective communication among different stakeholders, lack of incident learning motivations, need for communication among involved actors with varying levels of competence and background knowledge
[72]	NHS	Affects on system functions and society	Management of incidents	Cyber-physical	Researchers, governmental bodies, healthcare practitioners	Organisational structures complexity, accountability, inconsistent and heterogeneous technological landscape, no catalogue to systematically list all software and hardware deployed within the NHS, incident data not systematically processed and assessed at an infrastructure level, need for resilience capability assessment, lack of clearly defined responsibilities and security preparedness

Citation No.	Healthcare	Incident	Response	Security	Stakeholders	Challenges
[73]	EMR systems	"event that impacts the confidentiality, integrity or availability of an EMR system"	Detection	Confidentiality and availability of EMR systems, Cyber attack machine learning detection mechanism	Researchers, security practitioners in healthcare organisations	Response to incidents stemming from trusted insiders (systems and users), need for real data-sets, reduction of the implementation costs of machine learning security defences
[61]	Healthcare organisations	Cybersecurity incidents	IRPs	Cybersecurity response plans in healthcare, construction of better response strategies	Cybersecurity professionals and managers in healthcare organisations	Evaluation of incident response strategies in healthcare, tailoring of IRPs to organisational context, lack of research in incident response
[74]	Health information	Focus on privilege misuse, reference to hacking ransomware, phishing, privilege abuse, and misuse of EMR systems	Forensic audit logging	Health information forensics based on commonly involved assets and current threat landscape	Health service providers	Validation and practical applicability of proposed forensic architecture
[75]	System of systems	Fail to perform	Autonomous and intelligent cyber defence	Protection from cyber attacks	Recovery practitioners	Focus on electrical network system, can be strengthened by updating data/ prior belief
[76]	Hospital's IT systems	Cyber risk, threats, cyber breaches/cyber-attacks	Risk evaluation	Insurance costs	Insurers	Cyber risk modelling, quantification and the lack of historical claims data
[77]	Target system	Deliberate attacks, accidents, or naturally occurring threats or incidents	Prepare, adopt, withstand, recover [42]	Ability to continuously deliver the intended outcome	Organisations with critical missions	Time-management of response, validation and simulator calibration

with resiliency and recovery in [65], with management in [72] and with insurance in [76]. The selected set of papers studies response from many aspects, usually related either with its phases individually or as a whole and in other studies as broader positioning of response within healthcare organisations.

The concept of *security* is commonly associated with safety. Within this set of papers, that was the case only in [66] and even there, the proposed security approach adjusts to meet cyber-security needs. Examining papers spreading through the years (2005-2021), it also seems that security mostly in the past but also in the present focuses on information security and confidentiality, integrity and availability properties [63, 65, 66, 71, 73, 74, 75, 77]. However, in more recent studies, cyber-physical aspects are studied as well as moving from Information Technology (IT)-security to what is referred to in the broader literature as Operational Technology (OT)-security [70, 72]. Specific aspects of security are also studied in the relevant literature. The conceptualisation of security as vulnerable [65], the adaptability of security [65, 68] are two such examples. Moreover security is addressed from a socio-technical perspective [69] as an organisation-wide issue [64, 67]. In some cases defence [63] and forensics [74] as important elements of security are studied based on plans and insurance policies [61, 76]. Thus, security evolves as threats do. The threats become more sophisticated and dynamic, and security interpretations and knowledge reflect these changes.

Stakeholders and Desire Conflicts

We were also interested in the stakeholders of the projects. Most papers identified their stakeholders explicitly. When that was not the case, we made assumptions about the most relevant possible stakeholders. By doing so, we had the first indication about other sources that this project's stakeholders could retrieve treatments relevant to their goals, as specified in Section 2.1. More specifically, this project's *sponsor* (EPSRC) could refer to the socio-technical approach relevant to ransomware attacks [69]. This paper covers their need for a socio-technical approach to healthcare security partially, as is specific to one type of attack. *Security engineers* interested in systems dependencies and structured approaches to resilient operational security in HCCIs by-design could use the following resources [67, 61].

However, these works do not convey the details about how to transfer the existing knowledge to a healthcare system's development process. *Security practitioners* could benefit from the

usage of machine learning approaches, response algorithms and patterns identification [70, 73, 74] incorporating them in their incident response practices. Nevertheless, these treatments address parts of the problem and do not address actual managerial planning and decision-making within an evolving healthcare context. Moreover, as shown in Fig 2.1, cyber resiliency covers much more than just incident handling. Thus, further research on the subject is necessary to address the goals of our stakeholders.

Existing research indicates areas where more domain-specific research is needed. It is possible to form a structured approach for cyber resiliency with the current technical means. But validation and evaluation approaches for the assessment of IRPs and their resiliency capability is limited [63, 64, 66, 72, 74]. Additionally, the *financial conflict* of our project's stakeholders desires (cf. Section 2.1) is recognised in the relevant literature as a challenge [68, 73]. More restrictions in the form of time, security capabilities, actors skills, responders motivation and heterogeneity among systems are also addressed [64, 65, 68, 71, 72, 73] showing the need for a holistic approach.

The technological heterogeneity that introduces complexity associates with the healthcare context, and that yields the second stakeholders desire conflict, the *technical conflict* [70, 61]. Specific security mechanisms exist for aspects of cybersecurity [63], but research related specifically to cyber resiliency, let alone in healthcare, is very limited [61]. This is coupled with the challenges of incident quantification [67] and cyber risk assessment [64], enforcement of response plans and security practices during an incident response [63, 72] and the lack of cybersecurity expertise that results in outsourced resiliency that does not correspond to healthcare contextual needs that have the human-in-the-loop [64, 71].

2.4 Stakeholders Challenges and Goals

The financial conflict in the healthcare context rises from two of its particular characteristics. Firstly, the cybersecurity investments for the healthcare sector were chronically scarce, and only after actual incidents occurred, more investments were made [72]. However, resource allocation in the healthcare sector traditionally prioritises patients' safety. The importance of safety for healthcare organisations with limited resources results in trade-offs with other requirements, such as cybersecurity and resiliency related [72]. Secondly, the financial conflict is rooted in the long life cycles that characterises Medical Devices (MDs). Through the time frame of their use, the regulatory environment in which MDs operate changes and their designers and vendors have the responsibility to respond to newly discovered vulnerabilities, primarily when they concern operating systems and software [78].

A step toward addressing such challenges is by considering these issues at the design level [78]. The paradigm of security-by-design is well known. However, there is a need for cyber resiliency to be considered by design for healthcare systems. This consideration is relevant not just to the initial MDs design but to the design of incident handling approaches when threats materialise [78]. Furthermore, this approach can contribute towards affordable security by informing further the design process through the lessons learned [71].

Moving to the technological conflict, it seems to derive from particular characteristics of the healthcare sector that differ among various categories of MDs and even from one HCCI to another. In the case of MDs, energy and computational resources restrictions make many standard security mechanisms inapplicable (e.g., biosensors have energy limitations that rents some cryptographic cyphers out of reach) [78]. Designers need to be able to identify such

constraints from the design level and combine them with the environments in which they operate; in this example, the human body [78, 69]. Another technical limitation is related to the exchange of keys to secure communication channels as critical implementation constraints exist (e.g., pre-distributed secret keys can be compromised) [78].

It is especially challenging in closed-loop MDs, where the patient does not participate in a device's control, to make the necessary updates as a device designer or vendor. Security driven changes require configurations of the device's variables and actuation thresholds that can affect a device's behaviour [78]. Such configurations can be complicated to implement not only because these devices are sensing and actuating inside the patient but also because the suitable means to inform a patient can cause distress and affect an already fragile healthcare condition [78]. These are also social constraints imposed in the provision of a security approach, especially when it concerns the incident response planning, where such updates might be unavoidable and crucial for a patient's life, especially as malicious actors are involved.

These conflicts (financial and technological) need to be explored further in connection with stakeholders goals (cf. Section 2.1) and research challenges, as indicated in the literature. In this way, they can highlight the particular aspects of the problem domain that a potential treatment will need to consider.

The sponsor's goal for a *holistic and not just a technical cybersecurity approach in the healthcare context* relates with the complex challenge that characterises healthcare systems as they have cyber, physical and human components that produce and consume data. For example, insulin pumps that deliver medication to a patient's circulatory system are informed by the physiological characteristic of the patient's condition and, based on them, control the medication delivery appropriately [79]. This characteristic that makes healthcare systems cybersecurity design different from other systems is commonly referred to as the human-in-the-loop challenge. This challenge is further related to the user's capabilities of control over MDs. For example, open-loop MDs can be subject to social engineering attacks from a malicious entity to exploit human vulnerabilities [78]. In such cases, an attacker, instead of compromising the MDs (e.g., insulin pump system) it can rather mislead a user (i.e., patient) into making unsafe adjustments (e.g., the altered from the attacker glucose reading that the patient sees, leads him/her to inject more or less insulin than the one needed).

These problems are present and need treatment urgently. Characteristically, the National Healthcare Service (NHS) has been subject to criticism about the lack of organisational cybersecurity support and ineffective accountability when incidents do occur [72]. There is also increasing concern about data breaches initiated from internal malicious actors [72]. Moreover, it becomes clear, especially in the case of MDs, that the users need to understand possible systems' risks and be comfortable with the deployment of security mechanisms. This need is also relevant to cases where security configurations need to take place in a MD that does not involve user interaction (i.e., closed-loop MDs). For example, in response to an incident against an implantable cardiac defibrillator, the MD senses and actuates. That means that from its very design, it needs to consider such threats that can target the communication channel among its components or the sensing input that will lead to an incorrect actuation [80].

Security engineers looking for a *structured approach to develop by-design resilient operational security in HCCIs* face the lack of suitable existing treatments that do not consider just a heterogeneous and inconsistent IT landscape or its cybersecurity, but also understand the critical role of the problem context, especially of healthcare. Security engineers encounter another crucial challenge related to the prediction of threats and the collection of relevant data. Many reasons result in this challenge. On the one hand, security engineers are aware that the discovery of compromises is partial, and some successful attacks remain unknown. Additionally, even

when the discovery of compromises happens, their reporting might be omitted from fear of legal liabilities and costs. Furthermore, the cybersecurity community does not uncover any specific compromise facts as other malicious actors can use them to create updated exploits. Even when some data about attacks are released, they can be misleading, incorrect or even changed, and there are always zero-days that remain unknown until those that discovered them use them.

Security practitioners want systems designs *useful for their incident response practice*. They face the challenge of having cyber incidents data that are not systematically processed and assessed [72]. In other words, security practitioners cannot measure cyber risk, and vulnerabilities at a local level [72]. This inability results in the inability to plan and implement proper incident handling. They have to argue about resources allocation but lack the means to base and combine such needs on automated decision-making supported from agreed in advance treatment models.

2.5 Discussion and Closing Remarks

In this chapter, we identified this research project's stakeholders and their goals. We then investigated the existing literature systematically. The overarching aim of the systematic review was to investigate the effect, positive or negative, of the phenomena on stakeholders' goals. Throughout this review, it became apparent that the number of relevant studies is limited. Therefore, we aggregated them based on the incident response faces and the standard terminology. From there, it derived that to address the sponsor's goal for a *holistic and not just a technical cybersecurity approach in the healthcare context* there is a need for a by design framework that aims to enhance the cybersecurity decision-making MDs by considering socio-technical aspects that affect the resiliency of HCCIs. A treatment that addresses the security engineers' goal needs to connect cybersecurity with the healthcare context. Security practitioners will be better equipped to manage systems that have considered cyber resiliency and guide them to the development of incident response plans suitable for the infrastructure they are responsible for defending. In the following chapter, we explore existing treatments with the satisfaction of the goals and desires of this project's stakeholders facing the critical financial and technological challenges that concern them.

Chapter 3

Requirements Specification and Existing Treatments

3.1 Requirements Specification

The requirements specification design activity defines the desired properties of the treatment-to-be before its actual design. The actual specification guides the search for possible treatments. A *requirement* can be considered for this section as a goal for the treatment-to-be motivated from the stakeholders goals (cf. section 2.1). We refer to these requirements as *treatment requirements* (also abbreviated as TRs). The stakeholders' goals support the specification of TRs as these goals motivate the desirability of the specified TRs. Each TRs has two parts. It states *artefact requirements* (part 1) along with the relevant *context assumptions* (part 2). The order of the parts can vary.

Because rarely stakeholders that are involved in the problem can specify their requirements, design researchers, as owners of the problem (and thus also stakeholders), make choices jointly or on behalf of the other stakeholders [81]. In order to highlight the particular aspects that a potential treatment will need to have, the requirements specification activity takes the two conflicts (financial and technological) as identified in the systematic review 2.4. It explores them further concerning them, along with the stakeholders' goals and the research challenges indicated in the broader literature. In this way, the design researcher uses existing knowledge for the specification of requirements. Based on this knowledge of the healthcare cybersecurity resilience problem, the requirements for the treatment-to-be are as follows:

- **TR1** The treatment must allow security engineers to have a structured approach to develop by-design resilient operational security for healthcare systems of HCCIs.
- **TR2** The treatment must be usable for security engineers, i.e., by using the treatment, security engineers assist HCCIs and their security practitioners to be resilient to incidents.
- **TR3** The treatment must be useful for the security practitioners in their incident response practice, i.e., the effort to learn and to use are acceptable.

TR1 is a functional correctness requirement, and the other two (TR2 and TR3) are nonfunctional requirements. A *functional requirement* stands for the desired function of the artefact, where *nonfunctional requirements* stand for properties that must characterise the interaction of the artefact with its context. Stakeholders goals drive the requirements for usability and usefulness of the treatment-to-be. They are meaningful under context assumptions. In particular,

cybersecurity incidents that occur or affect the operational resilience of healthcare systems within HCCIs. The specified requirements motivated the RQ2 that we encountered earlier in Section 1.6.

3.2 Requirements Contribution to Goals

To connect stakeholders goals with requirements specified by the design researcher, we present them in the form of a *contribution argument*. A contribution argument consists of the artefact requirements and context assumptions indicating how they contribute to a stakeholder's goal. In other words, a contribution argument entails a treatment requirement and how it meets a stakeholder's goal. In this essence, a contribution argument forms a hypothesis in the form of a prediction that an artefact inserted and interacting with the problem context will contribute to stakeholders' goals. That also implies that for one requirement, many contribution arguments may exist. Subsequently, a treatment to a requirement may satisfy several goals from one or more stakeholders.

With the above specification, an argument is made that predicts a contribution to this research project. More clearly, in the healthcare cybersecurity resilience problem, the main argument is that:

- If the treatment allows security engineers to develop by-design cyber resiliency for healthcare systems of HCCIs; and is usable for security engineers and useful for security practitioners in their incident response practice,
- assuming that the healthcare systems and infrastructures have the cyber, physical and human aspects as abstracted and analysed as in the proposed treatment; then
- the proposed treatment contributes to EPSRC 's goal of producing a holistic and not only technical security approach in the healthcare context.

This argument is fallible, as there is no deductive reasoning that can support its conclusion with certainty. Thus it forms a fallible hypothesis. The fallibility of this hypothesis lies in the fact that the design researcher may have abstracted and analysed the healthcare systems and infrastructures incorrectly by and the treatment may turn out not to be as usable and helpful as to security engineers as the initial search suggested that it is.

3.3 Available Treatments

In order to progress in regards to the RQ2, we need to consider the possibility that existing research treats the problem under investigation in a manner that satisfies the specified requirements. Hence, we need to enhance the current systematic review. This enhancement is essential because we want to find specific existing treatments related to the problem domain and the specified requirements for the treatment. To accommodate that, we set two objectives. Firstly, we analyse the existing set of papers to see if there is a need to conduct a new systematic review of existing treatments for the problem domain. Secondly, we need to analyse if they provide evidence that they satisfy to some degree the specified requirements. From there, we will be able to decide if a second review is needed. This time though, the focus will be on the specified requirements.

Table 3.1: Operationalisation of existing set of treatments

Treatment	Purpose	Operationalisation	Citation
Adaptation of Incident Command System (ICS) for use in cyber incident response	Small to medium health care organisations to plan and manage before an incident occurs having a Cyber Incident Response Team (CIRT)	Three scenarios	[66]
Autonomic security management (ASM) framework	Healthcare Information Systems (HIS) to anticipate, detect, respond to known and unknown attacks with minimum human intervention	N/A	[68]
System for modelling data flow within healthcare infrastructures and Visualisation process	Assists information security officers of healthcare organisations to improve their cybersecurity situational awareness	Three case studies	[70]
Machine Learning-based and time series anomaly detection prototypes	Incident detection for Electronic Medical Record (EMR) systems	Two prototypes test design	[73]
Framework of eight aggregated response strategies (EARS)	Response strategies that could be deployed by healthcare organisations	N/A	[61]
Conceptual architecture	Capture forensic artefacts of privilege misuse	N/A	[74]
Bayesian network model	Address cyber risks and minimise the effects of the power system outage	One scenario	[75]
Bow-tie cyber risk classification and assessment framework	Assess risks, visualise areas of concern and record the effectiveness of implementing control barriers	One case study	[76]
Effects-based discrete event stochastic simulation	Resilience quantification	One prototype test design	[77]

We already know, based on the results of the systematic review (cf. Section 2.3), that the multidisciplinary studies in cybersecurity, resiliency and healthcare are limited. From the sixteen (16) papers selected, nine (9) of them offer treatments, from which only six (6) have been validated and consequently might offer evidence for the satisfaction of the specified requirements for the treatment-to-be. Therefore, the analysis starts with these treatments. It is expected to either find that treatment exists and satisfies the specified requirements or to search further. If a further search is needed, the focus will change. The new search will be concentrating on this project's specified requirements instead of the overall problem domain.

3.3.1 Operationalisation using existing treatments set

To analyse the existing set of papers (cf. 2.3), we need to introduce the concept of *operationalisation*. Operationalisation stands for how properties of the requirements relate to pieces of evidence that they are part of a treatment. Achieving operationalisation is expected to vary, but the results are comparable as the focus is on shared requirements. Different types of requirements operationalise in different ways. In this project, the specified requirements are either functional and nonfunctional (cf. 3.1). For operationalisation, this creates certain expectations. For the functional requirement (*structured approach to developing by-design resilient operational security for healthcare systems of HCCIs*), specific tests might have been designed. On the other side, the nonfunctional requirements (*assist HCCIs and their security practitioners to be resilient to incidents and useful for incident response practice*) is expected to be operationalised with the definition of indicators as measurable variables.

Table 3.1 aggregates the treatments, the purpose of their design, and their operationalisation. Only six (6) of the papers operationalise by designing specific tests in suitable forms for the functional assessment of their proposed treatments. For the rest of them, i.e., the three (3) remaining, we use the N/A that stands for 'not applicable'. From the treatments that opera-

tionalise, test design is used, which means that the focus is on functional properties. Hence, the existing treatments give less emphasis on their nonfunctional properties. This remark indicates that we can assess only the first treatment requirement (*structured approach to developing by-design resilient operational security for healthcare systems of HCCIs*). For this project's other two nonfunctional requirements, we can infer a need to design a suitable treatment. For the functional requirement of this project, we will decide after assessing further the relevant papers.

3.3.1.1 "Incident Response Plan for a Small to Medium Sized Hospital" [66]

In 2013, C. DeVoe and S. S. M. Rahman in their paper entitled "Incident Response Plan for a Small to Medium Sized Hospital" [66] utilised the Incident Command System model used in emergency services to demonstrate that any sized organisations can have a sufficient cyber incident response team.

The **treatment** proposed in [66] is a redesign of a preexisting treatment from the fire and emergency services with a focus on safety. The approach intended stakeholders are Cyber Incident Response Teams (CIRTs) and not security engineers as in this project. The different type of stakeholders shows that their approach considered cybersecurity and response after the design of healthcare systems. The treatment requirement for by-design resilient operational cybersecurity needs a different type of treatment that will start from the early stages of a healthcare system's design. The of [66] is very useful. Nevertheless, it does not tackle the functional treatment requirement of this project. Something justifiable as their purpose was different, and naturally, the treatment proposed is appropriate for that.

In [66] the **purpose** is indeed to design responses before they occur. It mainly emphasises the limited capabilities of small and medium-sized healthcare organisations and how planning can be pivotal. In comparison with this project's functional requirement, it has a slightly different context as is concerned with IT-oriented cybersecurity instead of OT-oriented cybersecurity, which is the context of this research.

The **operationalisation** of this project's functional treatment requirement can use the three scenarios designed and investigated by DeVoe and Rahman [66]. These scenarios make apparent that the proposed treatment is holistic and well structured. It indeed takes place before an incident occurs, from the planning and preparation stages of incident response. The scenarios are narrated at a high level and focus on cyber attacks. They also provide technical details in the form of specific implementations that CIRTs can experiment and use. For the above reasons, we believe that this paper does not satisfy our functional treatment requirement, primarily because of its narrower cybersecurity focus, the different stakeholder and narrated high-level operationalisation.

3.3.1.2 "A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures" [70]

In 2017, A. Boddy, W. Hurst, M. Mackay, and A. E. Rhalibi, in their paper entitled "A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures" [70] propose a system that captures user behaviour through advanced data analytics and visualisation techniques and can detect any divergence. They tailored the proposed system to unique network configurations of healthcare infrastructures.

The **treatment** in [70] is a machine learning system. For data processing, this treatment also uses visualisation techniques. Therefore the focus of the treatment is on data. For this

project, this means that once more, the treatment is IT and not OT-oriented. So the context of the treatment proposed in [70] has a different context compared to the treatment requirement of this project. Additionally, the stakeholders of the treatment are security analysts. The treatment can be used to either increase its accuracy by providing feedback or use it to understand and explore healthcare data. Accordingly, the cornerstone of the treatment is the visualisation and analysis of data flows. These aspects of the treatment are suitable for the original design purpose. Though they differ from the treatment requirement of this project as its stakeholders are security engineers, and that being so, they need a broader cybersecurity treatment.

The treatment's **purpose** in [70] is to face functional challenges related to the increased quantity of healthcare data to support security analysts. Analysts improve the implementation of the treatment, which can be helpful for security practitioners. In particular for the improvement of an infrastructure's situational awareness. This purpose is part of a resilient treatment but is concerned only with preparing and detecting attacks at a data level. It does not address all healthcare systems, and it improves situational awareness but not the full spectrum of resilience. Because being aware of an attack does not imply its containment, eradication and data recovery.

For the **operationalisation** of there treatment, Boddy et al. [70] use three case studies. To conduct them, they use different data sets. These case studies demonstrate the functionality of the proposed system for data monitoring and analysis. However, by-design resilience is not covered. The above observations lead to the conclusion that context, stakeholders and case studies differ from those of this project. As a result, this is also not a suitable treatment for the functional requirement of this project.

3.3.1.3 "ML-based cyber incident detection for Electronic Medical Record (EMR) systems" [73]

In 2019, D. McGlade and S. Scott-Hayward in their paper entitled "ML-based cyber incident detection for Electronic Medical Record (EMR) systems" [73] propose the use of machine learning and time series for anomaly detection specifically of availability and confidentiality attacks on Electronic Medical Records systems.

The **treatment** suggested in [73] is for anomaly detection. Its focal point is detecting confidentiality and availability attacks against Electronic Medical Records (EMRs). Because of that, it has a different context of cybersecurity than the one that this project attempts to cover. Cybersecurity properties in IT can be different or been prioritised in another way for OT. On that account, the treatment of McGlade et al. does not address this project's treatment requirement without reservations. Another reason for such reservations is that in [73] the treatment is for detection, and therefore, it does not cover all the phases of resilience. However, resilience is part of this project's functional requirement.

The **purpose** of the design of the treatment suggested in [73] is to detect incidents against EMRs. EMRs are not the only healthcare systems within HCCIs. This remark shows another indication that the treatment of McGlade and Scott-Hayward has a different scope than the one required from this research. The treatment involved the design of a specific solution. Even though the stakeholders are not specified in [73], knowing that this project's stakeholders are security engineers and practitioners, we can infer an incompatibility. This incompatibility stems from the fact the security engineers design cybersecurity and along with security practitioners choose among alternative solutions for the most appropriate for their healthcare systems or infrastructures. For this reason, the need for a particular solution is not consistent with the need for a by-design approach for security engineers and practitioners.

The **operationalisation** indeed demonstrates the detection capabilities of the treatment, as described in [73]. It takes place in the design and testing of two prototypes, each corresponding to one cybersecurity property at a time. Nevertheless, in real-world cases, it is expected that attacks will be multiple, occurring in tandem and affecting more than one cybersecurity properties. Such cases are essential for security engineers and practitioners. However, for the detection solution, no relevant test was demonstrated. For all the reasons presented above, we infer that the treatment of McGlade and Scott-Hayward does not adequately address this project's functional requirement.

3.3.1.4 "Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem" [75]

In 2020, N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton in their paper entitled "Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem" [75] examine a range of causes and mitigation techniques for the smart grid in an attempt to assess the overall cyber resilience of a system using a Bayesian network approach.

The **treatment** proposed in [75] is for the minimisation of cyber risks. Its focal point is detecting cyber risks of electric power systems, which are part of healthcare infrastructure. Because of that, it has a narrower context of cybersecurity than the one that this project attempts to cover. Moreover, Hossein et al. treatment does not address the full healthcare context and aims more on risk management as a preparation and lessons learned. Hence, their treatment does not cover all the phases of resilience. However, resilience is part of our project's functional requirement.

In [75] the **purpose** is to address cyber risks and minimise their effects. However, the scope is narrow and focuses on power systems. In comparison with this project's functional requirement, it has a slightly different context as it is concerned with IT-oriented cybersecurity (instead of OT-oriented cybersecurity). Specifically, it looks at three types of vulnerability (software, access and network). Furthermore, it does not focus on the healthcare domain but rather specific systems also used in healthcare.

The **operationalisation** in this case happens through specialised software that quantifies the variables and simulates the model. The quantification uses experts knowledge, statistical learning, historical data, and probabilistic estimations. It produces a set of assumptions about the system's nodes that can be useful for the planning and improvement of a resilience plan specific to a smart grid. This operationalisation covers technical aspects of a system, and even though it depends on human knowledge and decisions, it does not cover the social aspects of a smart grid.

3.3.1.5 "A quantitative bow-tie cyber risk classification and assessment framework" [76]

In 2021, B. Sheehan, F. Murphy, A. N. Kia, and R. Kiely, in their paper entitled "A quantitative bow-tie cyber risk classification and assessment framework" [76] propose a conceptual risk assessment framework that combines a bow-tie model with a risk matrix, designed to show cyber weaknesses and indicate proactive and reactive cyber defences.

The **treatment** suggested in [76] is for risk classification. Sheehan et al. propose a conceptual cyber risk classification and assessment framework designed to demonstrate the significance of proactive and reactive controls. Their treatment combines a bow-tie model with a risk

matrix to produce a cyber threat rating based on the likelihood of occurring and the potential severity of the resulting consequences. Their treatment is more related to preparation and post-incident activities. Thus, they do not address all phases of incident response, which is the scope of this research project.

The **purpose** of the design of the treatment suggested in [76] is to reduce organisational exposure to cyber risk and quantify the risk. Sheehan et al. associate this purpose with insurers. Insurance is one way to treat risk by transferring it to another party. However, from the treatment requirements of this project, more options need to be available to a decision-maker, such as avoidance, retention, sharing, transferring, and loss prevention and reduction. Hence, our purpose is broader.

The **operationalisation** of the cyber risk classification framework proposed in [76] uses a case study based on interviews and brainstorming sessions. Sheehan et al. recognise that their current do not incorporate uncertainty and residual estimation methods. The above shows that the context, stakeholders and case study differ from those of this project, and there are areas that their proposed framework can evolve to cover more aspects of resilience.

3.3.1.6 "Towards an organizationally-relevant quantification of cyber resilience" [77]

In 2021, T. Llansó and M. McNeil in their paper entitled "Towards an organizationally-relevant quantification of cyber resilience" [77] propose the Resilience Index (RI), a quantification metric of cyber resilience based on discrete event stochastic simulation over a mission timeline.

The **treatment** proposed in [77] is a simulator that computes the resilience index for target systems. Llansó et al. use similar definitions of resilience and recognise the lack of maturity to quantify resiliency in cybersecurity. Their treatment focuses on maintaining the mission's essential functions (MEFs) and consists of a model and a method as artefacts. More specifically, they use an effects-based discrete-event stochastic simulation that includes random variables. Nevertheless, they do not focus on the by design resilient operational security, but rather on preparation and resilience concerning the approaches of redundancy and deception. Their treatment is expandable, but currently, it does not cover the scope of this research project and is not specific to healthcare domain challenges.

The **purpose** of the design of the treatment recommended in [77] is to measure of overall resilience of a cyber system as it relates to the continuation of missions. In other words, Llansó et al. associate cyber resilience with mission resilience. However, their purpose concerns IT systems in general and not healthcare systems, leaving outside Operational Technology (OT) aspects that this research project is concerned with.

The **operationalisation** of the model and method proposed in [77] uses a prototype test design. Llansó et al. identify that the stage of their research simulates malicious impact and attacker behaviour that needs to be updated based on more current data. Additionally, as they designed a model, they are aware that the simulator simplifies a target system; consequently, other models can also represent the same system and its resilience. Their treatment is not fully automated, depends on the user's input and has not been properly validated.

Accordingly, taking into consideration the above, we understand that no treatment exists in our initial set of papers that addresses the two nonfunctional requirements. As for the functional requirement, six treatments address specific aspects of it. Even in these cases, the aspects addressed are only to some degree, satisfied. Thus overall, we can claim the need for further investigation for the treatment of this project's functional requirement. In other words, the treatment-to-be of this research needs to meet all the requirements as specified in

section 3.1, as not existing treatment addresses them all.

3.3.2 Search of healthcare cybersecurity reviews

The analysis of the existing set of papers did not find a treatment that answers the RQ2. As a result, this research needs to conduct a second systematic review. This second review is taking place in an attempt to identify treatments that satisfy, to some degree, the treatment requirements as specified at the beginning of this section 3.1. Unavoidably the treatments to be collected are expected to have a broader scope as they have not been found appropriate treatments in the first systematic review that covered cybersecurity, healthcare and resiliency.

The goal of this second systematic review is to collect treatments designed in earlier studies. These treatments need to satisfy, to some degree, at least one of this project's treatment requirements. As mentioned in the first review, this research activity is exceptionally requiring and time-consuming. We nevertheless decided to undertake this activity because its expected output can allow the formation of "working hypotheses". These hypotheses can be then tested on actual cases to identify if a redesign will be an appropriate approach or if the design of an approach from scratch is required.

To search for treatments that could satisfy this project's requirements, we started from existing systematic reviews to ensure that a survey is needed. From early on, we found that the majority of reviews are focused on the security of cyber-physical systems [82, 83, 84]. Some of them are specialised in existing treatments and concepts [85, 86].

Nguyen, Ali and Yue reviewed model-based engineering approaches used to address security concerns [85]. The majority of these approaches analyse one or more security challenges; however, less similar work is conducted that concerns or also includes possible solutions [85]. They also found that for the model's design are used either Domain-Specific Languages (DSLs) or Unified Modelling Language (UML) notation [85]. In regards to the Security Development Lifecycle (SDL) most approaches start to focus on requirements and design, and few works connect them with implementation [85]. The majority of treatments designed methods, tools and metrics in descending order [85]. Similarly, these treatments relate mainly to threats or attacks, then to vulnerabilities and fewer to security solutions [85]. They also found that most of the current body of knowledge uses academic case studies for smart grids [85].

Gunes et al. survey the different definitions of Cyber-Physical Systems (CPSs); their main concepts and domains [86]. They refer to healthcare along with medicine where issues of reliability rise and are of particular importance as they can affect multiple aspects of a patient's physiology [86]. Relevant is their work to this project's requirement for a structured approach to developing by-design resilient operational security because this type of security is closely related to cyber-physical systems security. For healthcare systems, in the cybersecurity literature, we also meet them as Medical Cyber-Physical Systems (MCPSs). This has been shown in relevant reviews [87, 88, 89].

Haque, Aziz and Rahman introduce a taxonomy for MCPSs [87]. For security, the taxonomy focuses on data and address privacy and encryption issues at different levels (i.e., application, data, user and network levels) [87]. Also Haque, Aziz and Rahman map existing MCPS application and there they include a security-related treatment (i.e., CYPsec [90])[87]. Dey et al. addresses the physical aspect of MCPSs and acknowledge the security issues that emerge [88]. The lack of inclusion of the physical aspect of security coincides with the review findings of Jalali et al. [54]. Dey et al. further connect their security concerns with reliability and safety challenges [88]. They emphasise the absence of a suitable analysis approach where

the complexity and interdependence of MCPSs and their operational context can be depicted and studied [88]. They stress that any potential treatment will need to start from the very development and architecture of MCPSs [88].

Gatouillat et al. review to what they refer as the Internet of Medical Things (IoMT) [89]. Similarly to Dey et al. [88] Gatouillat et al. stress the importance of reliability, safety and security [89]. Thought-provoking is that they extend reliability beyond containment to reactive response, a concept well known in cybersecurity (e.g., Moving Target Defence (MTD), self-organising systems and Byzantine faults) [89]. Because Internet of Medical Things (IoMT) focuses on the networking aspect of MCPSs papers that consider application challenges are reviewed [89]. Gatouillat et al. found that models for the study of biological processes, computing systems and hybrid systems do exist [89]. However, these models are different from those examining the concepts of robustness and security [89]. Another observation that they make is that in the current body of knowledge, there is a lack of studies related to the service layer of IoMT [89]. At the same time, most of the current research focuses on medical devices and the integration layer [89].

Reviews also exist for security treatments in the healthcare context [91, 92]. Fernandez - Aleman et al. report on EMRs security and privacy [91]. They found that most of the articles reviewed propose specific treatments [91]. Noticeably, some of them indicate that there might be a need to override security and privacy policies in cases of emergency [91]. Surprisingly, not all of the appropriate treatments for EMRs address the generation of evidence [91]. This omission can hinder post-incident reviews and improvement activities. Ma et al. [92] approach healthcare security from another point of view, that of medical devices. They particularly evaluate the security and privacy of medical imaging devices [92]. Their review focuses on vulnerabilities and possible attacks and contrasts them with the protection offered from security mechanisms [92]. There is also a survey that addresses healthcare CPS security at a higher level [93]. Rehman et al. identify security challenges, requirements and analyse existing authentication treatments [93].

Overall, the technologies used in healthcare infrastructures differ significantly. This diversification is a common theme that connects the reviews presented above. There is also a review that lists these different technologies used in healthcare [94]. They range from wearable devices and smartphones to cloud applications, big data, Internet of Medical Things (IoMT) and Medical Cyber-Physical System (MCPS) [94]. Another important remark is that cybersecurity resilience and healthcare has not been a common review interest. Although, there exists a review concerning the resilience of CPSs in general [85].

3.3.3 Search for cybersecurity resilience treatments

In this research, the centre of attention has the concept of cybersecurity resilience. It seems that it has not been studied excessively within the healthcare context. The systematic review that follows has a broader scope of searching for cybersecurity resilience treatments. We present an overview of the search strategy in Fig. 3.1. This strategy and the reasons for which we conducted it coincide with those used in the previous systematic review (cf. Section 2.2.2).

We conducted an *automated search* using electronic resources to search for relevant papers. For consistency, we used the same digital libraries as before (i.e., the IEEE Digital Library (IEEE Xplore), the ACM Digital Library, the ScienceDirect (Elsevier), the Scopus and the Web of Science). At first, we evaluated each paper for inclusion in the set of relevant papers based on the title, abstract and inclusion/exclusion criteria that remained the same with the previous review (cf. Section 2.2.4). We were inclined to include the papers at this stage unless they

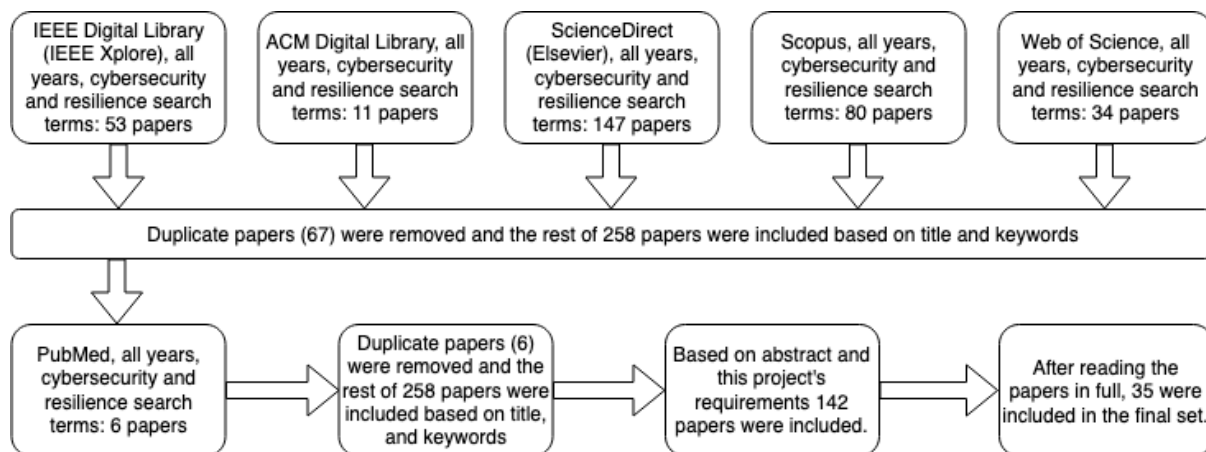


Figure 3.1: Selection process stages of second systematic review.

were irrelevant to cybersecurity and resilience. The three hundred twenty-five (325) papers identified from the different sources spread as follows:

- IEEE Digital Library (IEEE Xplore): 53 papers.
- ACM Digital Library: 11 papers.
- ScienceDirect (Elsevier): 147 papers.
- Scopus: 80 papers.
- Web of Science: 34 papers.

After removing sixty-seven (67) duplicates to examine a health-oriented digital library, we researched the PubMed database that focuses on life sciences and biomedical topics with the same criteria. That search resulted in the extraction of six (6) additional papers and overall of two hundred sixty-four (264) papers having removed six (6) duplicates, two hundred fifty-eight (258) papers were included based on the title and keywords. All these papers were further processed based on their abstracts, resulting in a set of one hundred forty-two (142) resources. We judged these resources based on this project's requirements. After reading the full papers and assessing their quality following the same criteria as in the previous review (cf. Section 2.2.5), we extracted thirty-five (35) papers. Regarding the quality of resources, once more, we followed the same assessment as in the previous review (cf. Section 2.2.5), and no exclusion of an article collected in the review process occurred due to nonconformity to the established quality criteria.

3.3.4 Data extraction and synthesis

Here we could make any decisions for data extraction and synthesis, we had to consider an essential observation. The second systematic review made apparent that once the context is broader than in the first review, the central concepts of this research (i.e., cybersecurity, resilience and healthcare) become more abstract. The second review resulted in a collection of cybersecurity resilience studies that cover the different areas of *operational resilience* as approached in the CERT® Resilience Management Model (CERT-RMM) [95]. CERT-RMM is a management framework designed by the CERT Division at Carnegie Mellon University's Software Engineering Institute, and it has been used broadly from infrastructures. This framework

centres around the security and survivability of assets to ensure the success of operational missions in the face of disruptions. Consequently, it covers many operational aspects (e.g., risk management, information security, supply-chain continuity, crisis management, workforce continuity, IT disaster recovery, emergency management and crisis communications) as well as a plurality of disruptions (e.g., natural, artificial, accidental, intentional, small, large, information technology-related, cyber and kinetic) [95].

This scope, however, is much broader compared to this project's scope. Nevertheless, it gave us a base for selecting relevant to this project's context studies. To be able to do this, the need for clear definitions of the terms became necessary. These terms could form clear boundaries for the problem domain and the selection of relevant papers. It seemed that resilience was used interchangeably with sustainability and robustness, something which has been observed from other studies too [96, 97]. In their work, they analyse these concepts within the context of *evolvability* [96]. Evolvability is an integral aspect of CERT-RMM too [95]. However, Urken et al. define *evolvability* in the context of systems engineering. They suggest that it is a necessity to design, test, redesign and brake systems. Now, this engineering evolvability is understandable and seems to coincide with cybersecurity and software engineering lifecycles. However, in healthcare, systems' evolutions will need to take place without causing harmful impacts.

Before examining the evolving engineering within the healthcare context, we need to distinguish between the terms resilience, robustness and sustainability. The World Economic Forum defined *resilience* for cybersecurity as "*the ability to continuously deliver the intended outcome despite adverse cyber events.*" [98, ?]. Björck et al. analysed this definition and found that it has four main variable components, namely: (i) 'Ability' is a part of the resilience definition that can have different layers of analysis (e.g., international, national, local, infrastructure, functional) [99]. This aspect coincides with the top-down and bottom-up approaches found in the first systematic review (cf. Section 2.3.2). (ii) 'Continuation' is the second part of a resilience definition and relates to the ability to change, adapt, or recover [99]. (iii) The 'intended outcomes' is the third component of a resilience definition. The intended outcomes can vary based on goals, processes or services that need to be maintained [99]. (iv) The 'adverse cyber event' is the fourth component of the resilience definition. It stands for one or more circumstances steaming from different sources (e.g., natural, cyber or human occurrences) [99]. The analysis of Björck et al. confirms that variations will characterise cybersecurity resilience studies because this variety stems from how each research project frames each of the components of the resilience definition.

This variety can be demonstrated using landmark research papers on cyber resilience. Urken et al. perceive the resilience of a system engineered as its destabilisation beyond its adaptation limits [96]. Looking back at the components of a resilience definition as indicated by Björck et al. [99] in Urken et al. [96] it takes the following form: Resilience analysis takes place at a system's level ('ability'). It is interpreted as a way that a system is safe to fail ('continuation'). It does so by maintaining a systems standard functionality and operating predictably ('intended outcomes'). These outcomes can be achieved when one or more destabilisations occur beyond a system's adaptation limits ('adverse cyber event'). This definition implies that in contrast with the cybersecurity intention to allow systems to fail-safe, cyber resilience addresses the need for a system to be engineered in a way that it is safe to fail [99].

The Department of Homeland Security has given another (extended) definition of resilience [100, p. 26]. Based on the resilience components by Björck et al. [99] it takes the following form: Resilience is analysed at a system, infrastructure, government, business, community, and individual level ('ability'). It does so by resisting, tolerating, absorbing, recovering from, preparing for, or adapting ('continuation'). It aims to reduce the consequences associated with an

incident, event, or occurrence. Resilience also impacts the likelihood and deters an incident, event, or occurrence from happening ('intended outcomes'). These outcomes can be achieved in the presence of an adverse occurrence that causes harm, destruction, or loss ('adverse cyber event'). This interpretation of resilience offers a broader definition compared to Urken et al. [96].

Additionally, Woods [97] characteristically demonstrate the wide variability of resilience definitions by providing four different ways to interpret it [97]. The variants in the resilience definition that Woods focuses on relate to the 'continuation' component. According to Woods, this component can be associated with a rebound, robustness, 'graceful extensibility' of performance or adaptation capacity and sustained networking adaptability [97].

The variabilities in the definition of the 'continuation' component show that the term 'robustness' can be used interchangeably with 'resilience'. However, Urken et al. differentiate it and consider it to refer instead to systems engineered to fail-safe, responding to internal or external disturbing occurrences [96]. Interpreted in this context of evolving engineering, robustness aims to maintain a system's normal functionality [96]. Alternatively, this means that robustness is related to occurrences that can be well-modelled and consequently belong to a well-defined set of adverse events [97]. If an occurrence is outside this set, the system will not evolve in a way that yields the intended outcomes. This note will imply that the system cannot be robust and restore its state. In these cases, a resilient system will then attempt to enable graceful degradation to minimise harm and continue to operate in some form that allows system recuperation [96].

To perplex the terms resilience and robustness from an evolving engineering perspective can be disturbingly erroneous. A poorly modelled set of occurrences activating adaptive system responses can create the expectation of increased system robustness. However, formal and theoretical research [101], as well as empirical analysis [102], have shown that this is not the case. Instead, expanding a system's ability to handle some additional occurrences increases the system's vulnerability in different ways or other occurrences.

To that, another term that can confuse is that of *sustainability*. Sustainable systems are engineered to have resources that will allow them to continue to operate predictably. It can be associated with reliability [96]. However, in contrast, resilience is not necessarily reliable as it offers knowledge via trial and error. Overall, resilience seems to be an overarching term that covers the areas where robustness and sustainability meet. In this way, an evolving system can be engineered by restructuring normal and abnormal systemic adaptive capabilities. Due to the broad coverage of the term resilience, before we can review the existence of treatments that satisfy this project's requirements, it is essential to define resilience for this project context.

To define resilience for this research is necessary to design an artefact based on the treatment requirements. We need to define all the variable components of resilience [99], in particular for this project (i.e., ability, continuation, intended outcome and adverse cyber events). To do so, in the following paragraphs, we document our decisions for each component separately. Finally, we present this project's definition of resilience.

We start with the 'ability' of resilience. The main stakeholders of this project are security engineers. In the TR1 (cf. Section 3.1) the development of by-design resilient operational security for healthcare systems is stated. In this respect, engineers need to be able to analyse resilience at a security level. This security is also part of HCCIs, according to TR1. Hence, security engineers need to design resilience for systems' security within the healthcare domain and, in particular, a critical infrastructure. What they want to be able to engineer is the resilience of these systems' security within a HCCI because heterogeneous stakeholders affect the design of these systems, what security engineers will be interested in how to manage the resilience

of these systems' security, which means the people, processes, and technology necessary to manage resilience.

To make security resilience cost-effective, we suggest that it follows the security-by-design paradigm. When it comes to 'continuation', TR2 (cf. 3.1) states that security engineers can use the treatment to design resilience, which means that security engineers need to support different forms of how they will design security continuation. Consequently, in their security resilience designs, they want to maintain a set of security constraints and sustain or at least not impact a critical healthcare service negatively if an incident does occur. For that, they need to address the impact of an incident on security and healthcare services to apply appropriate responses and return the infrastructure to a state of normal operations.

Security engineers and practitioners aim to reduce the consequences associated with an incident. They want to prevent the consequences of an incident from happening. Hence, security practitioners can use models of resilience-by-design for their systems to select and implement, appropriate to the situation, incident response practice. This aspect of the resilience definition for this project coincides with TR3 (cf. 3.1).

The 'adverse cyber events' that security resilience focuses on are named *incidents*. An incident stands for a negative occurrence that happens or is thought of as happening and leads to the failure of security constraints maintenance. This definition is similar to NIST SP.800-61r2 [4], but it has quite a subtle difference. It does not only allow an incident to be something that happened in the real world, but also it allows an incident to be imaginary and not occur in reality. The example of a hypothesised false positive alarm of an intrusion detection system can be treated as an incident even though it did not occur. The second meaning describes incidents that occur in computer systems. In this way, the term incident has two incidents: threat or an actual attack.

Based on the resilience definition components by Björck et al. [99] the definition of resilience for this research takes the following form: *Resilience is analysed at a healthcare cybersecurity context level ('ability'). Resilience is achieved in the presence of an incident as an adverse occurrence that happens or is thought of as happening and leads to the failure of maintenance of at least one security constraint ('adverse cyber event').* It does so by preparing, identifying, containing, eradicating, recovering and learning ('continuation'). It aims to reduce the consequences associated with an incident. Resilience also impacts the likelihood and deters an incident from happening ('intended outcomes').

Returning to the data extraction and synthesis of the collected papers, those papers that met the inclusion criteria (cf. Section 2.2.4) were further reviewed, and we selected from the relevant papers those proposing a treatment design. We grouped these papers into sets of studies addressing their analysis level (e.g., at a design level or real-time). Moreover, we looked at their treatment artefact/s, validation/evaluation method, and resilience definition components as defined by Björck et al. [99]. After the initial aggregation, we looked for design challenges that future research needs to address. We integrated the results from our synthesis with the suggestions we found in the individual papers. These suggestions were then used to specify areas where re-design could enhance these treatments.

3.3.5 Search limitations

This search is based on digital source and papers that the University of Brighton has access to. Since we conducted an automated search, we faced restrictions from the general indexing systems that supported such analysis. Regarding personal bias, we understand that there will

be instances where we will not be able to identify personal bias by ourselves. Nevertheless, we extracted resources and used predefined criteria to assess the inclusion or exclusion of the resources, tending towards inclusion in cases of doubt. Additionally, as we conducted a systematic review, the set of collected papers represents the knowledge available at a certain point in time. If and when more primary studies become available, a later extended systematic review may well be able to refine and revise the original findings.

Moreover, we restricted our automated search to papers that combined a set of terms from two domains that for each one, independent research exists that offers insight in great depth (cybersecurity and resilience). Consequently, there might be papers that we have missed, and we could find them with a broader search. The reason for our restriction was beyond time and resources in general, related to the focus of this research itself. We wanted to avoid collecting papers with a broader scope, meaning outside the intersection of the two domains, as this commonly causes the collection of less relevant information and complicates the aggregation process.

3.4 Systematic Review Results

This section discusses each of the treatment papers selected as relevant to the treatment requirements of this research. There were 35 resources selected. A first observation was that cybersecurity and resilience were initially not studied together. Instead, resilience was related to safety. As a result, treatments that consider cybersecurity with resiliency spread between 2009 and 2020. A second observation is that the publication venues were diverse. This variation may stem from the relative newness of the domain and the absence of focused venues and publications.

From the selected treatments, resilience was considered either as part of the whole development life cycle or from the design stage (by-design) or at run-time as adverse cyber events occur. The proposed treatments resulted in artefacts, mainly frameworks (methodologies, approaches) and models (conceptual, operational). Standard evaluation methods for the proposed treatments were case studies, examples, simulations and experiments.

Regarding the definition of resilience, 'ability' mainly refers to a systems-level, either only cyber or cyber-physical. Another type of resilience 'ability' involved physical, informational, social and cognitive aspects. The treatments associated resilience 'continuation' with the Observe–Orient–Decide–Act (OODA) loop. Alternatively, 'continuation' was specifically referring to a cybersecurity approach, such as self-healing configurations, Moving Target Defence (MTD), evaluation/situational awareness, monitoring and control. The 'intended outcomes' of resilience were mostly associated with goals, missions, functions, products and services prioritised as critical. Some other cases were about the assessment of resilience practices and their effectiveness. Resilience associated with various 'adverse cyber events'. These events were not only cyber attacks but also other anomalous conditions. Such conditions were safety hazards, unknown threats, natural and human events, any cause that is essential for anything critical, and security breaches and behavioural anomalies.

Overall it can be observed that more considerable ambiguity exists in what is an 'adverse cyber event' within the intersections of cybersecurity and resilience. A similar complication exists in the 'continuation' of resilience. The existing frameworks use a great variety of words that are defined slightly differently. Possibly it can be claimed that the Observe–Orient–Decide–Act (OODA) loop covers the wordiness along with specific cybersecurity approaches used for continuation (e.g., self-healing, MTD). Apropos of 'ability', the majority of treatments focus on a

system level. This system contains various components, such as cyber, physical and social. Lastly, the 'intended outcomes' seem to relate to the broader environment where the system operates and its associated critical objectives and operations.

Based on the above observations, we can return to this project's resilience definition (before the last paragraph of section 3.3.4). From there, it becomes apparent that:

- None of the treatments addresses the resilience 'ability' as related to the healthcare context and its security;
- Most of the treatments refer to the resilience 'continuation' covering the phases of NIST SP 800-62r2, but usually integrate them in fewer steps, closer related to the OODA loop;
- Most of the treatments are goal, mission, or function-oriented. In other words, their 'intended outcomes' depend on what is critical for the case under study. However, only those treatments that look at resilience assessment are concerned with the reduction of the consequences associated with an incident;
- Most of the treatments consider as 'adverse cyber event' cyber attacks. Though they do not clearly distinguish an adverse occurrence that happens (attack) or is thought of as happening (threat). Also, only one treatment considers as such events any security violation.

For these reasons, we conclude that a treatment that will cover the resilience definition used in this research project, contributing to stakeholders' goals, is necessary. Hence, the operationalisation of the above treatments cannot occur, and it is time to move on to the design of a new treatment that corresponds to this project's resilience definition.

3.5 Discussion and Closing Remarks

From the literature review, cyber resiliency seems to lack a precise definition shared among different researchers. Nevertheless, in contrast to cybersecurity, cyber resiliency is not about failing safe, but it looks into how to safely engineer systems' failures (known and unknown). In this context, safety relates to the risk of physical harm and the likelihood to occur. Safety-related consequences can have cybersecurity-related causes. Cyber resiliency capability will support the reduction of the frequency and impact of such occurrences. The literature suggests adaptability and continuation capabilities to attain these goals that incorporate risk management, incident response, and post-incident activities (also called lessons learned). However, these two terms have different meanings as they relate to different types of events. The engineering of adaptable cyber resiliency means that the events are known and expected. There predictability yields sustainability. In contrast to engineer cyber resiliency continuation, the events that occur are unexpected and unknown when systems design occurs. Any configuration, though, either to attain adaptability, sustainability or continuation, changes the system in a way that can lead to further exposure to threats and attacks.

From the above, it becomes apparent that a conceptual representation of the cyber resiliency domain will be helpful for researchers and practitioners. Its creation will be valuable for a shared understanding. It will also clarify how the different terms relate to each other, and all of them can support by-design cyber-resilient systems. The ability to design such systems, such as medical devices and building equipment, seems to be especially crucial for safety-critical infrastructures, like those that constitute a nation's healthcare sector. In the following

chapter, we further explore the need for a conceptual framework and how to design it as part of a treatment that will meet these project's stakeholders' requirements.

Table 3.2: Aggregation of treatments by publication year

Citation	Level	Artifact	Eval./Val. method	Ability	Continuation	Intended Outcomes	Adverse cyber event	Challenges
[103]	life cycle	operational framework for resilience	examples	critical systems and their key functions	resistance, absorption, restoration	missions, resilience objectives	nature, deliberate	translate concepts into operational means
[104]	by-design	framework for managing engineering change propagation	case study	components and attributes of a product/service	continuation of performance and completeness, observe, orient, decide, act	identify all the components/dependencies affected	industry-specific change	merge risk and impact factors into a model
[105]	run-time	extension of the INTERSECTION framework, OODA loop process testbed	N/A	systems of systems		security re-engineering	attacks, threats, misuse	more research in design and act technologies
[8]	life cycle	cyber resiliency engineering framework	N/A	organisation, mission, process, task, resource	anticipate, withstand, recover and evolve	mission assurance, resiliency goals, objectives, practices, and costs	cyber threats	motivate field evolution
[106]	development	conceptual framework	N/A	national (India) critical information infrastructure	corrective and preventive	national cybersecurity goals	IT attacks	financial and implementational
[107]	life cycle	cyber resilience engineering framework (CREF)	N/A	system, set of shared services, or common infrastructure	selecting, tailoring, and implementing security controls	support cyber resiliency	Advanced Persistent Threats (APTs)	lower-level selection of security controls
[108]	life cycle	approach to develop resilient dynamic data driven application systems	three experiments	cloud applications	encryption, replication, diversity, automated checkpointing and recovery	increase the difficulty for attackers to figure out the execution environment and exploit its vulnerabilities	cyber attacks	need for resilient cloud techniques
[109]	life cycle	resilience metrics	N/A	cyber system (physical, information, cognitive, social)	plan/prepare, absorb, recover, adapt	national policy goals linked to system measures	cyber attacks	assessment of heterogeneous interdependent networks
[110]	life-cycle	cyber resiliency engineering framework	N/A	components, technology, and process	anticipate, withstand, recover, evolve	assessment, missions, business processes, resiliency objectives	cyber threats	extend to accommodate new approaches
[111]	life cycle	model for simulating restoration	case study	bulk power system	absorb, adapt	resilience quantification and/or recover	large-scale disruptions that system's exceed criteria	evaluation and implementation
[112]	life cycle	network-based quantitative framework	simulations, quantitative evaluation	large-scale infrastructure	recover, robustness networks	hazard responses, recovery strategies	disruptive events	approximation of optimal recovery strategy

Citation	Level	Artefact	Eval./Val. method	Ability	Continuation	Intended Outcomes	Adverse cyber event	Challenges
[113]	preparation	threat response framework	N/A	organisation	response	security goals for incident management	cyber attacks (incident)	unity within a security programme
[114]	life cycle	systems engineering framework	notional example	cyberphysical system	management	risk assessment	cyber persistent, dynamic threats	measures to ensure resilience is built into the framework
[115]	preparation	infrastructure resilience-oriented modelling language	case study	infrastructure	withstand and recover	goals and operational dependencies	off-nominal (anomalous) conditions	accident analysis, tool support
[116]	life cycle	cyber resilience framework	case example	system, organisation, mission, or business process	anticipate, withstand, recover from, and adapt	situational awareness and events absorption	adversary conditions, stresses, or cyber attacks	more research in cyber resilience
[117]	by-design	modelling resiliency approach	scenarios	cyberphysical system	recovery	desired system state	safety hazards and security threats	safety/security simulations
[118]	life cycle	Cisco cyber resilience framework	N/A	enterprise architecture	identification, protection, detection, recovery, visibility, analytics, forensics	cyber resilience goals	cyber attacks	implementation, experience, commitment
[119]	after	cyber resilience assessment framework	example	physical, information, cognitive, social	plan and prepare, detect, absorb, recover from, adapt to	measurement of cyber resilience practices	cyber risk	collection and shearing of relevant data
[120]	by-design	system design approach	example	cyber system	configuration	goals	adversarial activity	relaxation of assumptions
[121]	life cycle	cyber resilience recovery model	simulation	incident response	configuration	predict resilience effectiveness	zero-day malware	application to complex scenarios
[122]	life cycle	cyber resilient strategy	N/A	enterprise architecture	continuation	achievement of organisational purpose	known/unknown attacks and threats	rethink organisational strategy
[123]	by-design	conceptual resilience governance framework for eHealth CPSs	N/A	cyberphysical system	adaptation	goals/objectives	natural, cyber, human	best practices of effective cyber-security solutions
[124]	by-design	cyber attacks modelling and simulating approach	use case	cyberphysical system	quantitative evaluation	compromise simulation	cyber attacks	implementation

Citation	Level	Artefact	Eval./Val. method	Ability	Continuation	Intended Outcomes	Adverse cyber event	Challenges
[125]	by-design	agile and resilient embedded systems (ARES) methodology and metric set	benchmark and flight tests	embedded cyberphysical systems	mitigation of threats that security cannot alleviate	mission assurance	any cause of loss of mission essential functions	further refinement, validation, application and automation
[126]	run-time	self-healing cyber resilient framework	simulation	network	self-healing	automated management	cyber attacks	extent to specific network types
[127]	by-design	SecUre and REsilient Cyber-Physical Systems (SURE) platform	three case studies	cyberphysical system	monitoring, control	resilience evaluation	cyber attacks	empirical research
[128]	life cycle	business continuity and disaster recovery planning (IBCDRP) model	case study	organisation (critical functions, resources)	continuity, resumption, restoration	evaluation of strategic and tactical decisions	natural and man-made hazards (simultaneous and sequential)	management of interdependent events
[129]	run-time	framework for resilient mission critical systems	tests	stateful applications	moving target defence, availability	mission survivability	anomalies	distinguish and analyse anomalies at run-time
[130]	by-design	manufacturing testbed, cybersecurity-resilience ontology and framework	N/A	system	return to nominal performance after an acceptable period, restoration	maintain the system in its required state of security	security breach	interoperability of cyber manufacturing environment
[131]	run-time	method for modelling the impact of cyber attacks	examples and experiments	network	threat assessment, justification of requirements	assess cyber resilience	cyber attacks	concurrent and unknown attacks
[132]	run-time	modelling and assessment approach	case study	Bayesian network	absorption, adaptation, restoration	risk assessment	diverge range of risks (natural, cyber, human)	improve accuracy
[133]	run-time	architecture for resilience enhancement	case study	physical, network, and application	reliability and operational normalcy	disturbances, including attacks	vulnerabilities and potential physical and cyber attacks	implementation difficulty
[134]	run-time	dynamic medical risk assessment model	case study	Bayesian network	safety measures assignment and adaptation	risk assessment	failures, repairs, and human errors	model healthcare complexity
[135]	life cycle	methodology for quantifying and mapping resilience	interviews, literature review, case study	physical, information, cognitive, social	plan, absorb, adapt	assess organisational resilience (missions, capabilities)	uncertain future events	limited ability to incorporate novel, resilience strategies
[136]	preparation	framework of cyber resilient behaviour	survey and pilot study	human behaviour	anticipate, monitor, respond, and learn	organisational needs related to human aspect of cyber resilience	cyber attacks	link behaviour change interventions to resilient behaviour of employees

Chapter 4

Cybersecurity Resiliency Domain Model

This chapter aims to introduce Build-In Resiliency Analysis (BINAs). BINA offers a syntactic and semantic reference for the comparison of security-oriented modelling languages and for resiliency-oriented modelling languages. Furthermore, BINA helps to unify the terminology used from different cyber resiliency engineering approaches. Consequently, it will help create a shared understanding of the cyber resiliency domain. For example, KAOS [137] needs to agree cyber resiliency engineering descriptions. It can use our domain model as the artefact for finding and agreeing the concepts of cyber resiliency and their meanings. Finally, the introduction of a model to present the constructs of cyber resiliency engineering will enhance the documentation generated, during and after incidents, and will help to capture the various constructs.

Section 4.1 shows the research approach used to set BINA. Section 4.2 summarises the different resources relevant to this interpretation. Section 4.3 shows the construct association; then Section 4.4 establishes and discusses BINA. The chapter closes with Section 4.6 presenting conclusions and limitations of the domain model.

4.1 Research approach

In order to follow a structured way of designing the domain model, we followed the research approach suggested by Dubois et al. [138] shown in Fig. 4.1. We modified this research approach to reflect the domain-related characteristics. With our project-specific adjustments, the research approach consisted of the two first steps as presented in [138]:

1. *Concept alignment*: identified the central concepts from the literature as well as the relations between them. Here the literature needed to be relevant to BINA. After the concepts and relations were collected, we joined them semantically to integrate the existing vocabulary. By their semantical integration, we analysed all of the selected works and in an identical way. This step led to the creation of two artefacts:
 - (a) A table that set out the concepts collated from the different approaches. It also showed the type of semantic relationships that indicated a form of similarity, such as synonymy (cf. Section 4.3);

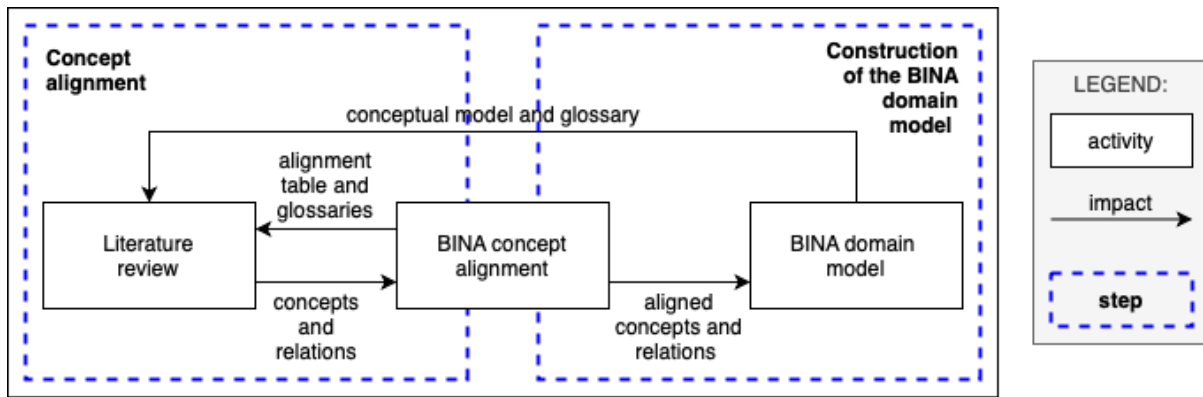


Figure 4.1: The research approach used for the design of the BINA domain model.

- (b) The terms' meanings, as defined in their primary sources. These meanings were presented in the form of a table that included the glossaries of different approaches (cf. Appendix B).

The concept alignment was not a linear process, but an iterative and progressive one. Every enhancement of the table supports a better understanding of the concepts' semantics in the existing literature. This literature (cf. Section 4.2) stems from four main types of resources:

- Cyber resiliency standards (cf. Section A.0.1),
- Cybersecurity-related standards (cf. Section A.0.2),
- Health-related standards (cf. Section A.0.3),
- Cyber resiliency frameworks (cf. Section 4.3.2),

Modelling languages covering cybersecurity are not included as part of the literature review. These languages will be discussed in Chapter 6, where we will use BINA domain model to examine them.

2. *Construction of the BINA*: defines a conceptual model using the outputs of the previous step. At this stage of the project, we defined a conceptual model of the cyber resiliency domain. We did so by using a UML class diagram (cf. Section 4.4). A UML class diagram [139] was the preferable representational approach for the conceptual model as its notation is common and well known. Further, it can show concepts and how they relate with each other, which is the expressiveness that this part of our treatment's design needed. This step led to the creation of two artefacts:

- A conceptual model, here BINA. This model involved the use of the collected constructs. They need to be named. It additionally illustrated how the constructs related to each other, using existing knowledge found in the literature.
- A glossary specific to BINA was then designed. The concepts were aligned by reusing and, if necessary, enhancing their meaning. The constructs' definitions came from the alignment step that also covered the relations between them.

As the domain knowledge changed, its model had to be redesigned. This meant that the process had to be restarted, leading to design changes in BINA.

4.2 Literature review

Following the research method presented in the previous section, we began with a survey of the literature. In particular, we focused on four types of resources relevant to the scope of cyber resiliency.

The first set of relevant resources form cyber resiliency standards. These standards address resiliency at a high level. Because of this, they can be used to build domain-specific cyber resiliency approaches. These standards are:

- NIST SP 800-184 [6]: This special publication guides recovery planning at two levels:
 - a tactical level that corresponds to the immediate execution of a recovery plan; and
 - a strategic level where the recovery plan improves continually to make events less likely to occur.

It also provides relevant metrics that potentially contribute to information systems resiliency enhancement.

- NIST SP 800-61r2 [4]: This special publication offers guidelines for incident response capabilities at an organisational level. In this way, the capabilities are independent of the particular characteristics of the systems that an organisation uses. These capabilities correspond to incidents management and, in particular, data analysis and selection of appropriate response.

Cybersecurity standards compose the second set of resources. These resources tend to have a specific section that clarifies the meaning of relevant terminology. There are cases where the standards view the terminology critically. Some resources contain resiliency related terms as well.

- ISO/TR 22100-4:2018 [140]: This report aligns safety with cybersecurity. This alignment supports manufacturers of cyber-physical systems to consider cybersecurity. In particular, after a system is implemented, as part of a system, or reaches the end-user. It contributes to the consideration and resolution of cyber threats that can impact the safety of a system.
- NIST SP 800-82r2 [141]: This report is a cybersecurity guide for different types of Industrial Control Systems (ICSs). There it can be seen that cybersecurity needs to consider other types of requirements (e.g., execution, dependability, and safety requirements) along with those of security. The report also presents a typical ICSs topologies. Additionally, it presents common to ICSs threats and vulnerabilities and suggests mitigative controls for cybersecurity risks.
- NIST SP 800-160v1 [142]: This standard focuses on the engineering of responsive and resilient systems. These systems have cyber, physical and human aspects that collectively provide wanted functionalities. It aims to highlight cybersecurity challenges and approach them through the establishment of engineering processes. These processes need to satisfy stakeholders goals and requirements, considering them from the early stages of a system's engineering process and its whole life cycle.
- ISO/IEC 27001:2013 [143]: This standard outlines security requirements related to the full life cycle of a system of an organisation. It addresses cybersecurity risks, along with

their assessment and handling. This standard describes requirements in a technologically neutral manner, meaning that they are not dependent on the specific organisation's technologies.

- ISO/IEC 27032:2012 [144]: This guide provides a cybersecurity outline. It explains how it relates to other types of security, such as information, network, internet and critical infrastructure security. It also describes the relevant cybersecurity stakeholders and their roles and how they can cooperate in pursuing cybersecurity objectives.

Health-related standards constitute the third set of resources. They deal with standards that address cybersecurity or/and resiliency within healthcare. Thus they associate closer to this research project's scope.

- NIST SP 1800-1 [145]: This guide gives a cybersecurity reference design for healthcare organisations. It focuses on the exchange through mobile devices of healthcare information among caregivers. The guide uses a specific scenario and technologies. However, the scenario is demonstrative and does not limit the guide's contribution. Rather, it shows the attributes and abilities that cybersecurity practitioners can utilise to recognise related tools that can be blended appropriately with the existing healthcare organisation's systems.
- ISO 27799:2016 [146]: This standard provides guidelines for the use of security standards within the healthcare context. It outlines the cybersecurity requirements of healthcare organisations. Specifically, it explains the controls in ISO/IEC 27002 in a way that suits the cybersecurity of healthcare information. The cybersecurity properties that it focuses on are the confidentiality, integrity and availability of healthcare data.
- NIST SP 800-66r1 [147]: This guide supports the implementation of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Rule. This rule centres on Electronically Protected Health Information (EPHI). It particularly concentrates on protecting the cybersecurity properties of confidentiality, integrity, and availability for EPHI. The protection required is corresponding to logically predictable threats, attacks, events and hazards.

Cyber resiliency frameworks comprise the fourth set of resources.

- MTR140499R1 [7]: This technical report addresses the cyber resiliency relating it to advanced cyber threats. It presents relevant knowledge associated with systems engineering. Mainly, it shows how different approaches, if implemented together, interact with each other (e.g. dependencies, synergies, conflicts). Furthermore, it looks at how cyber resiliency approaches impact cyber attacks, based on the stage of their lifecycle (e.g. reconnaissance, weaponisation, delivery). It also offers information about maturity and easiness to use various cyber resiliency techniques.
- MTR110237 [8]: This technical report addresses the necessity for cyber resiliency. According to this report, cyber resiliency relates to sophisticated cyber-initiated attacks that challenge the resiliency of information systems. It proposes a resiliency engineering framework to support organisations to deal with sophisticated cyber threats offering a method to analyse cyber resiliency in a structured manner. It also includes relevant metrics. The framework overall perceives cyber resiliency engineering as part of the assurance engineering of missions.

By reviewing this diverse set of standards, it became clear that cyber resiliency standards and frameworks see the term 'cyber resiliency' as a set of organisational capabilities that can be planned in the short and long term for the specific needs of a domain. According to cyber security standards, these capabilities involve cyber, physical and human aspects that need to collaborate. These aspects need to be part of the resiliency design from the early stages of a system's engineering to allow it to perform for its intended purpose, meeting stakeholders' requirements. Cyber security standards also emphasise the need for a shared terminology that clarifies the concept of resiliency and associated entities. Additionally, health-related standards address the need for cyber resiliency designed to understand the contextual restrictions of a healthcare setting that is increasingly mobile and remote. Cyber resiliency frameworks remind us of the importance of knowing the malicious attempts and capturing them, and analysing them along with their impacts. In other words, cyber resiliency standards and frameworks provided cyber resiliency and malicious attacks-related terminology. Cyber security standards provided us with sociotechnical terms and metrics. Finally, healthcare standards offered contextual constraints that cyber resiliency plans need to incorporate to be applicable for healthcare systems. Hence, we used these resources as input to design BINA's domain model capturing all these different aspects of the cyber resiliency domain.

4.3 BINA construct association

This section presents the first step of the research method shown in Figure 4.1. Based on the resources discussed in Section 4.2, BINA constructs are extracted and set out in a table (cf. Appendix B). Also, the elicitation of the relations among the constructs takes place. This section closes with a discussion about the constructs association.

4.3.1 Constructs to study

We began the construct association by determining the variety of constructs to examine. An essential construct to explore was cyber resiliency (also called cyber resilience, resiliency or resilience). Cyber resiliency is related to security requirements and the security mechanisms that are used to satisfy them. Therefore, these constructs are also crucial. According to the first step, as shown in Fig. 4.1, the above concepts are just part of the first iteration and will be reconstructed as this step repeats. The final iteration will yield a table that will be the result of this first step. It is essential to clarify that this step can continue later on, as the need for new constructs might arise due to various reasons (e.g., field evolvment, technological changes).

4.3.2 Constructs analysis

This section examines the fundamental constructs of cyber resiliency derived from the resources initially introduced in Section 4.2. It also considers constructs related to cyber resiliency. At this stage, aspects of cyber resiliency examined in [130][121][122] are not reviewed. Rather, the review of cyber resiliency associated constructs takes place at this stage. The overarching purpose of this activity is to collect and associate the constructs. These constructs will be essential entities for the design of the BINA. In regards to constructs' attributes, please refer to Chapter 5. Analysing all constructs in detail would generate a wordy and repetitive document and would not add sufficiently in value. Thus, we choose to describe the first iteration of this step. The iterations that followed for this and other constructs follow the same course of actions.

Cyber resiliency standards

NIST SP 800-184 [6] perceives **enterprise resiliency** as:

The ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions...throughout the enterprise security lifecycle. [6, p. 4].

NIST SP 800-61r2 [4] defines the term **incident response** that its meaning partially covers the interpretation of enterprise resiliency.

The mitigation of violations of security policies and recommended practices. [4, p. 60].

Both descriptions reveal that resiliency relates to security. This observation holds independently from the term used to describe phases or an aspect of cyber resiliency. Subsequently, we examine these definitions with those used in the cybersecurity standards. This examination takes place to refine our initial findings.

Cybersecurity standards

In ISO/TR 22100-4:2018 [140], resiliency is not defined, but the definition of cybersecurity covers only the protection of IT-systems. NIST SP 800-82r2 [141] does not use the term cyber resiliency but defines a **steady state** as:

A characteristic of a condition, such as value, rate, periodicity, or amplitude, exhibiting only negligible change over an arbitrarily long period of time. [141, p. B-16].

Resiliency can associate to the preservation or return of a compromised system in a steady state. The examination of the steady-state definition reveals that a system's performance relates to production/service criteria and time. NIST SP 800-160v1 [142] does not offer a resiliency definition. Its security definition stands for the absence of those states that can result in unacceptable distractions, damages or other forms of cost. [142, p. 171]. ISO/IEC 27001:2013 [143] defines two terms that cover cyber resiliency aspects. Firstly, the term **information security continuity** focuses on operational continuation, being very similar to a steady state

Processes and procedures for ensuring continued information security operations. [143].

Secondly, the term **information security incident management** is defined as having the meaning:

Set of processes for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents. [143].

However, this definition includes a new construct, that of an incident. The term 'incident' stands for an event occurring at any stage of a process, service, system life-cycle [142, p. 168]. ISO/IEC 27032:2012 [144] defines cybersecurity and cybersafety, but in both cases it limits their meaning to preservation and protection. Nevertheless, the definition of cybersafety is protection from undesirable states. The same standard defines a consequence as "*Outcome of an event affecting objectives.*

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and, in the context of information security, is usually negative.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects." [143].

Definitions of phrases or aspects of cyber resiliency as part of cybersecurity standards verify their close connection. Cybersecurity standards further associate resiliency with the terms incident and consequence. The concept consequence is commonly present in the reviewed standards and named as 'impact'. The term 'impact' appears as a result of an incident. Hence,

the definition of an incident seems to be an integral part of resiliency from an incident response perspective. In other words, it arises that the construct of 'incident' has an integral part in the understanding of resiliency and a link exists between them. However, more research about the term 'incident' is needed to determine. This repetition of the first step of the research method shown in Fig. 4.1 will focus on the term 'incident' to improve our understanding of this construct and its role in the BINA domain. Here we focus on the concept of cyber resiliency, and thus, we do not include it in the analysis.

Health-related standards

Healthcare standards do not seem to consider cyber resiliency. Rather they seem to focus on information security. ISO 27799:2016 [146] uses the information security definitions of ISO/IEC 27001:2013 [143] that we have seen above. NIST SP 800-66r1 [147] also does not provide a definition for resiliency. Nevertheless, it does define security, within the healthcare context, as protection of information systems from a set of events (e.g., unauthorised access, services unavailability, information disclosure) that violate security properties (i.e., confidentiality, integrity, availability) [147, p. A-6]. The above confirms that information security relates mainly to information systems. This term needs further investigation that extends beyond this analysis and the first iteration. This section does not include the investigation into this that followed.

Cyber resiliency frameworks

MTR140499R1 [7] defines **defensive Cyber Course of Action (CCoA)** as:

A set of activities or Tactics, Techniques, and Procedures (TTPs) employed by automation, cyber defenders (...) and, as needed, other cyber staff (...) and mission staff in response to adverse cyber events. [7, p. 12].

This definition introduces two other terms, the TTPs and the adverse cyber event. The same framework defines TTPs in terms of methods, standards and resources [7, p. 13]. MTR140499 R1 also defines an adverse cyber event as an occurrence that causes adverse consequences to cyber resources [7, p. 12]. This definition raises concerns in regards to the term impact. Further iterations will focus on clarifying this term and its connections with the other constructs. In MTR110237 [8] **cyber resiliency** is actually defined as:

The ability of a nation, organisation, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function. [8, p. 8].

This definition clarifies that cyber resiliency analysis can take place at different levels. The variations fall under one of the two categories, the top-down or the bottom-up. If cyber resiliency follows a top-down approach it is considered at national or local level and involves governmental participation [63][64][66][74]. If cyber resiliency follows a bottom-up approach, then it is analysed at an organisational level and involves internal and external stakeholders [65]. In a top-down approach, cyber resiliency relates to all national critical infrastructures or specifically to infrastructures of the same sector (e.g., energy, transportation, defence, healthcare). Whereas in a bottom-up approach, the analysis concerns a particular infrastructure (e.g., plant, facility) or specific missions, objectives, processes, systems, applications or even components.

Discussion about the construct of cyber resiliency

We can make some first observations after the first execution of the construct alignment step conducted for the concept of cyber resiliency. First, we can say that there is yet to be popularised the term cyber resiliency. It seems that parts of it are described using other concepts. The common denominator that every relevant definition entails is the relation of resiliency with security. The main difference that distinguishes cybersecurity from cyber resiliency seems to be that the first part is preventive and protective, whereas the second part is withstanding and responsive when cybersecurity does not go as planned. Resiliency relates to an unwanted occurrence, generally termed an 'incident', and an outcome commonly named an 'impact'. An incident can occur if an attack results in a security property violation or if a threat has or can exploit a vulnerability successfully. The outcome of an incident impacts objectives. We also recognised other constructs that are associated with cyber resiliency (e.g., asset). Repetitions of this step will hopefully clarify this further.

Furthermore, other related constructs are parts of cyber resiliency definitions (e.g., in MTR 110237 [8], the interpretation of cyber resiliency shows as potential constructs the terms capability, cyber resources and functions). Nevertheless, these observations are the outcome of the first execution of the step of constructs alignment on the construct of cyber resiliency. More repetitions of this activity on this and other constructs will improve our observations and further evoke cyber resiliency constructs.

4.3.3 Association table of BINA constructs

Following the collection of meanings of the BINA-related constructs (Appendix A), as performed for the resiliency concept in the previous section, association tables were produced iteratively. The tables used the constructs' meanings to analyse and arrange them with each other. Throughout this association task, a new construct was appearing (like the term *incident* in the prior section), or the interpretation of another construct was necessary to thoroughly comprehend the examined construct (as in ISO/IEC 27001:2013, e.g., for *information security incident management*, to reach a shared understanding for the meaning of the term *incident*). We then updated the glossaries of terms with the new term and its meaning. Thus, incrementally we assembled or modified this construct and its meaning based on findings of subsequent iterations.

This section discusses the alignment tables for the BINA constructs suggested in the studied references. We categorised the results, for clarity, by the family of the source. The complete alignment table is available in Tab. B.2 in Appendix B. Finally, we identified 13 constructs. They are numbered from (1) to (13), but not labelled for the moment (cf. Section 4.3.3). We present the constructs classified by category, as in Section 4.3.3: Domain-related concepts, Offensive-related concepts and Defensive-related concepts. These categories resulted following the BINA process, presented in Section 4.1. Domain-related constructs are constructs focused on the objective construct and expressing what has value for the infrastructure and needs to be protected. Offensive-related constructs are the set of constructs used to describe unwanted occurrences. Defensive-related constructs are the constructs used to counter unwanted occurrences, usually at a different level of granularity.

The constructs that are on the same line are constructs semantically equivalent. For example, in Tab. 4.2, the construct of *disturbance* in ISO/TR 22100-4:2018 is equivalent to the construct of *threat event* in NIST SP 800-82r2. The *disturbance* is defined as *an undesired change in a variable of a system that tends to affect the value of a controlled variable adversely* and *threat event* as

an event or situation that has the potential for causing undesirable consequences or impact. If several constructs are in the same cell, these constructs are semantically equivalent and from the same source. For example, as depicted in Tab. 4.1 for NIST SP 800-184, incident and cyber event are two constructs of NIST SP 800-184 that are semantically equivalent. An incident is a *violation of acceptable policies, or security policies and best practices*, and a cyber event is defined as *a specific cybersecurity incident or set of related cybersecurity incidents that result in the successful compromise of one or more information systems*.

The reader shall note that the tables proposed in this section are the final ones obtained after having performed every iteration of step 1. This explanation clarifies why each table has 13 constructs, which is equivalent to the final number of constructs used in the BINA. Sometimes, some concepts have no equivalence in the references. For example, in Tab. 4.1, the concept (3), named later *objective* (cf. Section 4.3.3), does not have any equivalence in NIST SP 800-184 and in NIST SP 800-61r2.

Cyber resiliency standards

In cyber resiliency standards, we did not identify all the 13 constructs (cf. Tab. 4.1). Only the constructs *asset* (2), *vulnerability* (5), *event* (6), *incident* (7), *threat* (10) and *Cyber Incident Response Plan (CIRP)* (12) were present with the names used later as constructs of BINA. The constructs *actor* (1) and *Cyber Course of Action (CCoA)* (11) had the form of specific instances. In particular, NIST SP 800-61r2 provided definitions for the actors *Cybersecurity Incident Response Team (CSIRT)* and *Computer Incident Response Centre, Computer Incident Response Capability (CIRC)* focusing on cyber resiliency actors. An *asset* (2) expresses an item of value for the achievement of an objective that *actors* (1) pursue. An *asset* (2) has *vulnerabilities* (5) that a *threat* (10) can exploit and cause a negative impact. A threat is the potential of a violation that along with an actual violation against security policies, standard or practices form *incidents* (7). For other types of unwanted occurrences that affect a system or infrastructure, the term *event* (6) captures them. To address incidents, cyber resiliency actors apply *CIRPs* (12) that along with *actors* (1) and security controls form the *CCoA* (11). However, cyber resiliency standards express *CCoA* by defining at a high level the terms *incident response* and *incident handling*.

Table 4.1: Association table for cyber resiliency standards.

Type	Concept	NIST SP 800-184	NIST SP 800-61r2
Domain	(1)	/	CSIRT, CIRC
Domain	(2)	asset	/
Domain	(3)	/	/
Domain	(4)	/	/
Domain	(5)	/	vulnerability
Offensive	(6)	event	event
Offensive	(7)	incident, cyber event	incident, cyber event, computer security incident
Offensive	(8)	/	/
Offensive	(9)	/	/
Offensive	(10)	/	threat
Defensive	(11)	/	incident response , incident handling
Defensive	(12)	CIRP	CIRP
Defensive	(13)	/	/

Cybersecurity standards

From the review of cybersecurity standards, we were able to draw some new conclusions (cf. Tab 4.2). Firstly, the construct of *objective* (3) seems to be of great importance for cybersecurity standards. They also express factors that impose restrictions and limitations on a system as *constraints* that later, we will refer to them in BINA mainly for security as *security constraints* (4). Cybersecurity standards define *risk* (9), and *residual risk* (8). The difference between the two terms relates to the application or not of CCoAs. In the case of *risks* (9) CCoAs are used to manage them, or their non-use is a conscious decision. However, in the case of *residual risks* (8), CCoAs are not applied and include the cases where the remaining risks remain unknown. Finally, they identify *security controls* (13) as mechanisms that address one or more security constraints.

Table 4.2: Association table for cybersecurity standards.

Type	Concept	ISO/TR 22100-4:2018	NIST SP 800-82r2	NIST SP 800-160v1	ISO/IEC 27001:2013	ISO/IEC 27032:2012
Domain	(1)	/	/	/	/	/
Domain	(2)	/	/	asset	/	asset, information asset, physical asset, virtual asset
Domain	(3)	/	/	/	objective	/
Domain	(4)	/	/	constraints	/	/
Domain	(5)	vulnerability	vulnerability	vulnerability	vulnerability	vulnerability
Offensive	(6)	disturbance	threat event	event, information security event	event	/
Offensive	(7)	IT-security incident	incident	incident	information security incident	/
Offensive	(8)	/	/	/	residual risk	/
Offensive	(9)	/	risk	risk	risk	/
Offensive	(10)	threat	threat	threat	threat	threat
Defensive	(11)	/	/	/	/	/
Defensive	(12)	/	/	/	/	/
Defensive	(13)	/	security control, technical control, operational control	security control	/	control

Health-related standards

Constructs used in health-related standards (cf. Tab 4.3) do not relate that much to cybersecurity as safety seems to be their central concern. In particular, the *actor* that they refer to is the *subject of care*. To provide healthcare services to the care subject, they recognise that healthcare-related information systems assist all aspects of healthcare services provision. In this essence, information systems are essential *assets* (2) of healthcare infrastructure, and they need to be secure in order not to harm the *actors* (1). Healthcare standards also recognise the importance of *security controls* (13). They refer to them using the terms *technical safeguards*, *physical safeguards* and *tools*. In this way, healthcare standards recognise that the cyber (*technical safeguards*), as well as the physical aspects of assets (2) (*physical safeguards*), need to be secure. The term *tool* is more specific to the actual type of technology and thus more restrictive than the term *security control*.

Table 4.3: Association table for health-related standards.

Type	Concept	NIST SP 800-66r1	ISO 27799:2016	NIST SP 1800-1
Domain	(1)	/	subject of care	/
Domain	(2)	information system	health information system	/
Domain	(3)	/	/	/
Domain	(4)	/	/	/
Domain	(5)	/	/	/
Offensive	(6)	/	/	/
Offensive	(7)	/	/	/
Offensive	(8)	/	/	/
Offensive	(9)	/	/	/
Offensive	(10)	/	/	/
Defensive	(11)	/	/	/
Defensive	(12)	/	/	/
Defensive	(13)	technical safeguards, physical safeguards	/	tool

Cyber resiliency frameworks

Finally, the cyber resiliency frameworks (cf. Tab 4.4) are compliant with the previous findings. Once more they consider *assets*, but name them as *resources* and *cyber resources*. Semantically, they correspond to separately manageable components, services, devices, capabilities that contribute to the achievement of an *objective* (3). Nevertheless, these frameworks instead of the term *objective* (3) refer to *missions* and *business functions*. They perceive them as activities or processes that are targeted to achieve a goal. Similarly they refer to *events* (6) and *incidents* (7) using the similar terms of *adverse cyber event* and *adverse conditions and stresses*. An *event* involves cyber resources that can have adverse consequences for other cyber resources. Contingency plans include them. These interpretations mean that *events* (6) are predictable, known and not necessarily malicious. Cyber resiliency frameworks also address *incidents* (7), but particularly as *cyber attacks* that are commonly carried out by cyber means and intends to adversely affect assets, objectives, or actors that depend on those assets.

Table 4.4: Association table for cyber resiliency frameworks.

Type	Concept	MTR140499R1	MTR110237
Domain	(1)	/	/
Domain	(2)	resource	cyber resource
Domain	(3)	mission, business function	/
Domain	(4)	/	/
Domain	(5)	/	/
Offensive	(6)	adverse cyber event	adverse conditions and stresses
Offensive	(7)	/	cyber attack
Offensive	(8)	/	/
Offensive	(9)	/	/
Offensive	(10)	/	/
Defensive	(11)	CCoA, TTPs	/
Defensive	(12)	/	/
Defensive	(13)	/	/

Discussion about the Association Tables

After identifying the different terms used in each BINA source, our assumption that the terminology in the ISSRM domain is not unified. Many different terms are used to depict the same

or similar constructs. Three to four different terms can correspond to the same constructs. Moreover, the same term is used to depict different constructs. The association tables help to connect the different sources. A practitioner might need to combine several sources in a project to enhance his/her results. S/he may also need to use some standards and frameworks in parallel to validate his/her results. Finally, for compliance purposes, s/he can use a standard or framework to fulfil the requirements. In all these cases, a practitioner needs to map the constructs of two (or more) approaches. The alignment tables are an artefact providing this capability.

4.3.4 Elicitation of relationships between BINA constructs

After identifying and aligning constructs, it is necessary to identify the relationships existing between them. In this section, the relevant resources (cf. Section 4.2) are analysed to extract relationships between the constructs. The process used is similar to the one applied for the elicitation of BINA constructs (cf. Section 4.1). Finally, we define relationships between constructs based on the selections of definitions used for the description of constructs.

Extraction of the relationship between two constructs

To demonstrate the analysis of relationships, we show the definition of relationships between the construct (10) (called threat in the resources) and (5) (called vulnerability). Of course, the existence of a relationship between two constructs is not mandatory, but after the analysis of the definitions for the construct association (cf. Section 4.3.3), we assert that these two concepts are related to one another.

In cyber resiliency standards [6, 4], vulnerability and threat are associated together in NIST SP 800-61r2 [4]. There the the term *vulnerability* stands for:

A weakness in a system, application, or network that is subject to **exploitation or misuse**. [4, p. 60].

This exploitation or misuse relationship seems to relate with the term *threat* that stands for the cause of exploitation or misuse of a vulnerability. This first standard is quite different in terms of the relationship between the two constructs: it is the only one not mentioning the exploitation of vulnerabilities by a threat.

However, the relationship between the two constructs is more explicit in cybersecurity standards, namely ISO/TR 22100-4:2018 [140], NIST SP 800-82r2 [141], NIST SP 800-160v1 [142], ISO/IEC 27001:2013 [143], ISO/IEC 27032:2012 [144].

More specifically, in ISO/TR 22100-4:2018 the term *vulnerability* is defined as:

weakness in the security of an IT-system that can be **exploited or triggered** by a threat [140].

Here the term vulnerability connects with the term threat through the relationship exploits or triggers. In other words, a threat exploits or triggers vulnerabilities.

In NIST SP 800-82r2 [141], it is *threat source* (concept (10)) that is related with vulnerability:

The intent and method targeted at the intentional **exploitation** of a vulnerability or a situation and method that may accidentally **trigger** a vulnerability. Synonymous with Threat Agent [141, p. B-17].

The same relationship is present in the definition of *vulnerability* that is

Weakness in an information system, system security procedures, internal controls, or implementation that could be **exploited or triggered** by a threat source. [141, p. B-18].

Similarly, NIST SP 800-160v1 [142] in Appendix J offers many examples of mitigation of persistent threats where it mentions the exploitation of relevant vulnerabilities. For example, it describes the cyber resiliency technique of non-persistence as

The adversary's attempt to **exploit** a vulnerability to achieve a persistent foothold is impeded if the attacked service is terminated because it is no longer needed by the defender [142, p. 136].

Nevertheless, the same standard does not provide an explicit definition that connects the two terms.

ISO/IEC 27001:2013 [143] states the relationship between the terms vulnerability and threat in the definition of the term *vulnerability*

weakness of an asset or control that can be **exploited** by one or more threats [143]

ISO/IEC 27032:2012 [144] uses a very similar definition for *vulnerability* too

weakness of an asset or control that can be **exploited** by a threat [144].

On both occasions, at least one threat *exploits* a vulnerability.

In health-related standards [146, 143, 147], the construct of *vulnerability* does not exist. Consequently, we could not infer any relationship between the two analysed constructs. Regarding cyber resiliency frameworks MTR140499R1 [7] and MTR110237 [8], threat and vulnerability are related together. In particular, MTR140499R1 in the integrity/quality checks, states that

... the malware can **exploit** a vulnerability; ... [7, p. 53]

In conclusion, the final direction is that one or more threats (10) exploit or trigger a vulnerability (5). Iterative reviews of relationships bring up terms *threat source* and *threat agent* that are in fact, aggregated in construct (10). This observation reveals that they can all be related to vulnerability by an exploits relationship, as is most often the case. Considering this aggregation, the most relevant to us appears to link construct (10) (called threat) and vulnerability (5) with an exploits link.

Summary of the relationship extraction

It is theoretically possible to define the same kind of alignment table for relationships between constructs, as previously done for specific constructs (cf. Section 4.3.3). The definition of such a table should indicate the multiplicities of each relationship. However, the first attempt at such an exercise [148] highlighted some limitations. The set of possible relationships between the constructs in the preceding section showed that each resource had its unique perspective of the relationships existing between the constructs. The difficulty sometimes reinforces this point to interpret natural language. It was already a weakness for construct association, but even more so for relationship extraction between constructs. The experience of Genon [148] has also shown that the utility of such a table is severely limited because it is difficult to read (construct association is more explicit than relationship association). The multiplicity introduction in such an alignment is elaborate too. The main problem is the lack of sufficient information available regarding multiplicities. Finally, such a table is not considered necessary for the definition of relationships. Most of the required information is in the collected definitions, provided in Appendix A. Sometimes, it is necessary to collect further information (like in MTR140499R1 [7]), but these cases remain rare.

To define the relationships between the constructs of the BINA, we examined the existing relationships found in the relevant resources. The examination was done by analysing each resource one by one and identifying every relationship existing between the resource constructs.

Based on the constructs' definitions, we analysed each construct to see how they linked with one another. The multiplicities were defined too. This review was repeated for each resource of the selected literature (cf. Section 4.2).

4.3.5 Overall remarks about construct association and relationship extraction

Regarding the outcome of the extraction and the association of BINA constructs and relationships, this research body of work provides a formality by aggregating the different informal resources studied. For each resource, a conceptual model can now be defined based on the extracted constructs and relationships. However, defining a conceptual model for each BINA resource is not an objective of our research project nor a step towards the achievement of our research objectives. Hence, we did not design the models of each resource. But, based on the extracted constructs (cf. Section 4.3.3) and the relationships among them (cf. Section 4.3.4), the various conceptual models can efficiently be extracted.

4.4 The BINA conceptual model

Based on the study performed, the first step of the research method (cf. Fig. 4.1) resulted in the association of the BINA constructs and the extraction of their relationships. The second step of the method included the construction of the BINA. It is a conceptual model represented in the form of a UML class diagram [149], composed by the constructs identified and presented in the association table (cf. Tab. B.2). For each of them, a name was chosen, inspired by their name in the literature (Section 4.4.1). A glossary was provided with the model, defining each construct of the conceptual model (Section 4.4.2). Finally, the constructs were linked together based on the relationships identified (Section 4.4.3). This domain model is further to the syntactic and semantic reference for the assessment of security-oriented modelling languages, with regards to their support of BINA (Chapter 6).

4.4.1 Names of the constructs

Each construct had a number initially, as shown in the association Tab. B.2. We needed to further determine a name for each of these constructs. Tab. 4.5 presents the proposed names for the thirteen constructs. We choose names based on various criteria. Initially, we considered the number of times that a name appeared to describe a construct in the resources. Then, the terminology coming from ISO standards [140, 143, 144, 146] was considered to be the most important resource, because it is generally the most accepted and used vocabulary. In the next section, we ordered and related these constructs using a UML class diagram. Moreover, we defined each contrast.

4.4.2 Constructs definitions

We ordered the BINA conceptual model and constructs' definitions, as we did for the association tables, meaning following the three major groups of constructs: (i) domain-related constructs; (ii) offensive-related constructs; and (iii) defensive-related constructs. Each construct is illustrated with the help of examples.

Table 4.5: Name of the constructs included in the BINA.

Type	Concept	Name
Domain	(1)	actor
Domain	(2)	asset
Domain	(3)	objective
Domain	(4)	security constraint
Domain	(5)	vulnerability
Offensive	(6)	event
Offensive	(7)	incident
Offensive	(8)	residual risk
Offensive	(9)	risk
Offensive	(10)	threat
Defensive	(11)	Cyber Course of Action (CCoA)
Defensive	(12)	Cyber Incident Response Plan (CIRP)
Defensive	(13)	security control

Domain-related constructs describe what domain constructs are essential for cyber resiliency and the criteria that need to be met to guarantee cybersecurity. The constructs are:

(1) **Actor**: represents an entity that has intentionality and objectives within a system or its infrastructural setting. An actor can be a social agent, an intelligent agent, a position, or a role. *Examples: surgeon; security engineer; maintenance team; incident response team; manager; patient; subject of care; nurse*

NOTE: The reviewed resources do not define the term actor. Rather particular instances of the term are defined (e.g., subject of care, Cybersecurity Incident Response Team (CSIRT), Cyber Incident Response Team (CIRT))

(2) **Asset**: separately manageable resources in cyber and/or physical space that can be used by multiple **actors** to achieve **objectives**. They have interrelated attributes that include type and criticality. An asset type can be tangible (i.e., physical) or intangible (i.e., virtual), or hybrid (cyber-physical). If an asset is cyber-physical, it means that it includes engineered, interacting networks of physical and cyber components. An organisation can use this attribute to enumerate assets and make the security engineer aware of them, affecting their management. For instance, this attribute could benefit the response process if a security engineer bases his decisions on the asset type. The second attribute, namely an asset's value, expresses the degree to which an asset is relied upon to achieve objectives. It can take qualitative and quantitative values within a scale. For example, an asset's value can be 'High' or '4' (on a scale of 1 to 5) if it is relied upon to provide essential services to clients, which is the decisive objective of this business.

Examples: operating system, Ethernet network; people encoding data; system administrator; air conditioning of server room, Magnetic Resonance Imaging (MRI), Implantable Medical Device (IMD).

NOTE: This construct is the generalisation of the security control construct.

(3) **Objective**: set by an **actor**, consistent with the infrastructure policy, to achieve specific results and can apply at different levels (e.g., strategic, infrastructure-wide, project, service and process).

Examples: decrease the waiting times in the emergency department; perform procedures like imaging, injections, infusions, x-rays; surgical procedures and operations; conduct telesurgery; safe remote pa-

tient monitoring.

NOTE: The term objective in GORE approach takes the name goal.

(4) Security Constraint: security requirement that imposes restrictions and limitations on one or more **objectives**.

Examples: confidentiality; integrity/consistency; availability/timeliness; authenticity/originality; non-repudiation/accuracy; possession/control; utility/relevance.

NOTE 1: A security constraint is a security requirement. It has the form of constraint towards objectives.

NOTE 2: A security constraint relates to risk transfer decisions when third parties as actors have restricted dependency relations. However, security constraints are irrelevant to risk avoidance and risk retainment cases.

NOTE 3: Each security constraint contributes to identifying security controls that create cyber resiliency by responding to incidents.

(5) Vulnerability: weakness of an **asset** or **security control** that can be exploited by a **threat**.

Examples: Meltdown; Spectre; BlueKeep; EternalBlue

Offensive-related constructs present the relevant components' definitions and the primary principles that should be taken into account when designing the possible offensive actions. The constructs are:

(6) Event: is any observable occurrence in a system or network that have not risen to the level of a violation of **security constraints** (e.g., reconnaissance) and is part of contingency planning.

Examples: fault; power loss; fire; flood; panic; reconnaissance; weaponisation; delivery.

NOTE: Event is a generic term used on some occasions as any observable occurrence. The definition provided in this section considers the construct incident and attempts to indicate their differentiation.

(7) Incident: single or a series of violations or imminent threat/s of violation of **security constraints**.

Examples: unauthorised disclosure of classified or sensitive information; theft of classified or sensitive information; unauthorised modification of classified or sensitive information; theft of equipment that contains classified or sensitive information; unauthorised access to areas containing IT equipment which stores classified or sensitive information.

NOTE: This construct is the generalisation of the threat construct.

(8) Residual Risk: is the **risk** that remains after the application of CCoAs and can also contain unknown risk or contain the risk that the application of CCoAs has not managed or resolved.

Examples: improving maintenance procedures does not contain the risk of human error; to cover cybersecurity risks, a hospital buys an insurance policy (but this would not cover the risk of the insurance company becoming bankrupt and failing to pay out should a cybersecurity incident occur); if the risk of a data breach is accepted then all this risk is not managed, and thus it will be a residual risk; if a hospital does not buy any radiological equipment for fear of cyber threats then the risk of competitors to push them out of the market remains as residual risk.

(9) Risk: is the consequence of an **incident** or **event** that can result in a range of negative conse-

quences associated with an undesirable change or non-change to **asset/s**, **CCoAs**, **objective/s**, **security constraints** and its initial impact can escalate through knock-on effects.

Examples: a malicious actor using social engineering on a physician of the hospital, because of the significant number of staff and weak awareness of its legitimate members, the actor could access workstations; another malicious actor penetrates the hospital's building pretending to be a patient and because of weak physical access control, manages to steal documents containing sensitive information and thereby to provoke loss of confidentiality of healthcare records.

(10) **Threat**: a potential cause of an **incident** which exploits a vulnerability and can result in a negative impact on **assets** and other undesirable **risks** from such impact.

Examples: WannaCry; Redux; Rhino; Nandao; Earth/Eve; Elderpiggy; Hammer Drill; Brutal Kangaroo; EternalSynergy; EternalRomance; EternalChampion

Defensive-related constructs describe the decisions and implementation that can respond to offensive activities. Cyber resiliency defence-related concepts involve various levels of design decisions. The constructs are:

(11) **CCoA**: a set or sequence of **CIRPs** and **security controls** employed by automation and/or **actors** in response to cyber **incidents**.

Examples: the incident response team will use the adaptive response to contain a cyberattack at a reconnaissance stage; if the attack progresses to the weaponisation stage, they will delay the attack utilising diversity; where the attacker has to deliver a malicious payload, they will negate the progression through dynamic positioning; to thwart the next stages they will use non-persistence.

NOTE: Takes the form of interconnected CIRPs, security controls and/or actors that participate in response to an incident.

(12) **CIRP**: an established set of activities or tactics, techniques, and procedures (TTPs) to address incidents against an infrastructure and/or system/s.

Examples: predetermined response stance; acceptable use policies; incident response team training program; users and host-based security education

NOTE: Generally, a CIRP can be a means for maintaining after the occurrence of an incident a security constraint that ultimately contributes to the achievement of an objective.

(13) **Security Control**: is a mechanism designed to address needs as specified by one or more **security constraints**.

Examples: dynamic reconfiguration; architectural diversity; non-persistent information; dynamic segmentation and isolation; behaviour validation.

NOTE: The focus of the security controls is to respond to incidents, and thus, they are closely related to cyber resiliency techniques (e.g., adaptive response, diversity, substantiated integrity)

4.4.3 Relationships and multiplicities of the BINA domain model

In this section, we highlight the relationships between the constructs of the BINA (cf. Fig 4.2).

An actor pursues zero or more objectives. To do so, an actor might use zero or more assets. Assets are essential to realising objectives because objective attainment requires zero to several assets. If an objective is pursued and has relevant associated assets, that does not imply that

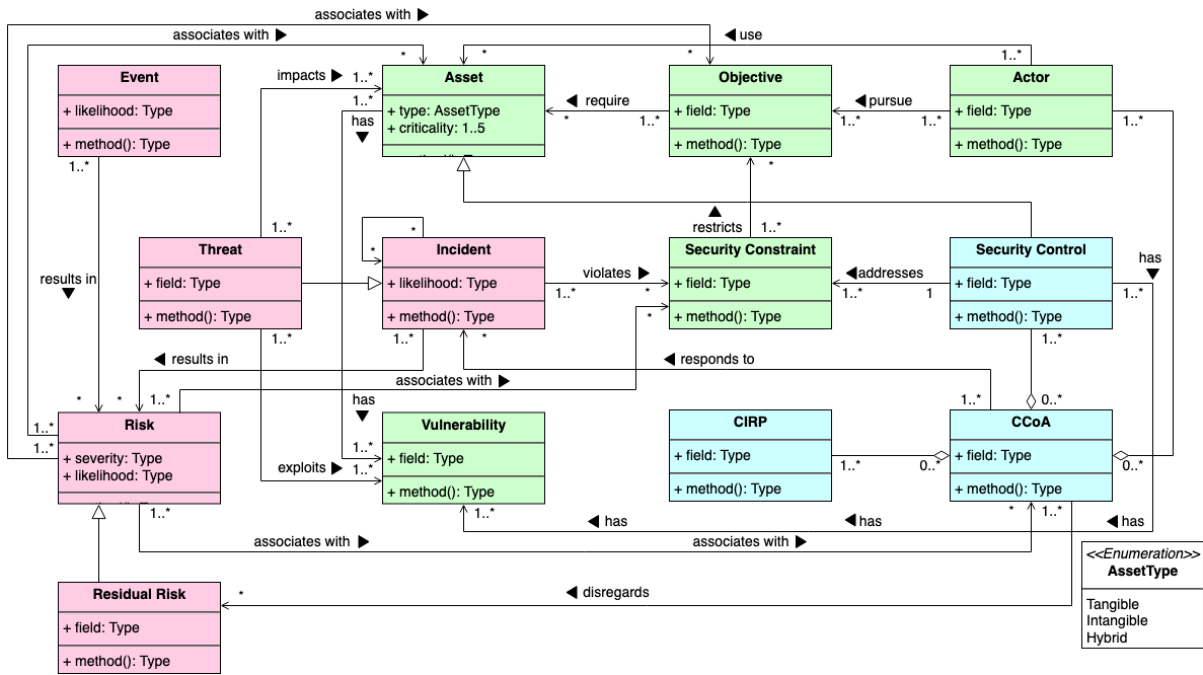


Figure 4.2: The BINA domain model.

the actor pursuing the objective will use the same assets. Assets can be specialised in security controls. Security controls to address security constraints, and a security constraint can restrict zero to several objectives. A security constraint can restrict many different objectives or not restrict any of them. A vulnerability is a characteristic of assets and security controls that can have from zero to several vulnerabilities. An asset or security control can potentially have a vulnerability. However, some assets and security controls instances might not have a vulnerability. At least not known at the time to the analyst.

In the context of cyber resiliency, an incident or threat can relate to one or more vulnerabilities. A specific threat can only be related to a specific incident. The threat exploits zero to several vulnerabilities. A threat impacts one or more assets, and several threats can impact an asset. The asset impacted by a threat is not necessarily the same as the one linked to the vulnerability exploited by this threat. For example, a vulnerability in the medical device operators, not adequately security-aware, can enable a threat to impact a server. If a threat is identified but has no relevant associated vulnerability (e.g., network attack on an offline system), it will neither be part of an incident nor a risk. Different threats can exploit a given vulnerability and, therefore, can relate to many different incidents. If no threat exploits a vulnerability, then no relevant threat is modelled.

A given incident or event leads to zero when an incident or event does not produce a risk that impacts assets, objectives, CCoAs. Many different incidents or events can cause risk. Sometimes, incidents or events can cause a risk that seems irrelevant and contained in none of the predicted risks. For example, the disclosure of medical information about patients could be relevant to healthcare infrastructure. However, if the attack fails to gather any medical information, then no risk has materialised. Moreover, one or several risks can lead to other (indirect) risks. For instance, the risk of unauthorised access to a database at a system level could lead to confidential information disclosure at a business level, resulting in the loss of customer confidence and/or legal penalties.

Risks impact assets, objectives and CCoAs. An asset, objective, or CCoA can be impacted by zero (if the analyst does not consider any risk as relevant) or several risks—further, a risk

impacts at least an asset, objective or CCoA. At the level of objectives, a risk negates one or more security constraints, and given security constraints can be negated by zero (if this security constraint contains no relevant risk) or several risks. One or several security criteria can be taken into account to assess the significance of a risk, but a security constraint can be concerned by none of the risks in the case where there is no impact for this constraint.

A CCoA signifies the decision to respond to one or more risks. Each identified risk has a CCoA (even if the decision is to accept the risk), and sometimes several of them can be combined (even if they are not mutually exclusive). CCoAs lead to one or more security constraints. A CCoA is composed of one or more security controls, CIRPs and actors. The same security control, CIRP and an actor can be part of several CCoAs. One of many CCoAs can maintain each security constraint. However, the CCoA for acceptance and avoidance maintains no security constraint. For example, when the risk is accepted or mitigated by security constraints. Finally, a 'security control' implements one or more security constraints, and one or several 'security control(s)' may implement the same security constraint.

4.4.4 Validation of the BINA

We performed an experts review for the validation of the BINA conceptual model, which led to the iterations of the research method depicted in Fig 4.1, and incremental improvements of the conceptual model. Practitioners and scientists already carried out the validation. In particular, we involved in the review five experts that voluntarily took part in the online session reviewing the modelling language. Two were from a technology company in Greece, one from a healthcare provider in the UK, one from a US medical devices producer company, and one from Swiss company that offers medical devices documentation management.

The experts were industry researchers. All experts had more than fifteen years of experience in software engineering and/or information security. Also, most experts were experienced in security engineering, while some experts had experience in healthcare cybersecurity and resiliency. Almost all experts were familiar with UML and other modelling languages. Each review was performed in a face to face workshop with the expert. They challenged the conceptual model regarding their view of cyber resiliency and their knowledge of the relevant standardisations and resources.

In the workshops, we first presented the project and the research method. Secondly, we introduced and explained the conceptual model. The practitioners and experts engaged in open discussions, which generated questions about the conceptual model. The discussions and questions were not based on a template but focused on the issues highlighted by each reviewer. All of their comments were analysed and discussed together, based on the information collected in the glossaries of Appendix A. Once we reached a consensus on the conceptual model, the process ended. The time spent for each interview varied from person to person, ranging from half an hour to several hours of presentation and discussion or stretching over several days by correspondence.

The main comments of the reviewers were that 1) the research method was reliable, and 2) the conceptual model was easy to validate because of the glossaries and the alignment tables. Moreover, the reviewers considered that for explaining the different constructs, using a conceptual model was more understandable than using verbal and textual means only. From this validation, we identified the areas that required redesigning. We did not have to reconsider the concepts and their relationships. Instead, we focused on their names, their definitions and the multiplicities.

The validation continued with the application of the conceptual model on a reality-based case study. Chapter 8 details this assessment. The conceptual model was used to introduce the BINA as the central artefact to catch the different concepts taking place in the different steps of the performed approach. Notably, one of the practitioners and suppliers of medical device manufacturers was interested in using the conceptual model and the potential to integrate it into their software tool to manage medical devices engineering.

The validation did have some limitations. We were able to involve six experts' review of the conceptual model. This set of participants is limited, and therefore, the conclusions cannot be generalised. Moreover, expert reviews are subjective, as they depend, for example, on their experience, knowledge, beliefs. The case study is more demonstrative as it applies the conceptual model to healthcare infrastructure. We discuss these limitations, in more detail, in Section 9.1. Regarding future work, currently, we are developing a software tool that should allow more accessibility and further validation of the conceptual model from other experts. The software tool will support the comparison exercise needed to understand the conceptual model and its usefulness for practitioners.

4.5 Benefits and Limitations of the BINA

This section highlights the benefits and limitations of the BINA conceptual model.

4.5.1 Benefits of the conceptual model

The BINA conceptual model provides several benefits for different users: for BINA practitioners, for researchers, or both.

Nomenclature level

The BINA conceptual model contributes to establishing a standard nomenclature for the cyber resiliency community. As shown in Section 4.2, there are several efforts from standardisation bodies, but they are still a work in progress. Cyber resiliency approaches are also increasingly introduced and learnt in various academic and professional curricula. However, due to the absence of a global terminology, new or specific ones are relied upon. As a consequence, we observed that practitioners experience communication problems when discussing cyber resiliency and related concepts. We think that the results of our research can help to reach harmonisation at this level.

Practice level

Although we have constructed the BINA conceptual model based on the existing literature on cyber resiliency, cybersecurity and health-related standards as well as cyber resiliency frameworks, the developed conceptual model can serve as the guidelines to investigate new emerging references, e.g., a new method or standard. The BINA conceptual model might suggest contextual information that the new resources should consider. Further, the BINA conceptual model itself might evolve when new relevant resources are determined. In this case, a new iteration of the research method (cf. Fig. 4.1) should be performed, considering the new resource.

However, the multitude of existing conceptual models relevant to cyber resiliency and its aspects leads often to uncertainty about their scope and depths. They generally have different coverage of cyber resiliency, and thus, of the underlying constructs. The association tables provided in Section 4.3.3 help us to provide interoperability between the different resources. It shows the equivalence of constructs between resources. The definition of the BINA conceptual model with its associated glossary is one step further toward interoperability between cyber resiliency and related resources. Practitioners can use it as a standard reference between several resources, with traceability provided by the association table between the BINA conceptual model and the resources.

Research level

We hope that the proposed BINA conceptual model can support the scientific community to understand the scope of cyber resiliency better and therefore achieve better integration of resiliency-related concepts in security-oriented modelling languages. Also, where several languages are put together in order to cover the cybersecurity lifecycle, the conceptual model can be used as the basis for the traceability framework that will support the mapping between the different models produced (as, for example, the traceability needed between a healthcare system and a cyber-resiliency model).

Moreover, the BINA conceptual model is also used in Chapter 6 to conduct the assessment of other security-oriented modelling languages. The BINA conceptual model serves as a guideline to support the analysis of security-oriented modelling languages [50, 32, 33]. In Chapter 6, we will also illustrate this comparison between the BINA conceptual model and the following security-oriented modelling languages: KAOS extended to security [50], Misuse cases [32] and Secure Tropos [33].

4.5.2 Limitations of the conceptual model

Successful practices have used formal and ontology-based approaches to define and compare the semantics of modelling constructs [150, 151]. In the cyber resiliency context and based on the feedback of these practices, we have decided first to follow an approach based on conceptual models, natural language descriptions and common sense to analyse cyber resiliency related resources. The reasons are the following:

- the analysed sources are neither easily understood nor already adequately formalised (as discussed in [152]), to let us apply a formal comparative semantics method in a realistic time-frame;
- a conceptual model complemented with natural language definitions of the central concepts of the cyber resiliency domain can be formalised. However, further formalisation of semantics [152], although eventually desirable (cf. Chapter 7), has recently been deemed too risky. Indeed, complete semantics would require significant effort that could be a waste of time, regarding our objectives, without first reaching a consensus on the partial formalisation;
- automated semantic similarity analysis (see [153]) pays off when domains are too complicated to be handled by domain experts or the amount of information to be compared is unmanageable by humans. We do not meet these conditions here.

Regarding the construction of a conceptual model, there are several techniques in software engineering and system development. These techniques are generally part of domain engineering. Precisely, domain analysis should define the essential components of the domain, organise an understanding of the relationships among these components, and present this understanding in a useful way [154]. In this context, we find approaches like in [155, 156, 157]. Although we do not use these techniques directly, as our aim was not to develop product lines, the method we used for defining the BINA conceptual model is compliant with these approaches. In particular, we have produced the three main artefacts required for domain analysis: a domain definition, a domain lexicon and a conceptual model.

As discussed in Section 4.4.4, the validation can still be improved. Although our validation through expert review and case study has some limitations, it appears to be the most efficient, appropriate and relevant means to achieve this project's objectives (cf. Section 1.6). The validation by other experts is still open. Moreover, a software tool is currently being built to assess the usability of the domain model for planning purposes with a broader audience.

4.6 Discussion and Closing Remarks

In this chapter, the BINA conceptual model was defined, composed of a conceptual model, represented in the form of a UML class diagram, and the definitions of its different constructs and relationships were explained.

First, a research method was presented, which aimed at defining, in a structured way, the design of the conceptual model. This research method relied on a survey of the cyber resiliency literature. The first step of the research method led to a BINA construct association. As found in the resources studied, definitions of terms were collected, and an assignment table was built, indicating synonymy or semantic similarity when approaches used different terms. Once we identified constructs, we also extracted the relationships between the constructs in the same manner. Then we designed the BINA conceptual model by assigning a name to each construct and by defining each construct and each relationship. The chapter ends with a discussion about the limitations of the benefits of the proposed conceptual model.

This chapter also focused on the definition and identification of constructs and relationships of cyber resiliency, as discussed in Section 4.3.2. However, estimation and evaluation are also at the core of cyber resiliency approaches. Therefore, the next chapter aims to improve the conceptual model with various metrics commonly used in security risk management and often found in the resources, such as the risk level or event likelihood.

Chapter 5

Delineation of the Cyber Resiliency Management Metrics

In the previous chapter, we defined the BINA model through a conceptual model and related glossary. The conceptual model is in the form of a UML class diagram, composed of a set of classes (constructs of the cyber resiliency domain) and their relationships. However, no attributes (or properties) of these classes have currently been determined. One of the projects linked cyber resiliency needs and measures of an infrastructure and applied them to healthcare systems. Cybersecurity approaches analyse infrastructure and system alignment [158]. To help in this alignment, a core part of cybersecurity approaches relates to risk measurement, incident response, and lessons learned activities. These activities help to evaluate the different constructs of BINA. The related publications of existing approaches propose different sets of metrics [4, 8, 7]. However, they vary with one another. Moreover, they are challenging for users. For example, the users need to read the documentation in its natural language, and thus, there is the potential for different interpretations. This chapter aims to add to the conceptual model, as attributes, the metrics of cyber resiliency.

The two main factors of cyber resiliency, concerning the infrastructure and cybersecurity alignment, are the security level and the value of the assets, as shown, for example, in [159]. We, therefore, aim to improve and automate BINA to reach the best Return On Security Investment (ROSI). The underlying research question addressed here is: what are the metrics relevant to perform cyber resiliency management and to explain the role of ROSI? The domain model improved with metrics can be used as:

- a guideline to identify which constructs to measure for cyber resiliency management and using which metric. Besides, BINA constructs, the introduction of a model to present the different metrics will improve the documentation generally provided in the literature and will help to catch the different metrics.
- a guideline for anyone to define their own set of metrics and incorporate them in a different method or tool. Here it is essential to clarify that we do not want to define a concrete cyber resilience assessment framework with precise metrics, as done in [119, 160]. We aim to identify, at an abstract level, the relevant metrics for cyber resiliency. We have this aim because each user may still want to choose his/her unique concrete approach for resiliency estimation, as set out in the next section, adapted for specific infrastructure and circumstances.

First, Section 5.1 describes the research method used to define the ISSRM metrics. Then, Sec-

tion 5.2 introduces the different concepts and methods used within this chapter. It presents the risk evaluation, the Goal-Question-Metric (GQM) approach and the ROSI concept. Section 5.4 and Section 5.5 demonstrates the application of the two steps of the research method, respectively, which we call metrics elicitation and metrics validation. Finally, Section 5.5 presents the improvement of our domain model with the metrics. The paper ends with its conclusion and future work in Section 5.6.

5.1 Research method

In order to determine the appropriate cyber resiliency metrics, we introduced a research method based on a combination of approaches (cf. Fig 5.1). This research method resulted in the introduction of cyber resiliency metrics as attributes to the BINA conceptual model, originating with their interpretation.

The first approach, used during Step 1 of the research method, is the GQM paradigm [161]. This approach elicits metrics in a top-down fashion, from general objectives to suitable metrics for their achievement. The main benefit of using GQM is that we define metrics focused on the main objectives of BINA. GQM is applied to the cyber resiliency domain. Therefore, the domain model presented in Section 4.4 is an input for this step. The application results in GQM models, leading to the set of cyber resiliency metrics.

The second approach, presented in Step 2 of the research method, is based on cyber resiliency standards and approaches survey. This procedure follows a bottom-up analysis of existing cyber resiliency resources to identify the metrics currently used. The resources are all those examined in Chapter 4 (cf. Section 4.2) that contain a process description and perform constructs' measurement. After excluding the resources dealing only with vocabulary, we first collect and extract the steps related to measurement. In general, to perform this task, we copied and rephrased, where necessary, sentences from the original resources. The rephrase was used to explain the measured constructs and their associated metrics to acquire relevant information. From there, we acquired an overview of how to process each cyber resilience-related resource. The outcomes of this step, for each resource, are:

- a set of its metrics;
- an examination table of the metrics;
- some conclusions for the resource with regards to the final set of metrics.

The attributes in the BINA conceptual model stand for the set of metrics identified for each resource. We present metrics as attributes for simplicity and comparison reasons. Then, we analyse the metrics of the studied resource to those defined through GQM. An examination table summarises this comparison. The examination table sets out the measured constructs of the resource and the relevant metrics. The table also includes their alignment with the constructs of the BINA conceptual model and the metrics gathered through GQM. If a new metric (i.e. one that has not been found with the GQM framework) is identified, it is necessary to evaluate its pertinence. If a deficiency in the GQM study is the source of the issue, then the GQM models may need to be redesigned to incorporate the new issue or to justify the exclusion of a metric. We also provided conclusions about the metrics of the resource and their contrast with regards to our metrics. The tasks composing Step 2 of the research method are performed iteratively for every selected source of the literature.

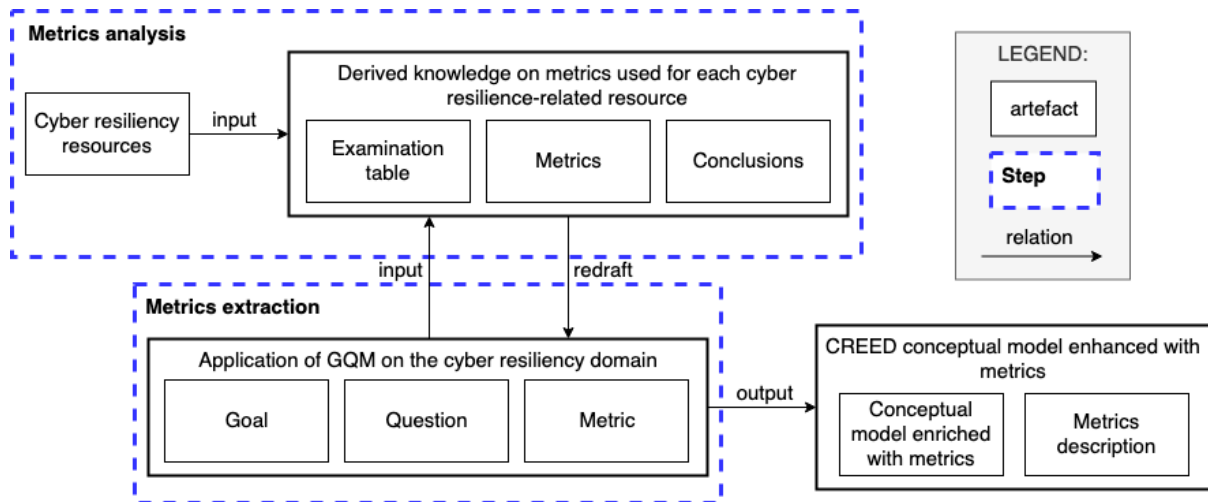


Figure 5.1: Research method for the BINA metrics determination.

To sum up, after the survey of the resources and the formation of the GQM models, we introduced the final set of metrics as attributes of the classes in the BINA conceptual model. Additionally, we offered complimentary explanations, proposed definitions for each metric, as well as an example of their use.

5.2 Theory

In this section, we introduce some theoretical constructs and methods used in this chapter. Firstly, we discuss risk evaluation and its various categories related to cyber resiliency. Secondly, we introduce the GQM approach, used in Step 1 of the research method. Lastly, we discuss the ROSI concept used to identify the underlying objectives that are useful for the actual application of GQM on the cyber resiliency domain.

5.2.1 Introduction to risk evaluation

Risk analysis consists of recognising and evaluating the different risk elements. Regarding risk evaluation, numerous approaches exist [162, 163, 164, 165]. Cyber resiliency resources tend to utilise the same approaches to measure defensive-related constructs. The various risk evaluation approaches belong to one of the following kinds: qualitative, quantitative, or a combination of both, commonly called semi-quantitative evaluation or risk estimation.

Qualitative risk evaluation

Qualitative risk evaluation methods are currently widespread in the healthcare sector [166, 167, 168]. They suggest a scale of levels for the qualitative description of constructs as a means of measurement. These scales have naturally occurring orders, and the difference between them is unknown. An advantage of qualitative estimation is its ease of understanding by the people involved in the evaluation activity, while a drawback is a dependence on the subjective choice of the scale. Examples of qualitative scales for safety and environmental impact are given in Tab 5.1.

Table 5.1: Example of qualitative scale (based on [5]).

Level	Name	Safety impact	Environmental impact
1	Negligible	Minimal injury	Minimal or no impact on the environment
2	Minor	Minor injury	Minor impact on the environment
3	Moderate	Moderate injury	Moderate impact on the environment
4	Major	Major injury	Major impact on the environment
5	Catastrophic	Death	Catastrophic impact on the environment

Quantitative risk evaluation

Quantitative risk management approaches offer a more precise measure for each construct through ratio (i.e. the relation between two constructs proving the number of times one construct includes another construct or the other construct includes it) or absolute scales (i.e. a system of measurement that starts at a minimum, or zero value, and progresses in only one direction). The evaluation's quality depends on the precision and completeness of the mathematical measures and the soundness of the used models. For example, a safety impact will be estimated in terms of each patient's time off work, as depicted in Tab 5.2. Most often, historical incident data of an infrastructure (e.g., hospital, pharmaceutical company, medical lab) or a sector (e.g., healthcare, transportation, energy) is used to provide quantitative suggestions. Naturally, an advantage of such an approach is its accuracy, but it involves high costs, and it can be lacking valuable data to produce meaningful results.

Table 5.2: Example of semi-quantitative scale (based on [5]).

Safety impact	Financial impact	Operational impact
Patient's time off work	Amount of claim in £	Interruption length in hours

Semi-quantitative risk evaluation

In semi-quantitative estimations, ordinal scales are also given to estimate concepts instead of quantitative values. In other words, a quantitative scale (i.e. classification based on values on variables) is reduced to a discrete scale (i.e. variables are measured across a set of fixed values) to become an ordinal scale (i.e. uses labels to classify measurements into ordered classes). The objective is naturally to produce, in a cost-effective manner, more precise results than those obtained by qualitative approaches. However, the evaluation remains naturally less accurate than quantitative evaluation. Particular care should be given to the definition of the scales to keep relevance in the equivalent levels and obtain helpful information about the relative criticality of the studied constructs. Examples of semi-quantitative scales are offered in Tab 5.3.

5.2.2 The GQM approach

The importance of measurement for management is well known. For cyber resiliency, the existence of metrics will allow:

- the determination of the strengths and vulnerabilities of the current processes and plans (e.g. what is the recurrence of certain types of incidents?);

Table 5.3: Example of semi-quantitative scale (based on [5]).

Level	Name	Safety impact	Financial impact	Operational impact
1	Negligible	No time off work required	Risk of claim remote	Loss/interruption of >1 hour
2	Minor	Requiring time off work for <3 days	Claim less than £10,000	Loss/interruption of >8 hours
3	Moderate	Requiring time off work for 4–14 days	Claim(s) between £10,000 and £100,000	Loss/interruption of >1 day
4	Major	Requiring time off work for >14 days	Claim(s) between £100,000 and £1 million	Loss/interruption of >1 week
5	Catastrophic	Death, permanent injuries or irreversible health effects or impact on large number of patients	Claim(s) >£1 million	Permanent loss of service or facility

- the provision of a reason for choosing or updating a resiliency approach (e.g. what is the impact of the resiliency mechanism A on the safety of the healthcare process B?);
- the evaluation of the quality of specific cyber resiliency processes (e.g. what is the incident density in a specific healthcare system after deployment?).

As its name indicates, the Goal-Question-Metric (GQM) approach is used to determine metrics based on assessment questions and goals [169]. In other words, GQM defines a metric based on a top-down procedure. This structure concerning this project assumes that for a healthcare infrastructure to access its cyber resiliency, we must specify the goals of the process/department/project and then trace those goals to the means intended to operationalise them. A guide is required to support the interpretation of the outcomes concerning the stated goals.

A GQM model forms a hierarchy of goals sharpened into questions honed into metrics [161]. The definition of a goal as an object is the initial conceptualisation. From there, the formation of a set of questions takes place. These questions relate to the assessment of achieving a goal and to the attempted way it is achieved. At the third level, the identification of a set of data associated with every question takes place. Fig. 5.2 depicts the generic structure of a GQM model.

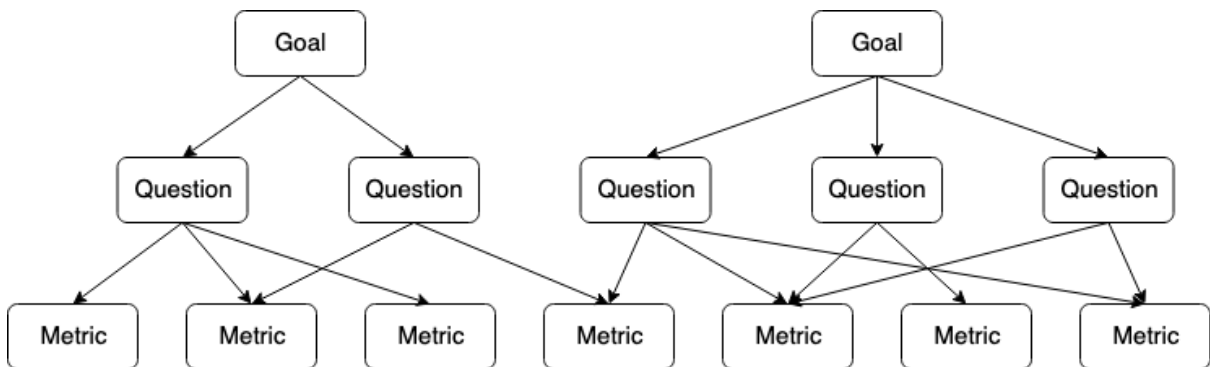


Figure 5.2: Generic structure of a GQM model.

5.2.3 On the definition of ROSI

There is no precise agreement about the perception of Return On Security Investment (ROSI). However, two approaches are the most used. One of them relates to cybersecurity costs to define ROSI [170], whereas the other focuses on incidents [171].

$$ROI = \frac{\text{Gain from investment} - \text{Cost of investment}}{\text{Cost of investment}}$$

This first definition involves expected returns (gain from investment), while the second definition, presented below, involves the loss expectancy before and after security solutions. Also, the second definition calculates ROSI for the fixed time of a year, while the first definition can be used on any period of time, based on the user's preferences.

$$ROSI = \frac{\text{Annual Loss Expectancy} - \text{modified Annual Loss Expectancy} - \text{Cost of the Solution}}{\text{Cost of the Solution}}$$

where:

$$\text{Annual Loss Expectancy} = \text{Annual Rate of Occurrence} * \text{Single Loss Expectancy}$$

$$\text{Return on Security Investment} = \frac{\text{Monetary Loss Reduction} - \text{Cost of the Solution}}{\text{Cost of the Solution}}$$

Therefore, to compare both definitions, we need to use the same time period of a year, which means that we will bind the first definition to one year to comply with the second definition. It also means that the expected returns of the first definition may be defined, over a given time period, in terms of a difference of loss. The expected returns are the loss expectancy before the security solution minus the loss expectancy after the security solution.

From the above, it becomes apparent that conventionally, cybersecurity budgets are evaluated by the return on investment (ROI). However, this approach has some undesirable side effects as the goal becomes an investment and not the missions that cybersecurity and resiliency want to achieve. This approach also excludes the sociotechnical character of cybersecurity and resiliency issues. There is no inquiry about return on investment for other IT aspects. This observation makes researchers question why ROI should be used for cybersecurity.

Fowler et al. [171] proposed a new way to evaluate cybersecurity investment decisions and measure the progress and effects of the investments and projects. They proposed to measure the progress of cybersecurity expenses against a plan. The plan should include all the cybersecurity phases, including resiliency goals and relate them to cybersecurity expenses (people, process, technology) to meet business objectives. To design artefacts relevant to this research direction, we needed to use the existing indexes and design relevant metrics based on known frameworks and, in particular, using the Goal-Question-Metric (GQM) framework.

5.3 Use of the GQM framework on the BINA domain

As presented in section 5.2.3, independently of how ROSI is defined, to achieve the best ROSI (which is the highest value of ROSI), it is necessary to:

1. Maximise the difference between the loss expectancy before incident response and the loss expectancy after incident response;
2. Minimise the cost of investment.

Regarding the BINA domain, the difference between the loss expectancies is related to the incident impact and its reduction. While the cost of investment is related to the costs from the application of CCoA (including the constructs CIRP and security control). These assumptions provide two aims for the GQM study, which are respectively the two roots of the GQM models (cf. Fig. 5.3 and 5.4):

1. Maximise the incident impact reduction
2. Minimise the incident response cost

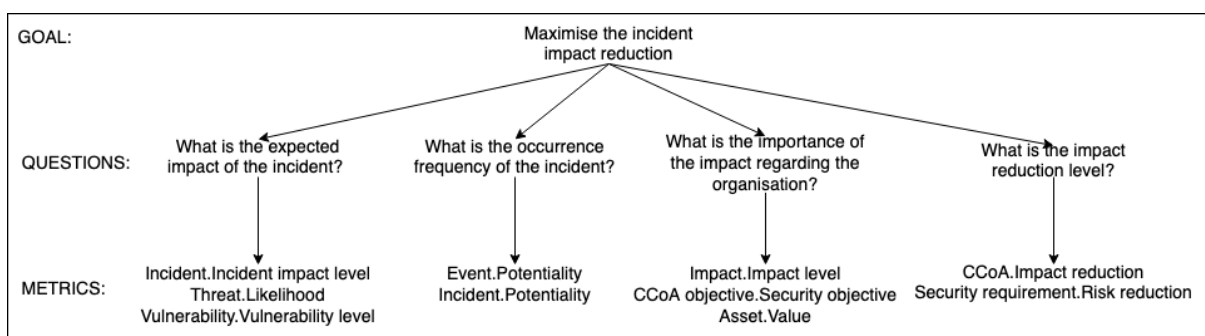


Figure 5.3: GQM model for the first aim.

With regards to the constructs of the BINA domain model, to maximise the risk reduction involves first knowing *what the expected impact of the incident is likely be*. The incident impact depends on an incident's *frequency of occurrence* and its *significance for the organisation*. It is also necessary to know *what the impact reduction is*. From the questions and the constructs of the BINA domain (cf. Fig. 4.4), related metrics are proposed. The GQM model (cf. Fig. 5.3), represents these metrics as attributes of a construct, with the following notation: *Construct.Metric*.

The first metric is the *Incident impact level* and is naturally associated with the concept of 'incident'. The impact of an incident is also associated with the occurrence frequency of the incident. It is depicted in the causal part of the construct of threat in the domain model and *Vulnerability level* of the vulnerability construct. The occurrence frequency of incident is summarised in the *Potentiality* metric in the event and incident constructs.

The risk importance is depicted in the consequence part of the incident, represented by the concept of impact. The *Impact level* is the metric measuring the importance of impact. The risk importance is also related to the intrinsic *Value* of organisational assets. A new concept, motivated by the need for a metric, is introduced in the domain model to describe the risk importance. This concept is named the 'security objective'. It expresses the application of security criterion on a business asset. This construct is needed because it is necessary to estimate the security need for each security objective to describe the risk importance completely. This metric is a crucial indicator to estimate the actual impact on the organisation and thus the risk importance regarding the business.

Finally, risk reduction, *Risk reduction level* shall be estimated for each incident response and security objective. The security constraint concept cannot be estimated in terms of incident impact reduction. The explanation is obvious when illustrated with an example. Let us consider

that the security objective "Perform network filtering" is implemented by the security constraints "Firewall" and "Perform firewall maintenance". It is impossible to allocate an incident impact reduction level to security constraint "Perform firewall maintenance" taken alone. The incident impact reduction estimation is only viable on incident response and security objective.

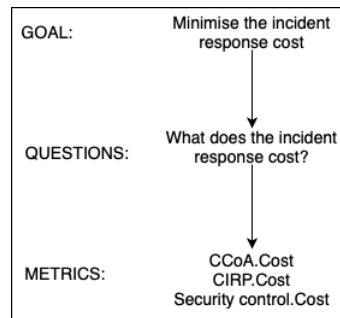


Figure 5.4: GQM model for the second aim.

The second aim of minimising the incident treatment cost involves fewer concepts and, thus, fewer questions. Only one related question is necessary: *what is the cost of the incident response?* Regarding the associated metrics, we know from the domain model that three risk treatment-related concepts are involved. A *Cost* metric is thus proposed for each of them to know their own value (cf. Fig 5.4).

It is necessary to note that, for clarity, the GQM models presented in Fig. 5.3 and 5.4 are those obtained after the last iteration of Step 2 (Figure 5.1). They thus represent the final set of metrics. Further explanations about each metric is provided in Section 5.5.

5.4 Examination of BINA approaches for metrics validation

The references surveyed for the metrics validation are all cyber resiliency sources containing a process description. In order to be able to measure cyber resiliency, we needed to use resources that offer a process for resiliency as this is what we intended to assess and consequently measure with the use of metrics. Therefore, cybersecurity standards [140, 141, 142, 143, 144] and health-related standards [145, 146, 147] are not analysed in this subsection, as they focus on the contextual and conceptual aspects of BINA. We have already extracted from these resources the relevant information for the domain model, but the same resources do not offer any attributes on those concepts that we could interpret as metrics and hence we had to exclude them from the metrics validation process.

Instead, we retain cyber resiliency standards [6, 4] and frameworks [7, 8]. Except for concepts and relations, these standards and frameworks further offered metrics to analyse resiliency processes. The study of each such resource results initially in the extraction of metric-related elements. Using these elements as a base, we do the following:

- construct the metric analysis table;
- enrich the BINA with the metrics extracted from the relevant resources;
- examine the compliance of the metrics elicitation process with regards to the GQM study (cf. Section 5.2.2).

5.4.1 Cyber resiliency standards

We start the analysis from the two cyber resiliency standards, namely NIST SP 800-184 [6] and NIST SP 800-61r2 [4]. Initially, we present the artefacts produced for each of these two standards. Consecutively, we provide their corresponding metric analysis tables.

NIST SP 800-184

As described in the research method (cf. Section 5.1), we first collect all the metrics used throughout the cyber resiliency standard NIST SP 800-184 [6]. Below, we describe the steps of the cyber resiliency standard involving constructs estimation, using the following conversions: *metrics* are in italic, and **associated constructs** are in bold. To enable traceability, we also provide the page number of the cyber resiliency standard.

- Assessing **incident** damage and *cost* (both direct and indirect) [6, p. 20]
- Expressing the organisational **risk** assessment *improvement* [6, p. 20]
- Estimating the *quality* of **Cyber Course of Action (CCoA)** [6, p. 20]

The preceding kinds of recovery metrics are displayed more analytically in Tab. 5.5. The two first columns are for the constructs of the BINA conceptual model and the constructs of the studied method. This alignment is a reminder of the one of Tab. B.2 in Appendix B. The two following columns depict the associated metrics of the studied method, as called in the method, and the associated metrics in the of the BINA domain model. Next, a column named 'definition' shows how this metric is determined or measured. For example, if the user can define a metric on a scale, this column indicates 'user-defined' for this metric. In another instance, if the metric has to be determined by other metrics or tools (e.g., matrix, specific software, confidential algorithms), this is stated in this column. The last column is named 'Unit', and if the metric is quantitative, its unit will be represented (e.g., £, hours, days). Otherwise, the proposed scale is listed.

Table 5.4: Metrics analysis table for NIST SP 800-184 [6, p. 20]).

BINA concept	NIST SP 800-184 concept	NIST SP 800-184 metric	BINA metric	Definition	Unit
Incident	Incident, recovery damage and cost	Monetary value	Value	User defined	User defined
Risk	Organisational Risk Assessment Improvement	Risk level	Risk level	f(Incident, Impact)	User defined
Cyber Course of Action (CCoA)	Quality of Recovery Activities	Effectiveness		Risk reduction	User defined

Fig. 5.5 summarises the metrics proposed by NIST SP 800-184 an used to enhance the BINA domain model (cf. 4.2).

NIST SP 800-61r2

Assessment in NIST SP 800-61r2 focuses on the concept of the 'incident' (Tab. 5.5). More specifically, NIST SP 800-61r2 [4] introduces four types of metrics for incidents. These metrics estimate the incident response capability and effectiveness. According to NIST SP 800-61r2 [4],

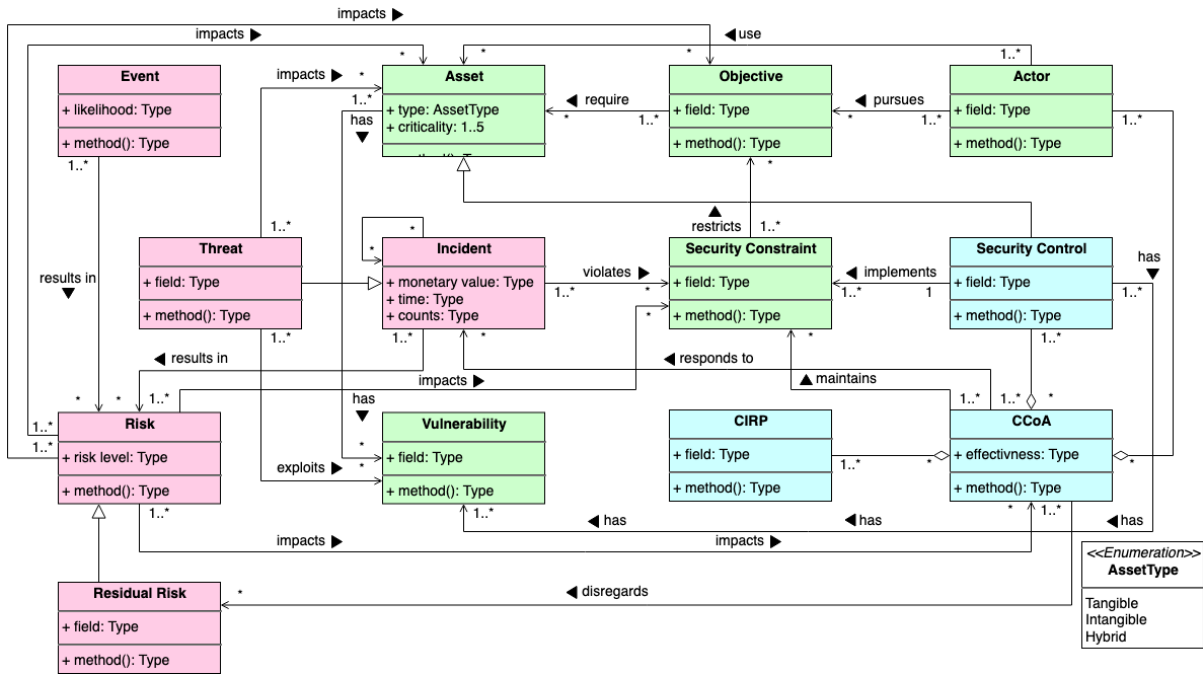


Figure 5.5: The BINA domain model enhanced with the metrics proposed by NIST SP 800-184

organisations should choose the appropriate metrics based on their reporting requirements and investment assessment systems. The focal point of all these metrics is that they are actionable. In other words, the metrics chosen by each organisation will be actionable for them. Not all metrics need to be used by organisations.

NIST SP 800-61r2 [4] metrics assess the overall number of incidents and also each incident. They cover the width of incidents with the overall **Number of Incidents Handled** metric and also the depth of each incident with the metrics of **Time Per Incident; Objective and Subjective Assessment of Each Incident**. These metrics of the NIST SP 800-61r2 [4] are:

- Produce *counts* the **incidents** under review, ideally for each incident category [4, p. 40].
- Measures the *time* of each **incident** (e.g., labour spent; elapsed time to each to each stage of the incident handling process; how long it took the IRT to respond to the initial report of the incident; how long it took to report the incident to management and, if necessary, appropriate external entities) [4, p. 40].
- Calculates the estimated *monetary damage* resulting from the **incident** [4, p. 41].
- Estimates *how effectively* **Cyber Course of Action (CCoA)** performed [4, p. 41].

Table 5.5: Metrics analysis table for NIST SP 800-61r2 [4, p. 40-41]).

BINA concept	NIST SP 800-61r2 concept	NIST SP 800-61r2 metric	BINA metric	Definition	Unit
Incident	Incident	Counts	Potentiality	User defined	User defined
		Time		User defined	User defined
		Monetary damage		User defined	User defined
CCoA	incident response	Effectiveness		User defined	User defined

Cyber Course of Action (CCoA) is used instead of Cyber Incident Response Plan (CIRP) here because it contains actors (i.e., IRT) that can assess themselves. Moreover, CCoA covers CIRP in the context of NIST SP 800-61r2. Overall, both constructs use the same metric, which suggests that either of them can be used at this stage. However, it is not meaningful anymore to use two constructs with the same metric, and thus we use one of them to express the newly introduced metric.

5.4.2 Cyber resiliency frameworks

The analysis continuous with the two cyber resiliency standards, namely MTR140499R1 [7] and MTR110237 [8]. As we did in the previous section, we present the artefacts produced for each of these two standards below. Consecutively, we provide their corresponding metric analysis tables.

MTR140499R1

The measurements related to MTR140499R1 [7] are in the form of guidelines. These guidelines are for security engineers and architects that need to select cyber resiliency techniques. The measurement steps of the MTR140499R1 [7] are:

- Determine the *maturity* of **security controls** for cyber resiliency application of different implementation approaches [7, p. 19].
- Set the *risk level* throughout the cyber attack life-cycle determining the attack **risk** [7, p. 19].

Table 5.6 summarises the different concepts measured and their associated metrics. MTR140499R1 suggests the consideration of the relative maturity and readiness for security controls of different implementation approaches. MTR140499R1 addresses the importance of considering risk at the different stages of Advanced Persistent Threats. Throughout the cyber attack lifecycle, different risk levels and hence resilience and response techniques will adjust accordingly. The various concepts in MTR140499R1 are estimated in qualitative values. Table 5.6 sets out these units, which the framework recommends to adapt depending on the context.

Table 5.6: Metrics analysis table for MTR140499R1 [7]).

BINA concept	MTR140499R1 concept	MTR140499R1 metric	BINA metric	Definition	Unit
Security control	Cyber resiliency technique	Maturity Readiness		User defined	User defined
Risk	Advanced persistent threat	Effect	Risk level	Risk level= f(Threat level, Vulnerability level, Asset value)	Scale

MTR110237

MTR110237 [8] does not define metrics for resilience engineering. Instead, it recognises the need to measure cyber resiliency and enables an organisation to select a set of cyber resiliency metrics that adequately cover their cyber resiliency domain. The suggested metrics are:

- Stipulate the *time period* of the **vulnerability** [8, p. 60].
- Determine the *time* of **Cyber Incident Response Plan (CIRP)** [8, p. 60].
- Set out the *likelihood* of **threat**, considering that there will be cases of false positives (i.e., detection of threats that do not exist) and false negatives (i.e., failure to detect threats that do exist) [8, p. 60].
- Establish *availability time* of the **objective**, where the term 'objective' stands for the service [8, p. 60].

Table 5.7: Metrics analysis table for MTR110237 [8]).

BINA concept	MTR110237 concept	MTR110237 metric	BINA metric	Definition	Unit
Vulnerability	Vulnerability	Time period		User defined	User defined
CIRP	Cyber resiliency	Time		User defined	User defined
Threat	Fault	Likelihood	Likelihood	User defined	Very Low, Low, Medium, High, Very High
Objective		Availability time		Priority=f(cost, effectiveness)	Rank

The set of metrics discussed in MTR110237 [8] come from different sources and are not necessarily the only ones that can be used to cover the cyber resiliency engineering domain. Instead, they are samples of current work. However, the existing cyber resiliency metrics are subject to challenges. Firstly, security and resiliency have to be measured for complex systems. The systems' complexity makes the definition of metrics for security and resiliency and analogous capabilities and functions more difficult. Secondly, cyber resiliency is commonly measured within the context of mission. Cyber resiliency metrics are therefore interpreted and assessed in a context that may have high or low granularity. Thirdly, a metric needs to be reproduced in a repeatable way. Also, any evaluation has associated cost and availability issues related to the gathering of relevant data. Thus the feasibility of a metric needs to be evaluated on a case by case basis [172].

5.5 Enhancement of the BINA conceptual model with metrics

Elicitation (Section 5.3) and validation (Section 5.4) of the metrics result in the enrichment of the BINA domain model, by completing it with the BINA metrics. The metrics are reported in the domain model under the form of attributes. The resulting BINA domain model is presented in Fig. 5.6.

The first modification of the BINA domain model is the removal of residual risk. This construct can be modelled as instances of risk without connections to a security control or a CIRP. For example, the risk of *need for ongoing resource commitment-economic challenge* has no 'addressed' relation with a CIRP *outsourcing*. It is also relevant to determine the value of the assets. Actors use assets as they pursue objectives that require them (cf. Fig. 5.6). The value of assets is used as an input to estimate the security constraint need of each asset, e.g., in terms of confidentiality, integrity and availability. An asset with a high value may generally have a higher security constraint need than an asset with a low value in the organisation's business. For example, a new vaccine patent is estimated to have a higher value than the file of

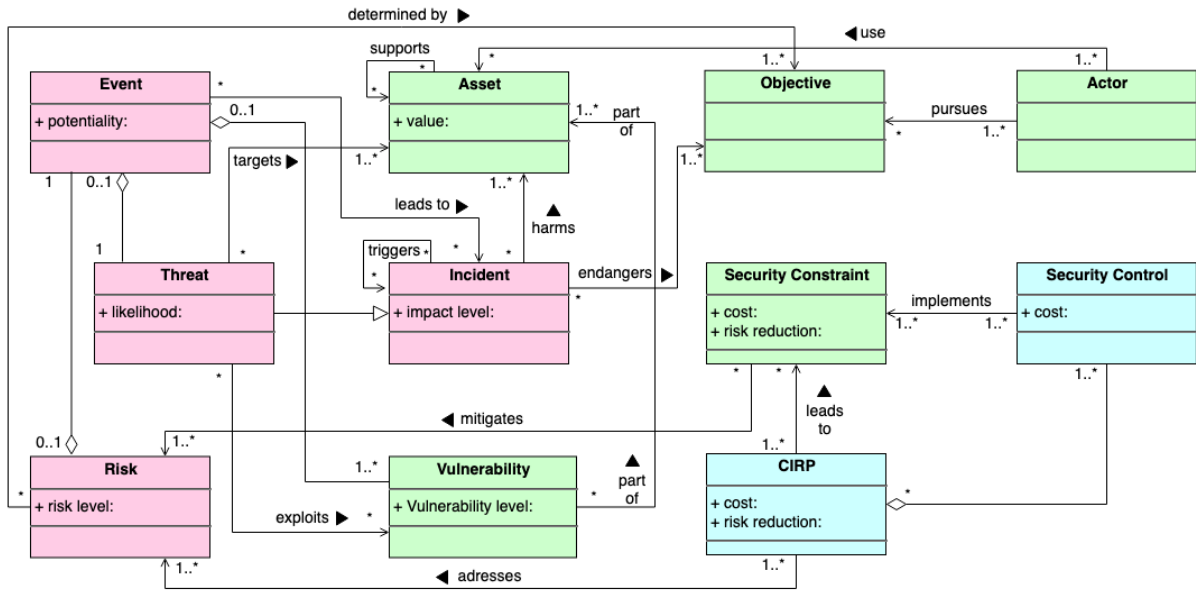


Figure 5.6: BINA domain model enhanced with metrics

clients of the organisation. Both need to be confidential. Consequently, the security objective "confidentiality of new vaccine patent" has a higher security need than "confidentiality of the file of clients".

Example: The process of vaccine patent design has been identified as an asset. Its value is considered very high for a pharmaceutical company. Now the security need of this asset is determined for each selected security constraint. On a scale from 1 to 4 its confidentiality is estimated as 4, its integrity as 3 and its availability as 2. Not disclosing confidential patent designs to competitors is seen as major, compared respectively to the integrity of the designs and their availability. Even though they are less critical, they are also to be examined.

For risk-related concepts, the risk is estimated by its level. The risk level depends on the event potentiality and the impact level of an incident occurring. These two constructs compose the risk. The event construct is composed of threat and vulnerability. Their respective levels are estimated through likelihood and vulnerability levels.

Example: A social engineer can penetrate the pharmaceutical company's building to steal a copy of a new vaccine patent. Regarding the context (motivation for patent theft, exposition of the building), the likelihood of such a threat is estimated as 2 on a scale going from 1 to 3, i.e. this threat can happen sometimes. A set of vulnerabilities is highlighted, regarding this threat, like the lack of physical access control. The total vulnerability level is estimated at 2 on a scale from 0 to 3, i.e. the vulnerability is high because no effective security control is in place. Based on these two levels, the potentiality of the event is estimated at 3 on a scale from 0 to 5. The impact coming from this event, directly related to the security objective of confidentiality of vaccine patents, has a level 4. Finally, the risk level is estimated at 12, based on the potentiality of the event and the impact level.

In incident response-related constructs, CIRP and security constraints are estimated in terms of risk reduction performed and in terms of cost incurred. As discussed in Section 5.3, security controls can be estimated in terms of cost (i.e., cost of buying a firewall, cost of maintaining it by a security officer). The risk reduction metric of some security controls taken alone has no merit. For example, the risk reduction of the security officer maintaining the firewall cannot be estimated alone without considering the general effectiveness of the firewall. However, the risk reduction metric applies to the CIRP. If the risk is transferred, a residual risk can

remain even after a response plan has been put in place. This leads to a degree of risk reduction that needs to comply with associated security constraints. For risk acceptance, the risk reduction is equal to 0, the risk being accepted as it is. The risk is withdrawn for risk avoidance, so the risk reduction metric can no more apply.

It is essential to mention here that the risk reduction and cost metrics are not directly derived from one another. The cost of a CIRP is not the cost of the total cost of security constraints, and similarly, the cost of a security constraint is not the total cost of the related costs. As seen in the domain model, a security constraint can be used in several CIRP. For instance, a security constraint like "users access restricted according to access control policy" can be used to reduce external and internal threat actors. The same applies to CIRP, which can be used to implement several security constraints. Defining a function, like relating the cost of CIRP and the cost of security constraints, is not relevant for this context. Each user can define their function relating to the different CIRP metrics. For instance, if the cost is estimated quantitatively, the cost of a security constraint composed of two controls could sum the cost of the two controls. Whereas, if the cost is estimated qualitatively, the security constraint control can be a qualitative approximation of the two related security controls. Similarly, the risk reduction metric can be estimated.

Example: A pharmaceutical company decides to reduce a risk with the use of relevant controls. The security constraint "protection of secure areas where only authorised personnel has access" is decided. The pharmaceutical company has decided to use entry detectors and access badges for that purpose. The total monetary cost is £7000. A CIRP requiring only this constraint can also have a total cost of £7000. As for the risk reduction metric for both the security constraint and the CIRP, it can have a value 8 because the new risk level, reviewed based on the updated vulnerability level is 4.

5.6 Summing-up the BINA metric elicitation

The purpose of this chapter is to recognise and determine a set of metrics for the cyber resiliency domain. The research method for the extraction of these set of metrics needs to be careful and systematic. For that reason, we combine two complementary approaches. Firstly, the GQM approach is used to elicit the different metrics through a focus on the objectives of the cyber resiliency domain, i.e. reaching the best ROSI. Then, we review the metrics proposed in the literature. In this way, we move towards a more exhaustive metric elicitation regarding current cyber resiliency standards and methods used to attain similar objectives. It is important to note that the metrics proposed are at an abstract level. Based on the objective and granularity level wanted from a method, the implementation of metrics can differ. The metrics can be implemented differently within a method qualitatively/quantitatively or through several metrics. For instance, the likelihood metric of a threat can be considered in terms of the static probability of natural threats (in %) or the qualitative evaluation of human misbehaviour. This example shows that implementing these metrics requires an understanding of the context and aim of their usage. In this way, their implementation will think about the best way of using them, depending on the objective and the granularity level wanted. Therefore, the proposed set of metrics has to be considered with an implementation variability.

In this chapter, the elicitation metrics are validated through literature analysis. To acquire a concrete instantiation and validation of their relevance, their testing in a real case is essential. In Chapter 8, the metrics are used in the framework of an ISO/IEC 27001 certification. There BINA is at the core of the standard. An instantiation of these metrics is offered, and feedback is given with regards to their use.

5.7 Discussion and Closing Remarks

In this chapter the BINA domain model was improved by the metrics used in BINA in order to reach the best ROSI. The metrics were represented as attributes of the conceptual model and defined through a glossary.

Firstly, we presented the research method used to define relevant metrics. Subsequently, the theory of different constructs and approaches used to identify them were presented. This included the risk estimation, the GQM method and the definition of ROSI. The research method followed consists of two main steps. The first step is the application of the GQM method to the BINA domain model. This step results in a set of metrics needed to perform incident response and reach the best ROSI. The second step is the validation of the metrics based on the relevant literature that focuses on measuring similar constructs. In this way, the GQM application for BINA was reviewed iteratively, based on the outputs gained from the second step. Lastly, the BINA domain model was enhanced by a set of metrics defined through the application of the research method. Then conclusions were presented.

After defining the BINA domain model enhanced with metrics, the aim is to compare it with the existing security and incident response modelling languages. In the following chapter, we delve into the assessment of various security modelling languages with regards to the constructs of the BINA domain model.

Chapter 6

Assessment of the BINA by using Security and Incident Response Modelling Languages

This chapter will compare security modelling languages with the BINA domain model. These languages are KAOS extended to security [50], Misuse cases [32] and Secure Tropos [33]. The research question of this chapter is *how is incident response supported by security languages, and is there a need for enhancements*. The main anticipated outcomes are:

- Evaluation of the hypothesis that the existing security languages overlook incident response;
- Assessment of the coverage of existing modelling languages to BINA constructs;
- Identification of enhancements to be made to the languages to make them suitable for incident response.

The scope of this research project is limited to cyber resiliency during early requirements engineering (Section 1.3.1). Thus, we are not considering languages used in later stages of the life cycle (i.e. SecureUML, UMLsec). Within the scope of this research, we assess KAOS, Misuse cases and Secure Tropos. We chose these modelling languages because (i) they focus on eliciting security requirements from the early stages of a system's development; (ii) they capture incidents and system requirements from a sociotechnical perspective; and (iii) they offer a semantic and syntactic representation of the security domain which makes them comparable with the BINA domain model as designed based on the literature. After examining and analysing these languages, we found that Secure Tropos was the language that better distinguishes the BINA constructs, offers the most coverage of the syntactic and semantic elements of the BINA domain model and is extendable and consequently can incorporate cyber resilience-related entities. Thus, we provide adjustments for Secure Tropos. A complete assessment of all the relevant languages remains as future work.

Section 6.1 explains the research method applied for language assessment. It is used from Section 6.2 to 6.4 to report assessment of KAOS, Misuse cases and Secure Tropos. Section 6.5 summarises the results and presents an assessment of the languages. Then cyber resiliency-aware Secure Tropos is presented in Section 6.6. Finally, the conclusions of this chapter are in Section 6.7.

6.1 Research method

The result of languages assessment is the alignment of constructs of the security-oriented modelling language and the BINA domain model. This alignment shows the construct coverage of BINA by each language (Fig. 6.1). Each language examined has a purpose, meta-model and textual documentation. We use the BINA domain model as a reference for language comparison.

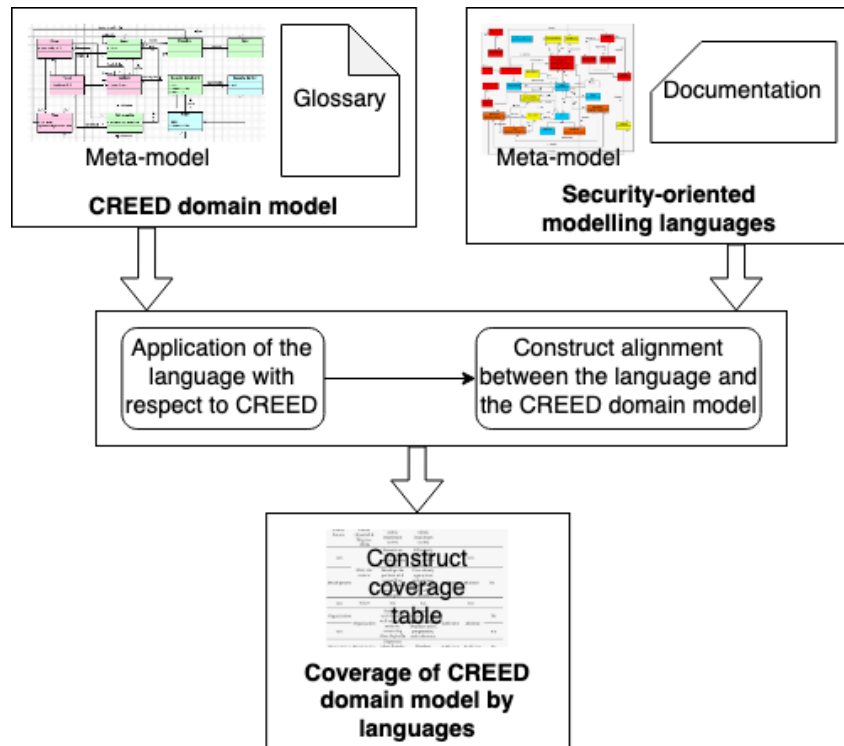


Figure 6.1: Research method applied for the assessment of BINA support by security modelling languages

For each language, we need to use a running example to explain the alignment of the language with regards to the BINA domain model. The running example will illustrate the use of the language to address the security risks during the early stages of systems development. We then consider how the constructs of the language are used to address BINA constructs. Next, we perform the alignment focusing on constructs definition and the relationships between them. This step is performed incrementally by iterative analysis of the textual documents and the meta-model. The artefact produced is a table highlighting the lack in each existing modelling languages to support BINA. In this table, for each BINA construct, we gather the synonyms found in each language's literature. Then, we identify the modelling construct of the security-oriented meta-model used for representing the BINA construct. Finally, the last column illustrates the constructs with some examples extracted from the running example.

It is crucial to clarify that the alignment does not represent equivalence between a security language construct and the BINA construct. We highlight only the support provided by the language to model BINA. On the other hand, no information is given about how the construct of a security language is mapped/represented in the BINA domain model. For example, Section 6.3 shows that, in Misuse cases, an actor can be used to represent a BINA threat agent. However, it does not mean that the construct of an actor is strictly equivalent to the construct of a threat agent: actors can represent regular agents performing a task in the organisation, like

an engineer or a microbiologist, for example.

6.1.1 Running Example

Pharma Invent is a (fictitious) pharmaceutical company in the healthcare domain. It is a Small and Medium Enterprise (SME) located in Ireland and has 30 employees. Its activity is based around the production of differentiated, high-quality and needed healthcare products. Pharma Invent specialises in designing vaccines and the development of clinical diagnostic testing for healthcare providers and countries. Pharma Invent aims to improve the quality of its products and the efficiency of its production processes utilising new technologies.

The company is composed of five departments. The strategic direction of the company comes from the managerial department. The secretarial department is handling office tasks, supportive to the other departments. The sales department communicates and maintains clients' records. The scientific department designs healthcare products, and the finance department handles administrative, legal, compliance and financial processes.

The information systems infrastructure of Pharma Invent consists of 14 computers in the scientific department, 4 in the sales department, 2 in the administration department and 2 in the secretarial department. The management has 2 laptops. All computers are connected to a local Ethernet network. A printing server and a file server are available for the whole company. Every service is connected to the Internet. Office software is used on each computer. Ecogreen software is used for the management of sales, Cytel is used as epidemiological computing software, EpiTools is an R package for epidemiologic computing and graphics, OpenClinica is an open-source clinical trials software, and NetSuite Manufacturing Edition offers an integrated platform for accounting and the financial department.

6.1.2 Generic security requirements process

Security requirements elicitation activities usually follow an overall process composed of general steps used in security requirements engineering methods. However, overall the different approaches do not put the same weight on the activities performed. After all, this is one of the aspects that make each approach unique. The overall security requirements elicitation and analysis process is illustrated in Fig 6.2 as a UML activity diagram.

Step 1: Determination of context and assets The process starts with a study of the company's context and the identification of its assets. In this step, the company and its environment are described, focusing on the sensitive activities related to cybersecurity. The existing information system is defined.

Example: From the Pharma Invent activities presented in Section 6.1.1, we take vaccine testing data as an asset that should be protected. At the level of information systems, such data are created by vaccine researchers on computers connected to the Internet.

Step 2: Determination of security goals At this step, the security needs of the company are determined. The security goals are elicited through asset identification and their importance for the company. Security goals are commonly determined in terms of confidentiality, integrity, availability, privacy, non-repudiation and other properties of the assets.

Example: During the collection, the vaccine testing data should be kept confidential

Step 3: Assessment and analysis of risks The third step of the process is risk analysis,

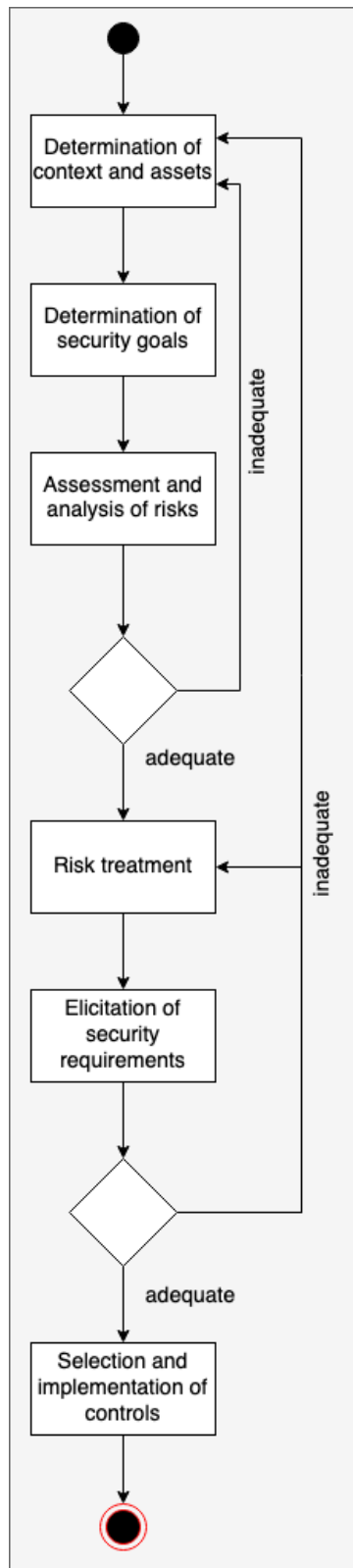


Figure 6.2: Security requirements elicitation and analysis process

eliciting which risks can impact assets and threat security goals. Crucial at this step is the identification of risks and estimation of their level either qualitatively or qualitatively. The risk level is evaluated against the security goals determined during the second step of the process (cf. Step 2). It could be necessary at this step to thoroughly review the context and asset

identification if the risk assessment is considered unsatisfactory. In that case, an iteration of the previous two steps can take place.

Example: A competitor of Pharma Invent can try to use conventional operating system and network protocol weaknesses to penetrate on the computer of an employee, where are stored some confidential vaccine testing data. This risk has an estimated level that is adequately high to be thought through further.

Step 4: Risk treatment After having assessed potential risks, risk treatment decisions can be made at this step. Risk treatment measures can include avoiding (not getting involved in, or act to withdraw from, a risk situation), reducing (taking actions to reduce the probability, negative results, or both, associated with risk), transferring (sharing with another party the responsibility of loss caused by a risk) or retaining risk (acceptance of the weight of loss from a specific risk). The decision is commonly based on the cost-effective assessment between risks and risks treatment.

Example: Pharma Invent can choose to decrease the risk of an operating system vulnerability with a security control such as vulnerability update policy suitable for the information systems used from the vaccine researchers.

Step 5: Elicitation of security requirements Security requirements on the information system can be expressed as security constraints on other goals that mitigate risks. This is the case when the risk reduction has been decided. However, security constraints can emerge from other treatments, like, for example, risk transfer generally needing some constraints on the third party. At the end of the risk treatment step, followed by the security constraints definition, if they are considered unsatisfactory, the risk treatment step can be revised, or all of the preceding steps can be reviewed from the definition of the context and the relevant assets.

Example: The following security requirement has been chosen to be implemented on the Pharma Invent's information system: Procedures for monitoring the use of vaccine data processing should be established, and the results of the monitoring activities need to be reviewed regularly.

Step 6: Selection and implementation of controls Requirements are implemented using security controls, i.e. system-specific countermeasures, that are implemented within the organisation.

Example: A firewall and an Intrusion Detection System (IDS) are selected and implemented within the Pharma Invent's information system.

As highlighted by the two decision points of the process, the process is iterative. It should be performed as many times as necessary until reaching an acceptable level for all risks, also considering new risks emerging after security control determination and occurrence of incidents. The risk remaining after applying the security measures is referred to as 'residual risk'. Only the main steps are depicted in the process, but others are possible and proposed within the different approaches. As a risk management process is taking place, some other parallel processes are also generally suggested. For example, a process for risk communication can guarantee effective communication among stakeholders and affect their decisions. This process helps stakeholders to understand the organisation's risk management process and its results. Risk monitoring and review is another crucial process. After reaching an acceptable level for risks, the risk management process should be monitored and regularly reviewed as risks are not static. Ideally, the risk management process should be continuously performed to keep the organisation's operations and its associated security requirements aligned with the measures taken and the appropriate security level.

6.1.3 An overview of Security and Incident Response Modelling Languages

In this section, we offer a brief overview of security and incident response modelling languages and their suitability to be included in the BINA domain model evaluation.

Business Process Model and Notation (BPMN) [173] is a common technique used for business process modelling. It has a syntactic and semantic structure that allows the instantiation of business processes in Business Process Diagrams. BPMN focuses on business processes, and as such, it relates closer to a system's implementation stage. Furthermore, it focuses on business functions and not system properties. These aspects of BPMN indicate that even though it is widely used and has been extended to represent security and risk constructs, it is not relevant with the BINA domain model as it does not address the early stages of a system's requirements elicitation and analysis. BPMN is not suitable for evaluating the BINA domain model for these reasons.

The cyber security modelling language (CySeMoL) [174] allows quantitative analyses of the cyber security of enterprise architectures. It allows the instantiation of entities associated with known attacks and countermeasures. These entities are further enhanced with true or false attributes that form the likelihood of occurrence. However, this modelling language focuses on technical aspects of systems and attacks and has an extensive notation more specific to cyber security than a domain in which the system might operate. The constructs are particular, and if compared with the BINA domain model, most of them will correspond to three constructs like entity, event and security control. Additionally, cyber resiliency constructs would have to be analysed based on current practices with limited space for future or real-time adjustments of these approaches, as the modelling language has a low-level granularity that will need to be adjusted every time from a user to make the language expressive. Also, the visual representation is not simplified to enhance understanding. Hence, we decided that using CySeMol to evaluate the BINA domain model will not be suitable.

Knowledge Acquisition in autOMated Specification (KAOS) [175, 176] is an approach that uses a metamodel and instantiates it for a particular system. It offers a conceptual model, a process and guidance on acquiring requirements. It has a well-defined terminology and examples of how the structured language can be used for automation. KAOS has a sociotechnical perspective as it is based on goals and covers security and resiliency aspects because it can represent the system's goals for robustness, safety, and consistency. Thus, we conclude that is an approach that can be used to evaluate the BINA domain model.

Misuse cases [32] are a method of modelling system behaviours that are unwanted. In this way, misuse cases represent requirements of aspects that should not materialise for a system-to-be., that is, behaviours that should not occur in a system. Within the cyber security context, misuse cases are used to represent attacks against a system that can lead to unwanted system behaviours. Misuse cases describe requirements at a high level and are based on semantic and syntactic definitions. This means that they are easy to communicate and analyse before implementing a system. This is aligned with the context of the BINA domain model, and an evaluation using misuse cases is appropriate. In more recent extensions of misuse cases [177], researchers try to make them executable and closer to real-time behaviour. However, these extensions are out of the scope of this research that focuses on requirements and hence are not included.

Secure Tropos [33] is based on the Tropos methodology, which uses the concepts of goal-oriented modelling languages to analyse cyber security from a sociotechnical perspective. It extends the Tropos methodology by adding security entities during the early stages of a system-to-be. It also offers an implementation process that supports the elicitation and analy-

sis of cyber security requirements that a system needs to meet stakeholders requirements. Secure Tropos has a modelling language that allows comparison with the BINA domain model as it examines a system from its early stages of design and development and focuses on cyber security and incidents in the form of cyber threats and attacks. Hence, Secure Tropos is considered suitable for evaluating the BINA domain model.

SecureUML [178] was initially designed to instantiate role-based access control and relevant security constraints. It is a modelling language based on the Unified Modelling Language (UML) that instantiates specifications for access control aspects of a system. It is cybersecurity-related and can support relevant automation as it is closer to implementational aspects of a system-to-be. BINA domain model focuses on earlier stages of a system's development and has a broader cyber security perspective; thus, Secure UML is not used for its evaluation.

UML State Machine Diagrams [179] offer a semantic and syntactic definition of the behaviour of a system at different stages. In this way, a change in a system is seen as a result of inputs and its previous states. This can relate to incidents and the resiliency states of the system. However, the changes this approach captures are closer to either intended behaviour by the legitimate manufacturer or closer to a real-time monitoring system. Both these aims are out of the scope of this research. BINA looks at socio-technical aspects and changes in these systems that occur because of malicious intent and are hard to predict and/or observe when they occur. Hence, we do not use UML State Machine Diagrams to evaluate the BINA domain model.

UMLSec [180] extends the Unified Modelling Language (UML) to allow the design of cybersecurity entities in the diagrams of a system's specifications. UMLsec is related to the later stages of a system's development after the requirements elicitation and analysis. In particular, it expresses criteria for evaluating the security aspects of a system's design using formal semantics. We omit UMLSec in the BINA evaluation because it is used for later stages of a system's life cycle.

Babiceanu R.F. and Seker R. [181] presented in 2017 their concerns for security requirements for control systems within manufacturing processes. They realised that if someone accesses these systems can exploit them and cause harm. They proposed an ontology representing resiliency for the software aspect of manufacturing networks. BINA looks into cyber and physical aspects of systems, not just software but also hardware, due to the presence of cyber-physical attacks designed to manipulate physical elements through cyber means. Babiceanu R.F. and Seker R. use their ontology at a requirements level and their overall framework to apply cyber-resilient software manufacturing systems. Their proposed modelling environment is narrower than BINA, so we do not use it for the BINA evaluation.

Chapurlat V. et al. [182] introduced a model-based method for re-engineering critical infrastructures to be resilient. They wanted to model the behaviours of critical infrastructures, evaluate their resiliency and identify relevant metrics. They were looking into existing critical systems and not systems-to-be that BINA does. They focused on simulating systems to assess their performance and did not focus on early requirements on these systems. Chapurlat V. et al. also a combination of existing tools to assist the creation of behavioural simulations and overall evaluation. However, the BINA domain model does not instantiate a system's behavioural but rather sociotechnical aspects and uses a tool specific to the domain model definition. Hence, we could not use the combinations Chapurlat V. et al. suggested for the BINA evaluation because their proposal has entities that belong to a more generic risk assessment context and catch only the behavioural aspects of an existing critical system than a by-design cybersecurity resilient system like BINA attempts to do.

Häring I. et al. [183] focus on the resilience of cyber-physical systems from unwanted

events. Their approach looks at existing systems' and under development systems' quantification capabilities. They formally define resiliency and its components to identify optimal treatments. They recognise the challenges to predicting and assigning probabilities to the resiliency of non-linear, discontinuous, quality changing or highly dynamic systems. Their formal representation offers more expressive means for cyber-physical resiliency requirements than constructs necessary to capture and analyse these requirements. For this reason, we could not include their approach to the BINA evaluation process.

6.2 Evaluation of BINA by KAOS

The assessment of BINA support by KAOS is done by analysing the KAOS metamodel [175] and textual explanations provided by the associated literature. The following sections present the use of KAOS on the running example following the generic process and then associates its constructs with the BINA domain model. Finally, observations are presented as a discussion at the end of the section.

6.2.1 Modelling BINA with KAOS

In this section, the example proposed in Section 6.1.1 is adapted to illustrate BINA following the steps described in Section 6.1.2.

- **Determination of context and assets.** In this step goals are defined and refined in the KAOS goal model, as depicted in Fig. 6.3 and Fig. 6.4. The main goal studies in the example is *Accomplish vaccine design validated*, which is refined in *Parameters are reliable*, *Perform structured experiments calculation* and *Avoid unauthorised calculation modifications*. More details about the information system are given to the operational model. The goal *Perform structured experiments calculation* is associated to the agent *Vaccine researcher* and the operations *Enter vaccine information*, *Launch calculation* and *Select experiment parameters*. Finally, the objects used within the operations are defined, like *Database of parameters*.
- **Determination of security goals.** As seen in Fig 6.3, the determination of security objectives occurs in the same model and at the same time as the elicitation of other goals. *Avoid unauthorised calculation modifications* is an example of a security objective, meaning that the integrity of vaccine calculation should be preserved. This security objective can be reached through two alternative goals *Avoid unauthorised access to data* and *Avoid unauthorised server configuration*.
- **Assessment and analysis of risks.** Risk analysis is done by building an antimodel, like in Fig. 6.5. The antigal analysed is *Accomplish credentials known from the attacker*. This antigal is refined in sub-antigoals *Accomplish username known from the attacker*, *Accomplish password known from the attacker*, *Accomplish extract password from the user* until reaching anti requirements *Accomplish social engineering activities to find the password* assigned to anti agent *Attacker*. Vulnerabilities are also identified in the antimodel, such as *Employee*, not security-aware. Finally, in the operation model, the operations performed to satisfy the goal *Accomplish social engineering activities to find the password* are defined.
- **Risk treatment.** In KAOS, risk treatment is defined through the countermeasure chosen for managing the antimodel, and its associated vulnerabilities and antigals. In the running example, the countermeasure chosen from *Pharma Invent* is *Vulnerability avoidance*, in order to avoid that employees are not security-aware.

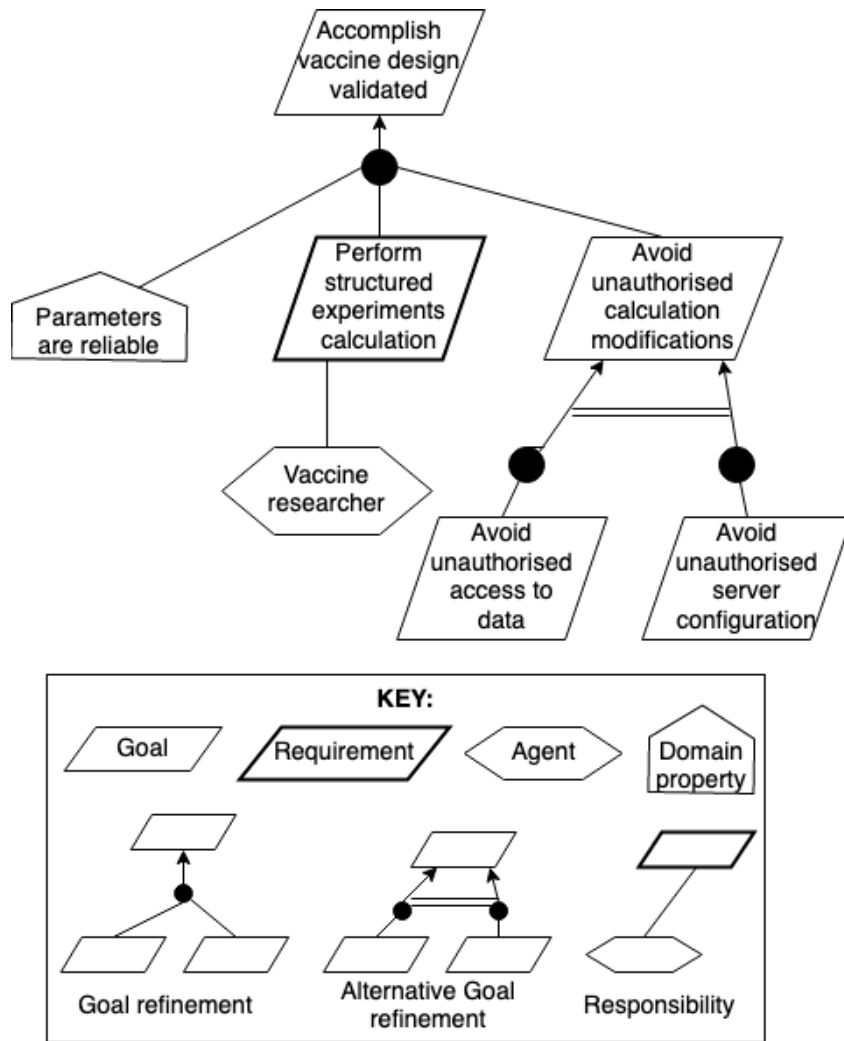


Figure 6.3: Partial goal model for the Pharma Invent

- **Elicitation of security requirements.** New security goals are emerging from this countermeasure. A new goal model is thus instantiated with new security goals, requirements and expectations. In Fig. 6.3 a new requirement called *Organise a security training plan* is added to the goal model presented in Fig 6.7. This requirement is assigned to the *Security officer* agent.
- **Selection and implementation of controls.** The update of the goal model, which might include the refinement and the operationalisation of the newly added goals, constitutes the new system to be, as in Fig. 6.7.

6.2.2 Association of KAOS with BINA domain model

In Tab. 6.1, we display how KAOS incorporates the BINA domain model. We explain the mapping with examples from Fig. 6.3 to 6.7.

Domain-related constructs. KAOS focuses mainly on the security of the system-to-be, without separating the information systems from business aspects. Thus, we align BINA constructs concerning assets with the KAOS object and expectation (cf. Tab. 6.1). KAOS describes states of the system-to-be using objects attributes. The purpose of the security goals is to pro-

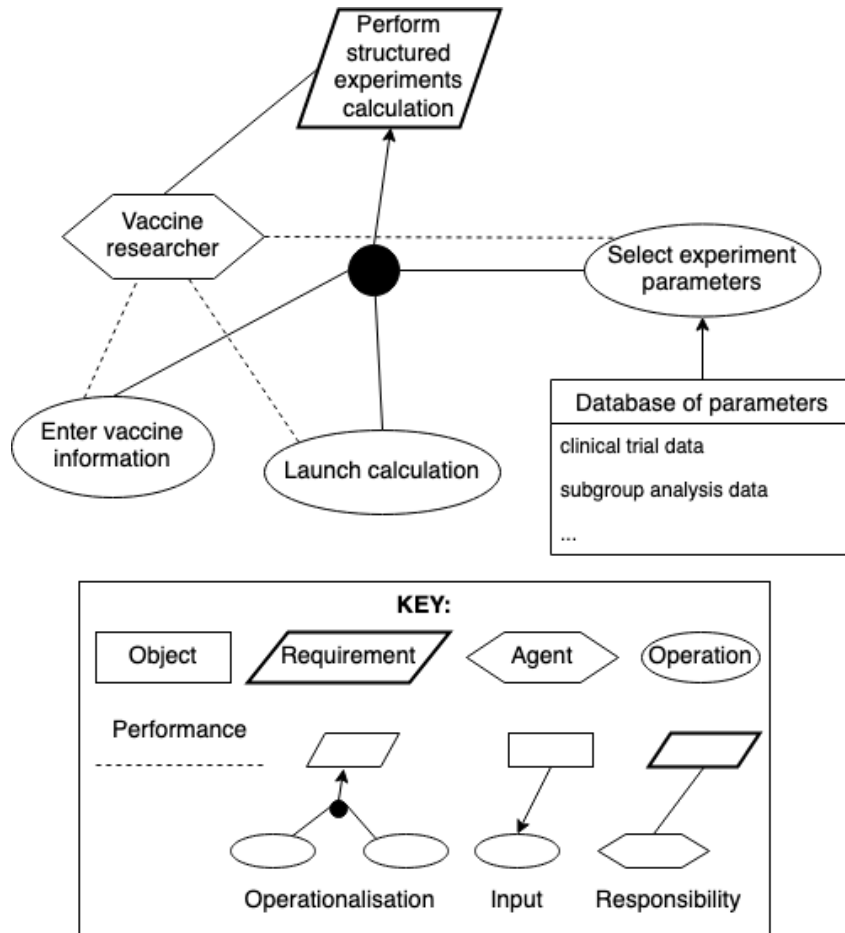


Figure 6.4: Partial operation model for the Pharma Invent

Table 6.1: Construct alignment between KAOS and the BINA domain model.

BINA constructs	KAOS constructs	Instances
Actor	Agent	Attacker
Asset	Object, Expectation	Accomplish vaccine design validated
Objective	Goal, Object attribute	Avoid unauthorised calculation modifications
Risk	-	-
Incident	-	-
Event	Goal (in anti model)	Accomplish credentials known from the attacker
Threat	Expectation (in anti model)	Accomplish password known from the attacker
Vulnerability	Domain property	Employee not security aware
CIRP	-	-
Security constraint	Requirement	Organise a security training plan
Security control	new model implementing security constructs	-

protect system states against malicious activities. In terms of KAOS, this means that the security goals should define confidentiality, integrity, availability, privacy goal and object attributes, which are concerned with potential risk events and threats [175, 176]. Thus, we align both security goals and object attributes concerned by an anti goal with BINA security constructs

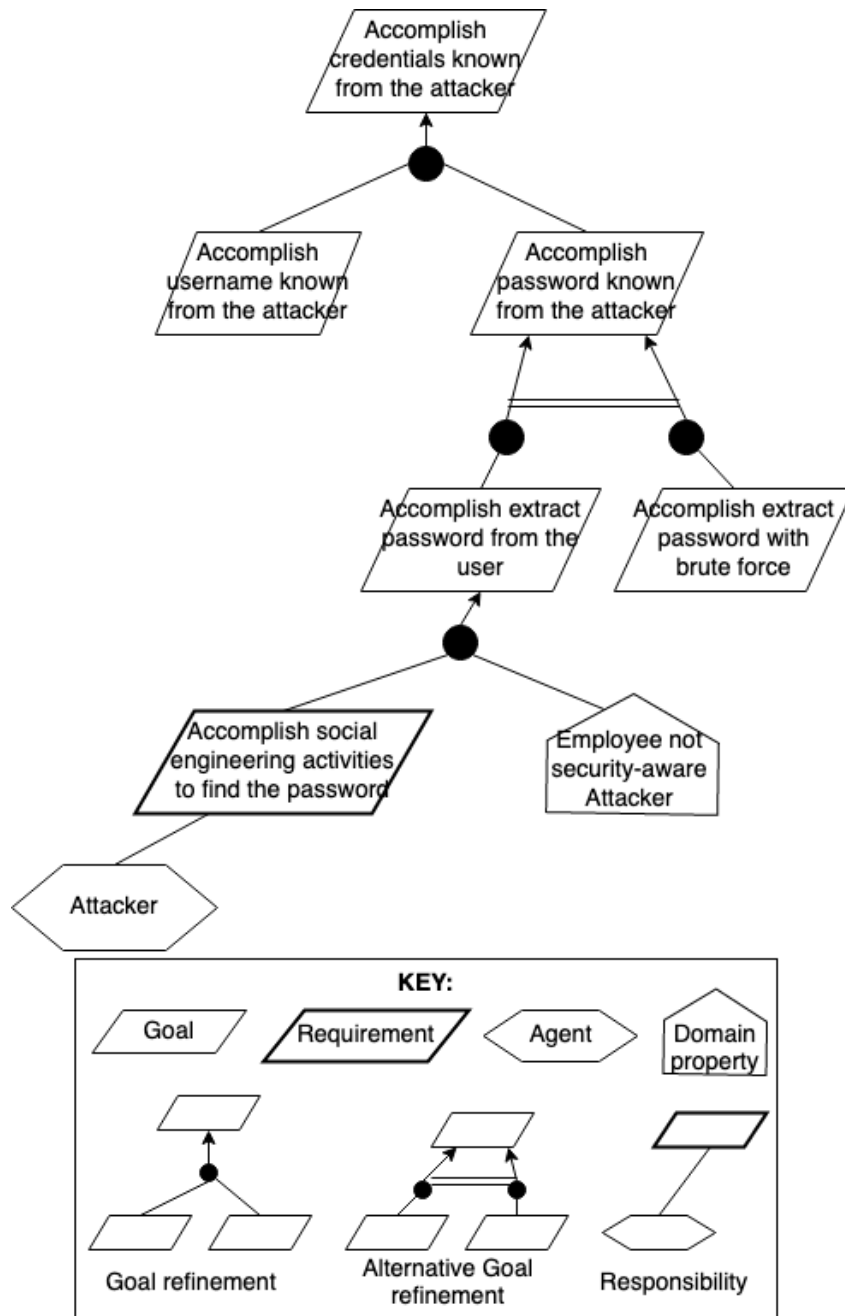


Figure 6.5: Partial antgoal model for the Pharma Invent

like event and threat.

Offensive-related constructs. In Tab. 6.1, we align together BINA event and threat with KAOS anti goal and anti expectation respectively. Anti goals stand for different abstraction levels, so they can be refined until they become anti requirements or anti expectations assigned to an anti agent. At higher abstraction levels, an anti goal might be considered as the event which, according to BINA domain model, is a combination of threat and one or more vulnerabilities. At lower abstraction levels, an anti goal, anti requirement, or anti-expectation threat is a potential attack or incident to assets. In Tab. 6.1, we align BINA vulnerability and the KAOS domain property. The domain property is a hypothesis that holds independently of the system-to-be. In correspondence, BINA vulnerability is defined as a characteristic of assets.

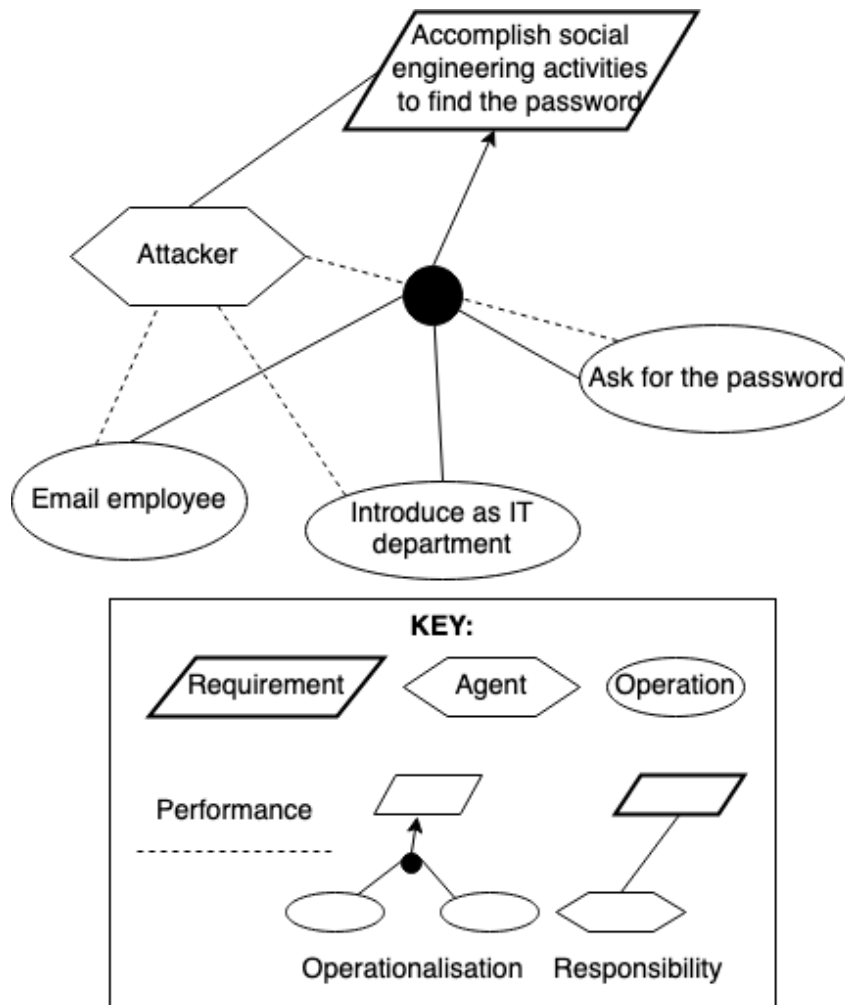


Figure 6.6: Partial antigoyal operational model for the Pharma Invent

In KAOS, an anti agent monitors or controls objects and their attributes, thereby threatening the system-to-be. In Tab. 6.1, we align the BINA actor and KAOS anti agent. KAOS does not address two risk-related constructs from the BINA domain model: risk and incident.

Defensive-related constructs. BINA CIRP corresponds to the countermeasures that are elaborated after identification of the anti goals. Countermeasures are not KAOS modelling constructs, but instead modelling idioms or 'patterns' adopted by modellers [175, 184]. In KAOS, the countermeasures usually result in new security goals, which need to be further refined into realisable security requirements and expectations. In Tab. 6.1, we align BINA security constraints and the KAOS requirements [176]. The refinement and operationalisation of the new security goals, their concerning objects and attributes, and their assignment to agents lead to new system-to-be components realising the necessary security means. Concerning the BINA domain model, these new system constructs correspond to controls.

6.2.3 Discussion

The alignment of KAOS with the BINA domain model highlights some limitations. The coverage of KAOS appears to have opportunities for amendments:

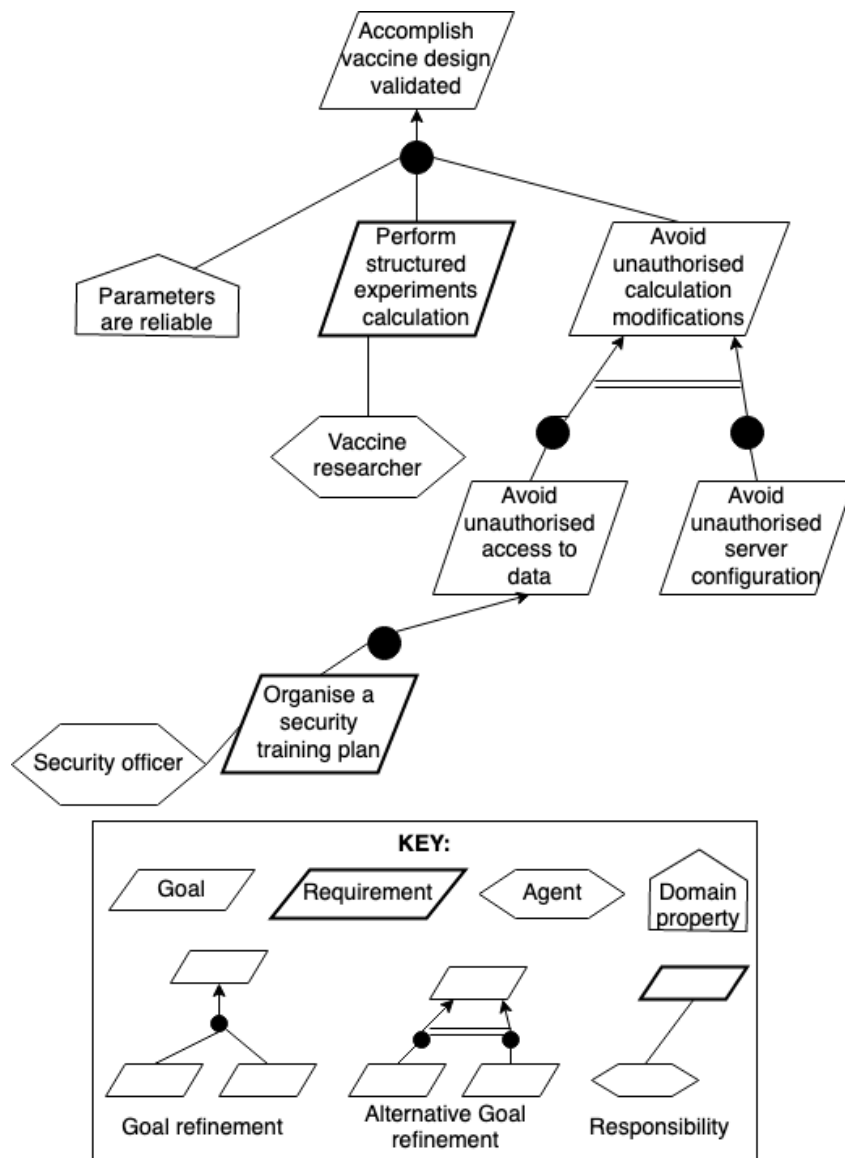


Figure 6.7: Security requirements and controls modelling in KAOS

- We could not find sufficient empirical evidence that would provide us with a complete model of a secured system modelled with KAOS. The works we succeeded to identify on the KAOS extensions to security include [175, 176]. However, they only illustrate the major security modelling principles. The models presented in these works are limited and do not provide many modelling details. As the conclusion, Tab 6.1 lists only the primitive language constructs and their correspondences to the BINA domain model. However, we must note that one can also identify construct combinations to model some aspects of security risk management as the modelling patterns. The models presented in Fig. 6.3 to 6.6 suggest a few simple modelling patterns that address security risk management concerns. For instance, we can observe that a threat *Accomplish social engineering activities to find the password* will be presented as anti requirement or expectation and permanently will be assigned to anti agent *Attacker*. In Fig 6.8, we can also observe the pattern for risk event. It is a combination of the anti goal *Accomplish extract password from the user*, at least one anti requirement or expectation *Accomplish social engineering activities to find the password* and domain property *Employee not security aware*.

- Similar constructs of KAOS are used to support different BINA constructs. For instance, a goal can be used to model assets, security constraint, event and threat. Thus, we can determine that a goal is a threat or an event, whether it is part of an anti-model. However, for the other cases, no way to distinguish one BINA construct from the other is provided.
- KAOS does not address two constructs from the BINA domain model: risk and incident. This can be partially explained by the fact that KAOS was not specifically designed to consider the business context of an information system. However, these constructs might be derived from the implicit description of the modelled problem. For example, in Fig. 6.5, we presented a risk event as the goal *Accomplish password known from the attacker*. Achievement of this goal might lead to an incident called *Vaccine experimentation calculation modified by attacker*. Further, this might form a chain of incidents like *design mistake, legal costs*. The incident might be characterised by introducing new goals and defining concerns between the goal/anti goal and object/anti object models. However, this requires further theoretical and empirical investigation. Similar argumentation can also be provided about other BINA constructs, like risk.
- Some KAOS constructs only provide partial coverage of the BINA concept. For instance, the countermeasures proposed by KAOS only partially cover the BINA cyber resiliency in terms of CIRP. An agent substitution is used in KAOS to replace a vulnerable agent assigned to a threatened goal with a less vulnerable one for the threatening anti-goal. However, it only partially covers the CIRP of risk transfer because the vulnerability is not always on an agent when choosing the risk transfer approach.



Figure 6.8: KAOS pattern for BINA event

6.3 Evaluation of BINA by Misuse Cases

The assessment of BINA reinforcement by Misuse cases is done by examining the Misuse cases meta-model [32] and textual explanations provided by the associated literature [185, 186, 187]. Initially, the use of Misuse cases for supporting the BINA is depicted. Then, the constructs of the language are semantically aligned with the BINA domain model. Finally, a discussion with regards to the alignment is provided.

6.3.1 Modelling BINA with Misuse cases

In this section, we examine how Misuse cases can be used for cyber resiliency. Our application follows the steps of the generic security requirements process described in subsection 6.1.2. We

utilise the example of subsection 6.1.1. Further, we present and use the constructs of Misuse cases.

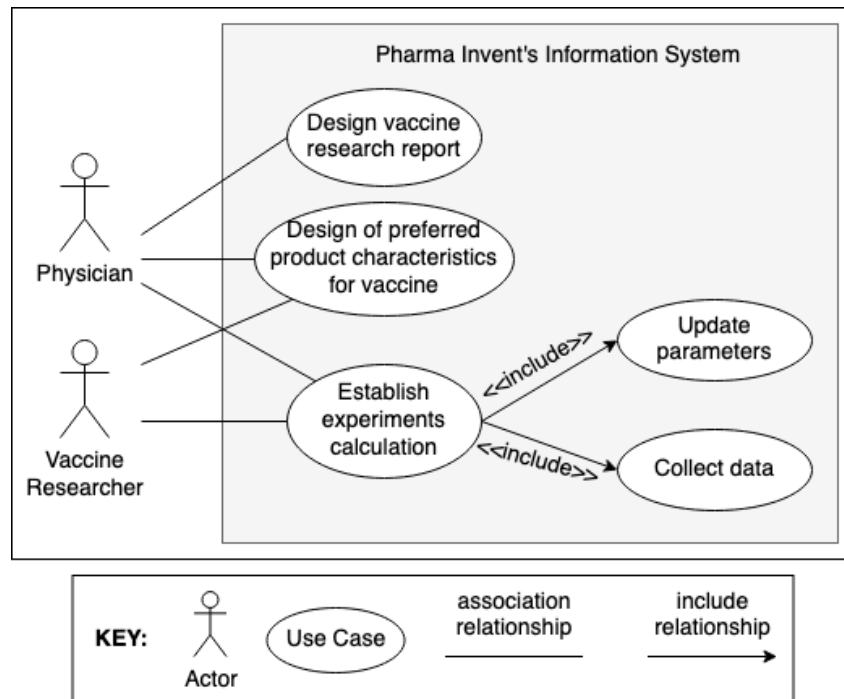


Figure 6.9: Asset modelling in Misuse cases

Determination of context and assets. In Fig. 6.9, a use case diagram for the Pharma Invent's information systems is presented. We focus on the actors *physician* and *vaccine researcher*, who communicate using the *Pharma Invent's information system*. The *physician* is involved *Design vaccine research report* and both actors in *Design of preferred product characteristics for vaccine* and *Establish experiments calculation*. *Establish experiments calculation* includes two cases, namely *Update parameters* and *Collect data*.

Determination of security goals. Determination of security goals is not supported by Misuse cases as there is no suited construct. In the running example, we focus on the integrity of the experiments calculation. This means that once the structure calculation is established, unauthorised users cannot change it.

Assessment and analysis of risks. In Fig. 6.10, we identify misuse cases, which involve the malicious actor *Attacker*. The *Attacker* threatens the integrity of *Establish experiments calculation* with the misuse case *Steal login credentials*. This misuse case includes another misuse case, which describes certain steps in more details *Apply social engineering*.

Risk treatment. Misuse cases do not suggest any risk treatment. However, following the generic security requirements process, risks can be treated using security controls as security use cases.

Elicitation of security requirements. The use case *Conduct awareness training* (cf. Fig. 6.11) is the security use case, which mitigates the identified misuse case *Apply social engineering*. It is part of the use case *Organise a security training plan* initiated by the *Security officer*.

Selection and implementation of controls. Misuse cases do not propose any technique to select and implement controls. Thus, to select between alternative security controls, other approaches will be needed.

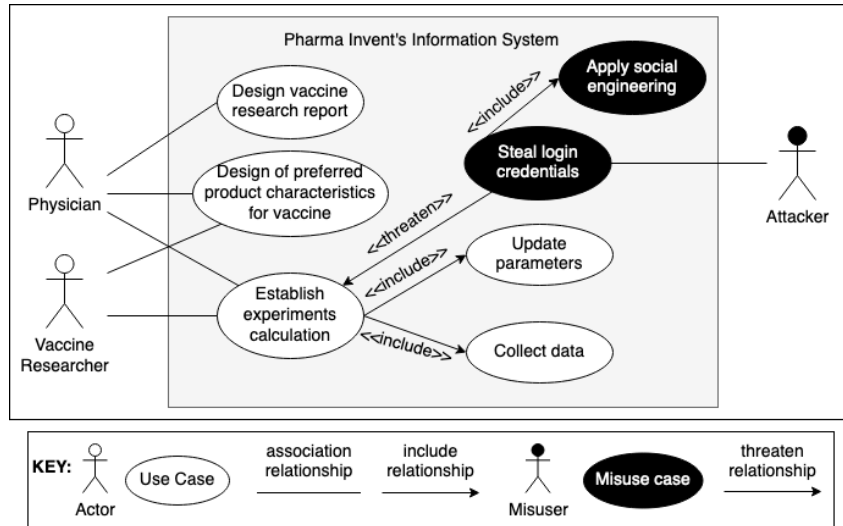


Figure 6.10: Modelling Risk in Misuse cases

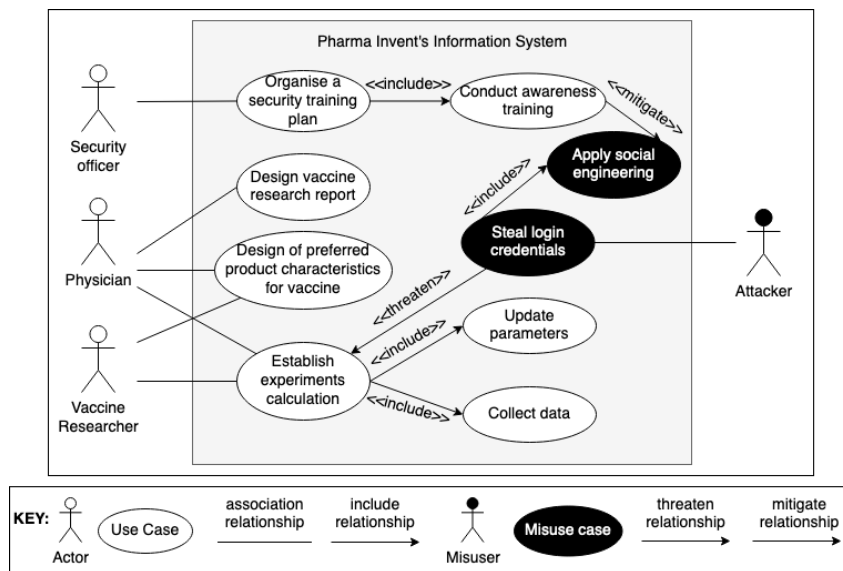


Figure 6.11: Modelling Security constraints in Misuse cases

6.3.2 Association of Misuse cases with BINA domain model

In this section, we analyse how Misuse cases constructs are matched to BINA constructs. Tab. 6.2 suggests an alignment between the BINA domain model and Misuse cases.

Domain-related constructs. Tangible and intangible assets are subject to cyber-attacks. A use case represents something of value for its owner [32]. This interpretation corresponds to the BINA notion of an asset. The process guidelines for misuse cases modelling suggests focusing on 'normal' actors and the main use cases and assets as they have been requested [32]. The assets in misuse cases can be information, location, activities and skills [32]. For instance, in Fig 6.9, use cases are considered as BINA assets. The use case relationship *includes* forms new assets. This relationship is part of the assets construct too. From the relevant literature [185, 186, 32], it becomes apparent that a use case typically represents the interaction between user and system to achieve some wanted function. Hence, use cases are suitable for

Table 6.2: Construct alignment between Misuse cases and the BINA domain model.

BINA constructs	Misuse case constructs	Instances
Actor	Actor Misuser	Vaccine researcher Attacker
Asset	Use case	-
Objective	Use case	Establish experiments calculation
Risk	Misuse case	Steal login credentials
Incident	Misuse case	-
Event	Misuse case	-
Threat	Misuse case	-
Vulnerability	-	-
CIRP	-	-
Security constraint	Use case	Organise a security training plan
Security control	Use case	-

functional requirements but not necessarily for non-functional ones, such as security requirements.

Offensive-related constructs. The risk involves constructs that relate to the notion of impact in Misuse cases. Misuse cases can be defined at different levels of abstraction [185]. A high-level description of a misuse case corresponds to the notion of risk. The security threats can be represented from the misuse cases as acted from the misusers [185]. The *threatens* relationship can be seen as a harms relationship between threat and asset in the BINA model. The possibility of relations between misuse cases and use cases in terms of potential *includes* relations seems to associate with the notion of event. An event for BINA represents any observable occurrence in a system or network that have not risen to the level of a violation of **security constraints**. Misuse cases view a use case as a standard system functionality that can malfunction, causing a threat.

Defensive-related constructs. Security requirements for Misuse cases form independent security use cases [32]. A security use case has a *mitigate* relationship to a misuse case. It can be inferred that security use cases are equivalent to BINA security constraints. The misuse case *mitigates* relationship corresponds to the BINA mitigates relationship. However, the relationship in Misuse cases indicates how security use cases mitigate a misuse case. Hence, Misuse cases do not correspond to the BINA notions of risk incident response plan or security control.

Use case diagrams display the context of textual templates that represent each use case. Although we have mainly focused on the diagrammatic representation of Misuse cases, Misuse case templates are also relevant to the constructs of the BINA domain model. An example template is given in Fig. 6.12.

The *business rules* is relevant to the BINA asset construct. The majority of the template focuses on terms relevant to risk-related constructs. For example, the BINA risk is addressed by *risk*. The BINA construct of vulnerability is specified by the categories *trigger*, *assumption*, *pre-condition*. The BINA incident can be seen through the *threat* as it describes the impact whereas the BINA construct threat is more relevant to the entries *basic path*, *alternative path*, *extension points*.

It is important here to clarify that the Misuse cases template depends on the detail of the misuse case under study. More specifically, if a misuse case is instantiated at a high level, the

Name	Steal login credentials
Summary	A malicious actor steals credentials allowing him to access internal systems
Basic path	Phishing email
Mitigation points	Employees have relevant training and regular testing
Extension points	Apply social engineering
Trigger	True, it can happen at any time
Assumption	No biometrics are used
Preconditions	Malicious actor can find employees email addresses
Threat	Unauthorised actor modifies pre-establish experiments calculation
Mitigation	Employees do not disclose their credentials
Business rules	Only authorized users can access
Misuser	Skilled
Stakeholder	Vaccine researcher
Risks	Time loss for reestablishment of calculations
Scope	Information system
Abstraction level	Misuser goal
Precision level	Focused

Figure 6.12: Example of the Misuse cases template

precondition would correspond to a vulnerability. However, if a misuse case is defined at a lower level of detail, the precondition will define the system's state. If that is the case, then the BINA domain model will not have a construct that corresponds to the precondition.

6.3.3 Discussion

Tab. 6.2 gives a representation of the coverage of Misuse cases for the BINA domain model. Some extensions can be suggested to Misuse cases if used for cyber resiliency:

- Misuse cases do not distinguish some constructs that represent different constructs in the BINA domain model. For instance, assets, objectives and security constraints are represented using the same visual construct for a use case. For misuse cases, such differentiations seem as nuances as the focus is more on preventive security.
- For some constructs (e.g., risk, event, incident), Misuse cases do not provide modelling constructs. Misuse cases do not cover all constructs of the BINA domain model. For example, when using misuse cases models, one needs to describe how to model risk, event, incident, security constraints, CIRP decisions and security controls. Some of these constructs can be defined in the misuse cases template, for example, incident as a threat, trigger, assumption and precondition. Other constructs can be defined by extending the misuse cases template with additional entries. However, that can increase the complexity of misuse cases extending the level of granularity of the analysis.
- It is also observed that some constructs are partially covered. For example, Misuse cases model risks, including residual risks or impact using the concept of 'misuse case'. However, the language excludes modelling of the threats to the vulnerabilities that make such negative occurrences possible.

6.4 Evaluation of BINA by Secure Tropos

This section illustrates how we can use the Secure Tropos approach to analyse security risks and derive appropriate countermeasures from these risks. We summarise the discussion on alignment in Tab. 6.3. This alignment is based on the Secure Tropos literature [33, 188, 189], sometimes presenting part of the Secure Tropos meta-model [33].

6.4.1 Modelling BINA with Secure Tropos

In this section, the running example proposed in Section 6.1.1 is adapted to illustrate BINA, following the steps described in Section 6.1.2.

- Determination of context and assets.** Fig. 6.13 shows an actor model, representing the actors playing a role in the estimate definition and the associated dependencies between actors. In our example, the actors are *Scientific department*, *Sales department* and *Client*. The dependencies are of two kinds: resource dependency *Evaluations*, *Vaccine mockup*, *Medical experimentation plans* and goal dependency *Manage pharmaceutical projects*, *Experiments calculation structure* but can also be a soft goal or a plan dependency. More information about the dependencies is provided in the goal model, clarifying how the actors' reason about goals to be fulfilled, plans to be performed and available resources. It completes the actor model with each actor's reasoning about its internal goals, plans, and resources. In Fig. 6.13 the goal model of the *Scientific department* shows that, for satisfying the goal *Experiments calculation structure*, two different plans are possible *Manually* and *Software support*. Plans and resources necessary to perform the experiments calculation with a software tool are also defined.

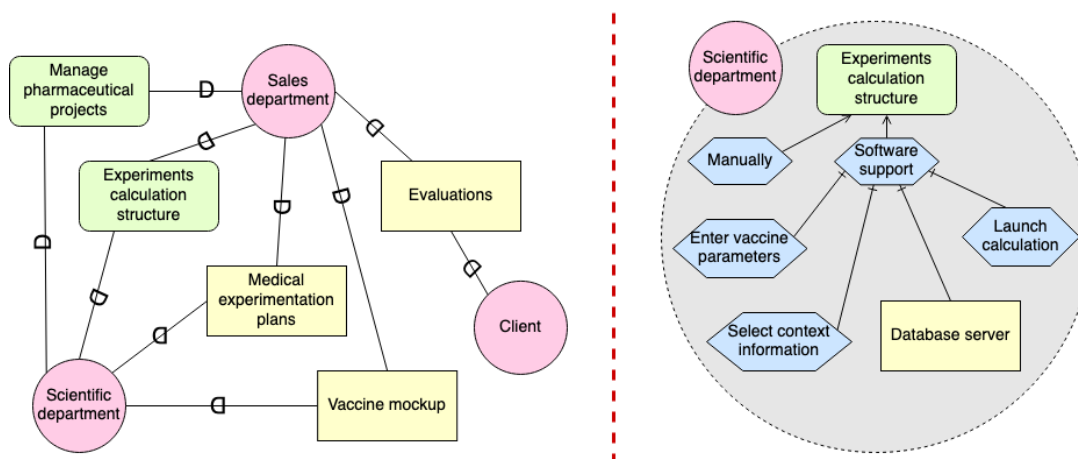


Figure 6.13: Actor and goal models of Secure Tropos for assets modelling.

- Determination of security goals.** The BINA security objectives are expressed in Fig. 6.14 through security constraints, restricting some dependencies. For example the *Sales department* should *Preserve the integrity of experiments calculation* and the *Scientific department* should *Manage to keep evaluations private*. The latter is related with a constraint link labelled 'restricts' to the plan *Software support* in the goal model by adding security constraints, the goal model becomes security-aware.
- Assessment and analysis of risks.** Fig. 6.15 focuses on possible risk event. A Secure Tropos threat to the software *Influenza vaccine production documentation* is identified in the

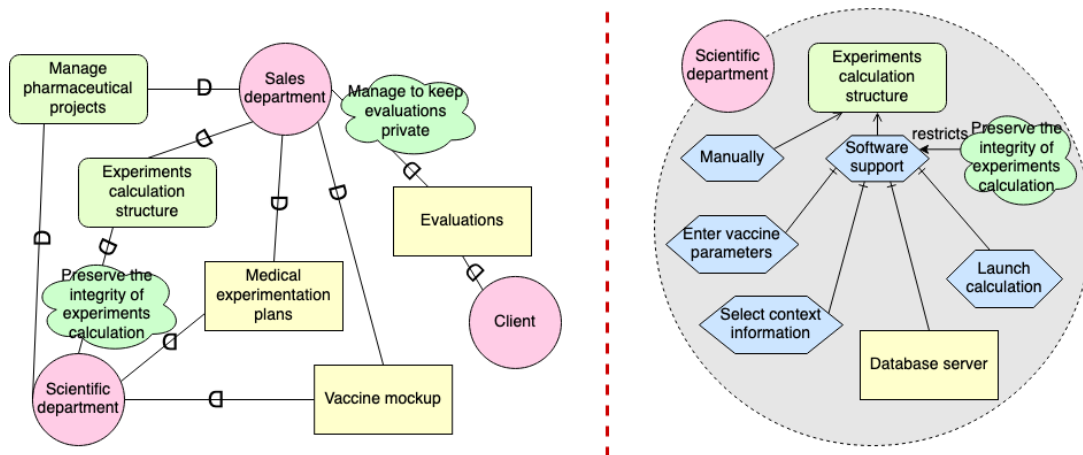


Figure 6.14: .

attack diagram of Fig. 6.15. The attack diagram is an adaptation of a security reference diagram we introduce, including elements of the security-enhanced goal model. The threat is about *Authentication attack*, aiming for an attacker to authenticate to the tool. A security attack scenario completes this diagram. It shows that the goal of the *Attacker* is to know the login data of a user of the tool. To achieve his goal, he uses social engineering. He believes that at least one employee is not security-aware, which constitutes a vulnerability in this context. His attack targets the resource *Database server* of the *Scientific department*. In Fig. 6.15, the security attack scenario can be seen as the refinement of the security event identified in the attack diagram.

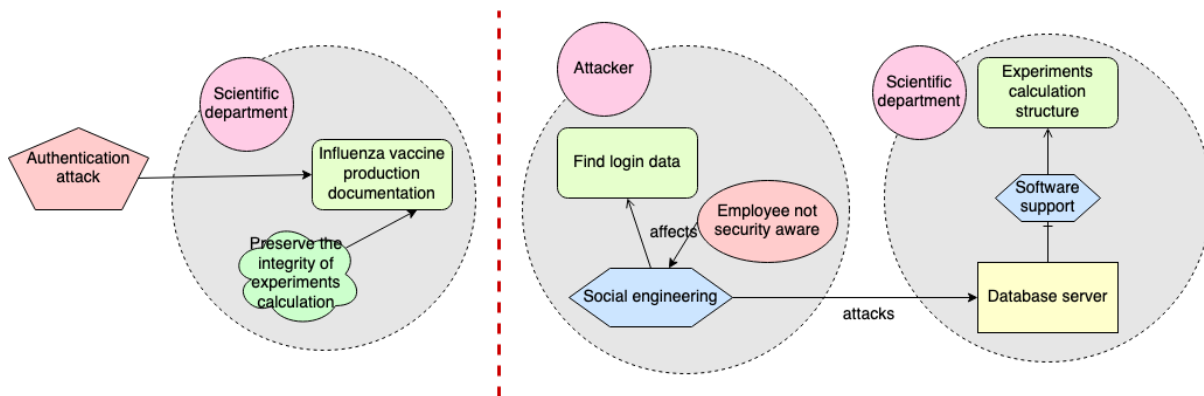


Figure 6.15: Actor and security models of Secure Tropos for risk modelling.

- **Risk treatment.** In the running example, the risk approach selected is to decrease the risk by adding some secure goals/plans/resources. Commonly, other choices are possible, like avoiding the risk by changing the security-aware actor and/or goal models or introducing another actor, as the third party, to partake in the risk.
- **Elicitation of security requirements.** The risk treatment choices lead to alteration of the security-aware goal model of Fig. 6.14. A secure goal *Make all users security aware* is introduced, satisfied by the security plan *Perform security awareness training*. This plan has a positive contribution to the security constraint *Preserve the integrity of experiments calculation*, as depicted in Fig 6.16.
- **Selection and implementation of controls.** Qualitative goals (also called soft goals) can

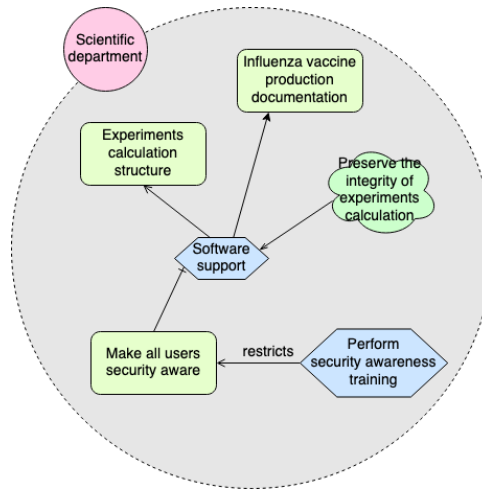


Figure 6.16: Security constraints modelling in Secure Tropos.

be used to reflect on the diversity between control alternatives. This step takes place after controls are determined, which usually happens during the design phase.

6.4.2 Association of Secure Tropos with BINA domain model

To investigate how Secure Tropos can aid to resolve BINA queries at the early stages of information system development, we have examined the existing Secure Tropos literature in order to comprehend its main principles and constructs. Then, we have implemented Secure Tropos in the running example. This implementation strongly follows the process introduced in subsection 6.1.2 and the constructs suggested by the BINA domain model. The result is the semantic alignment between BINA and Secure Tropos as depicted in Tab. reftab:st. This table displays how Secure Tropos and in which cases can be aligned with the principles of BINA.

Table 6.3: Construct alignment between Secure Tropos and the BINA domain model.

BINA constructs	Secure Tropos constructs	Instances
Actor	Actor	Scientific department
Asset	Resource	Database server
Objective	Goal, soft goal	Influenza vaccine production documentation
Risk	-	-
Incident	-	-
Event	Threat	Authentication attack
Threat	Goal, plan	Find login data
Vulnerability	Vulnerability	Employee not security aware
CIRP	-	-
Security constraint	Security constraint	Preserve the integrity of experiments calculation
Security control	New model, implementing security components	Perform security awareness training

Domain-related constructs. In Secure Tropos, we recognise that the business and information system description the constructs *actor*, *goal*, *resource* and *plan* are used. For example, the actor *Scientific department*, the goal *Manage pharmaceutical projects* describe the process necessary for

the Pharma Invent to achieve its objectives. Resources like *Medical experimentation plans* and *Vaccine mockup* characterise the valuable information assets. All the instantiations mentioned above are relevant to the constructs of actor, objective and asset of the BINA domain model.

The business operations are mainly supported by the information system of the *Scientific department*. The this department's operation *Experiments calculation structure* is performed through the plans *Manually* or *Software support*. The BINA security constraints on objectives characterise the security and incident response needs. In Secure Tropos *goals* and *softgoals* in particular can assist in the identification of higher-level security criteria. Depending on the context, it might be necessary to refine them using *security constraints* like *Manage to keep evaluations private* and *Preserve the integrity of experiments calculation*.

Offensive-related constructs. Risk is defined by the event of the risk, matching to the *Authentication attack* in Fig. 6.15. The expected negative outcome of the risk between the *Authentication attack* and goal *Influenza vaccine production documentation* is called the impact of the risk. Here, the incident negates the security constraint *Preserve the integrity of experiments calculation*.

In Fig. 6.15, the goal *Find login data* associates to the threat relating the potential attack targeting the asset *Database server*. The threat agent *Attacker* triggers the threat given that the malicious actor knows about the absence of security awareness for an employee, as recognised by the vulnerability *Employee, not security aware* in Fig. 6.15. To break into the *Scientific department system*, the *Attacker* conducts an attack where she uses *Social engineering*.

In Tab. 6.3, the construct of vulnerability resembles the BINA construct. The fact that the actor in the role of the attacker thinks she knows might be right. In this case, the vulnerability will correspond to vulnerability in the sense of the BINA. However, facts known by the attacker might be wrong; in this case, there is no similar construct in the BINA. Finally, vulnerability does not represent vulnerabilities in the system but is not known by the attacker.

Defensive-related constructs. In our case, we utilise risk reduction decision. This leads to an alteration of the information system design, lessening the identified risk. New security constraints (cf. Fig. 6.16) are identified as the goal *Make all users security aware* and the plan *Perform security awareness training*. We demonstrate the security control using the Secure Tropos *goal* and *plan* constructs, however, depending on the chosen risk treatment decision, the combination of *actor, goal, resource, plan* and *security constraint* might result in different security control systems. A new model performing the essential security elements is the output of this phase.

6.4.3 Discussion

The association of Secure Tropos constructs and the BINA domain model has shown some limitations of Secure Tropos to investigate cyber resiliency at the early stages of the design and development of a system-to-be. At the same time, it proposes possible improvements for Secure Tropos in the context of cyber resiliency.

- Secure Tropos provides guidelines as to when and how to use each construct. These guidelines allow avoiding misinterpretations of the BINA constructs. For example, in Tab 6.3, the planning construct can be used to model assets, threats and security constraints. For greater detail, labels or syntax changes or the creation of separate diagrams can be used.
- It is noticeable that Secure Tropos could be enhanced with the addition of constructs

to cover the constructs of BINA. Tab. 6.3 indicates that several constructs such as risk, CIRP and incident are not in the Secure Tropos approach. Consequently, we can define graphical constructs to address these concepts or provide methodological guidelines for how these concepts can be addressed in the Secure Tropos models.

- The semantics of individual modelling constructs should be adapted so that they adequately represent BINA constructs. For example, as discussed previously, the vulnerability construct only partially covers vulnerability. A potential enhancement is to propose the modelling construct which would appropriately support the modelling of system vulnerabilities.

6.5 Summary of language association

In this section, we make some remarks regarding cyber security-oriented languages, after their association with the BINA domain model. Misuse cases [32] are mainly focused on eliciting *threat agents* and *attack methods*. For that, they integrate use cases with threat use cases. KAOS [175] focuses on safety-critical information systems but does not have a risk-driven approach. On the other hand, it does cover security concepts like *threat* and *vulnerability*. Secure Tropos [33] also is not a risk-driven approach, meaning that it does express *risk* or *impact*. However, it does cover *threat* and *vulnerability* constructs. Tab. 6.4 summarises the BINA.

Table 6.4: Examination of BINA support by security-oriented modelling languages.

BINA	KAOS	Misuse case	Secure Tropos
Actor	Agent	Actor, Misuser	Actor
Asset	Object, Expectation	Use case	Resource
Objective	Goal, Object attribute	Use case	Goal, soft goal
Security constraint	Requirement	Use case	Security constraint
Vulnerability	Domain property	-	Vulnerability
Event	Goal (in anti model)	Misuse case	Threat
Incident	-	Misuse case	-
Risk	-	Misuse case	-
Threat	Expectation (in anti model)	Misuse case	Goal, plan
CIRP	-	-	-
Security control	New model	Use case	New model

The examination of the security-oriented languages for their support to the BINA domain model allows to review and enhance the proposed language constructs. The main enhancements are:

- ability to distinguish the BINA construct represented, when the same modelling concept supports several constructs;
- ability to provide coverage of the language for the BINA constructs not supported;
- ability to extend a language when some BINA constructs are only partially covered.

Although we did not wholly study the other security-oriented modelling languages, we surveyed them and provided some preliminary conclusions. The coverage of Predictive, Probabilistic Cyber Security Modeling Language ((PCySeMoL)-Cy-2) [190] is indeed focused on how attacks and defences relate quantitatively, instead of investigating the cyber resiliency

lifecycle. The cybersecurity modelling language (CySeMoL) [191] focuses on enterprise-level system architectures coupled to a probabilistic inference engine. In that way, the probability of successful attacks against the systems can be estimated. However, the language does not extend to cover cyber resiliency and probabilities of incident response plans to fail or succeed. The Tropos Goal-Risk framework [192] handles risk management at a high level, without considering security constructs. A full analysis of those languages will produce outcomes of higher accuracy.

6.6 A cyber resiliency-aware Secure Tropos

This section intends to develop syntactic, semantic and methodological extensions to Secure Tropos that would aid the modelling of cyber resiliency and its relevant plans. We start by suggesting extensions to the concrete syntax and show how they transfer to the abstract syntax. Then, we set methodological guidelines. Finally, we discuss the extensions for the BINA domain model.

6.6.1 Concrete syntax extensions

In Section 6.4, we have distributed the concrete syntax of Secure Tropos according to three construct categories: domain-related, offensive-related and defensive-related constructs. In addition to the BINA constructs aligned in Tab. 6.5- 6.7, we consider how BINA relationships (e.g., targets, triggers, endangers, harms) can be represented with Secure Tropos. Moreover, in Section 6.6.2, we relate Secure Tropos concrete and abstract syntax.

Domain-related constructs. The BINA *asset* (cf. Tab. 6.5) construct is expressing both *plan* and *resource* Secure Tropos constructs and their compositions constructed using the relations *means-ends* and *contribution*. Moreover, BINA *objective* is addressing the Secure Tropos constructs of *goal*, *soft goal* and *hard goal*. An *asset* can *contribute* positively or negatively to an *objective*. When an *asset contributes* positively to an *objective* then a *means-ends* relationship can be used. An *asset* can be also *decomposed* to its sub-components, based on the granularity of the analysis.

An *objective* is related in Secure Tropos as well as in BINA with a *security constraint*. A *security constraint* restricts an *objective* in BINA as it does for a *goal* and *hard goal* in Secure Tropos. Whereas in Secure Tropos a *soft goal* stands for security goals that have the form of security constraints. Hence, the *restricts* relationship with them is omitted in the Secure Tropos metamodel [9]. A *security constraint* can be *decomposed* to more specific constraints as the focus of Secure Tropos is to elicit and analyse security requirements in the form of constraints to objectives.

Each *security constraint* is imposed by an actor, shown with the *has* relationship and is also delegated to another *actor* to be accomplished. This BINA relationships are similar with those of Secure Tropos. An *actor has* a *security constraint* because an *objective* based on the *means-ends* relationship needs one or more *assets*. *Assets* have *vulnerabilities*. These *vulnerabilities* can be known or unknown and actors can choose to ignore them for case specific reasons. However, these *vulnerabilities* are the driving force for the existence of *security constraints*. As the research context of Secure Tropos as well as of BINA is the cyber security domain, the *vulnerabilities* instantiate cyber security related vulnerabilities.

Tab. 6.5 shows the domain-related constructs of Secure Tropos and BINA along with the

concrete syntax of Secure Tropos. Whereas Fig. 6.17 displays how the relevant section of the BINA metamodel is enhanced in this iteration of its assessment.

Table 6.5: Domain-related constructs.

BINA Constructs and relationships	Secure Tropos Constructs and relationships	Concrete syntax
Asset	Plan, Resource	
Actor	Actor	
Objective	Goal, Soft goal, Hard goal	
contribution	contribution	
means-ends	means-ends	
decomposition	decomposition	
restricts	restricts	

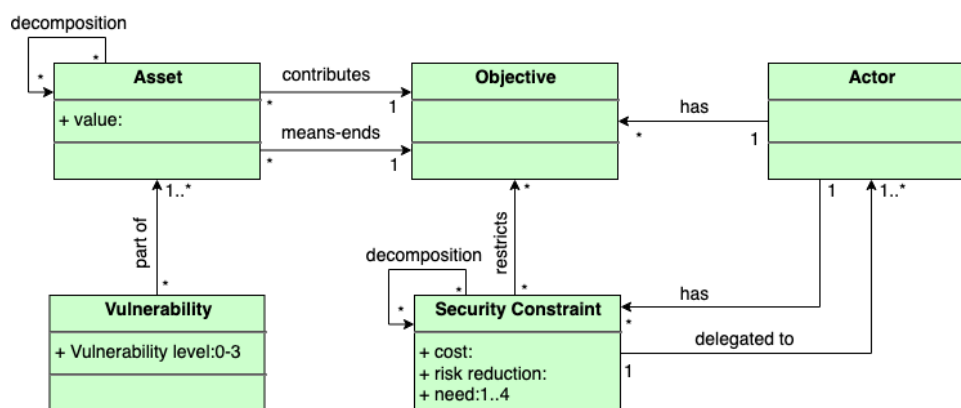


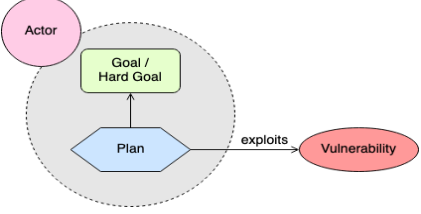


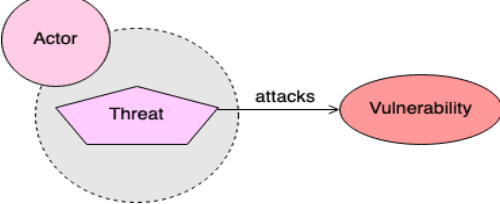
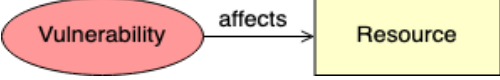


Figure 6.17: Enhanced BINA domain-related constructs.

Offensive-related constructs. As presented in Tab. 6.4, Secure Tropos constructs can be used to model offensive-related concerns. However, there exists a high chance to misinterpret the presented information as Secure Tropos is focused on prevention. Thus, we recommend differentiating the concrete syntax of these Secure Tropos constructs. Secure Tropos *attacks* relationship represents the *exploits* relationship of BINA. In order to be compliant with BINA, we also introduce the *impacts* relationship, which defines a link between *threat* and *asset*.

Then we can represent the *event* of the risk using a combination of constructs (i.e., actor, goal, resource, plan and vulnerability). In this case, and *event*, takes the form of a security attack hypothetical scenario representing details of the event. To generalise this representation, one can use the Secure Tropos *threat* constructs. This representation is used for the identification of risks to assets. Where a *risk* is seen as a combination of an *event* and its *impact*.

Table 6.6: Offensive-related constructs.

BINA Constructs and relationships	Secure Tropos Constructs and relationships	Concrete syntax
Threat	Threat	
Vulnerability	Vulnerability	
Event	(a) combination of agent, goal, plan, vulnerability; (b) threat	 
Risk	combination of threat and impacts relationship	
Incident	-	-
exploits	attacks	
affects	affects	

Defensive-related constructs. For the need of modifying BINA constructs, we also need to update the visual syntax of defensive-related constructs. This becomes apparent from the construct *security control*. This construct can be presented through various Secure Tropos constructs and relationships. Thus, misinterpretations can occur. *Security requirements* mitigate the identified *risk*. This relationship is called *mitigates* and is defined as a link between the constructs of *security constraints* and of *risk*.

The relationship *implements* in Secure Tropos is between the constructs of *security mechanism* and *security objective*. Whereas according to the BINA domain model this relationship links the constructs *security control* and *security constraint*. Also the relationship *addresses* is introduced in BINA between the constructs *CIRP* and *incident*. Not having equivalent constructs in Secure Tropos prohibit us at this stage for being able to offer a visual representation.

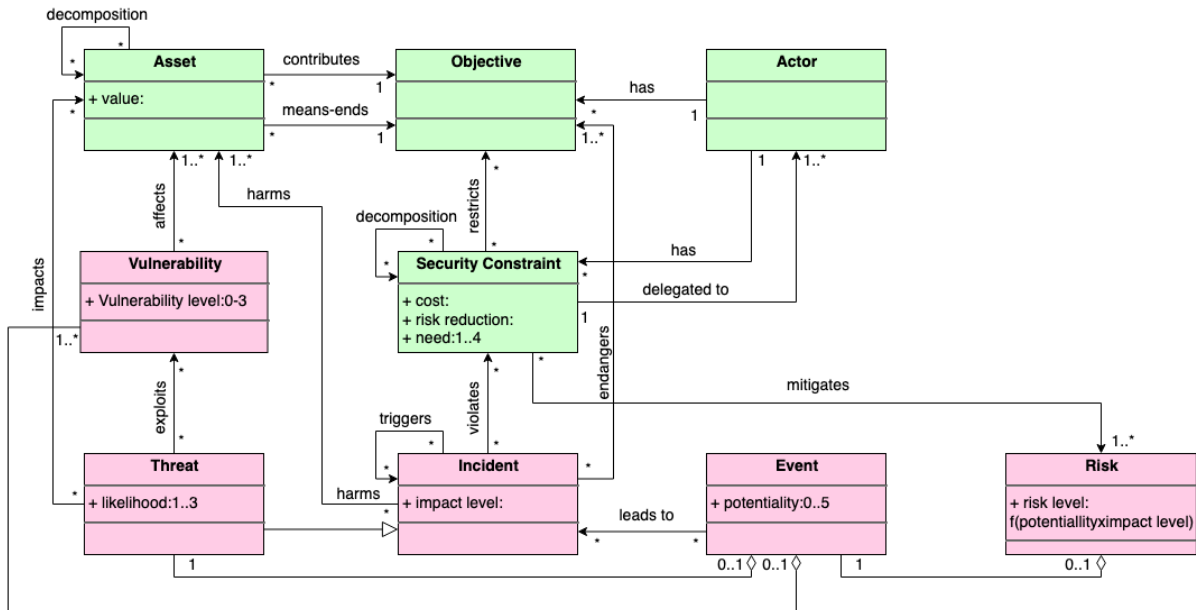


Figure 6.18: Enhanced BINA offensive-related constructs.

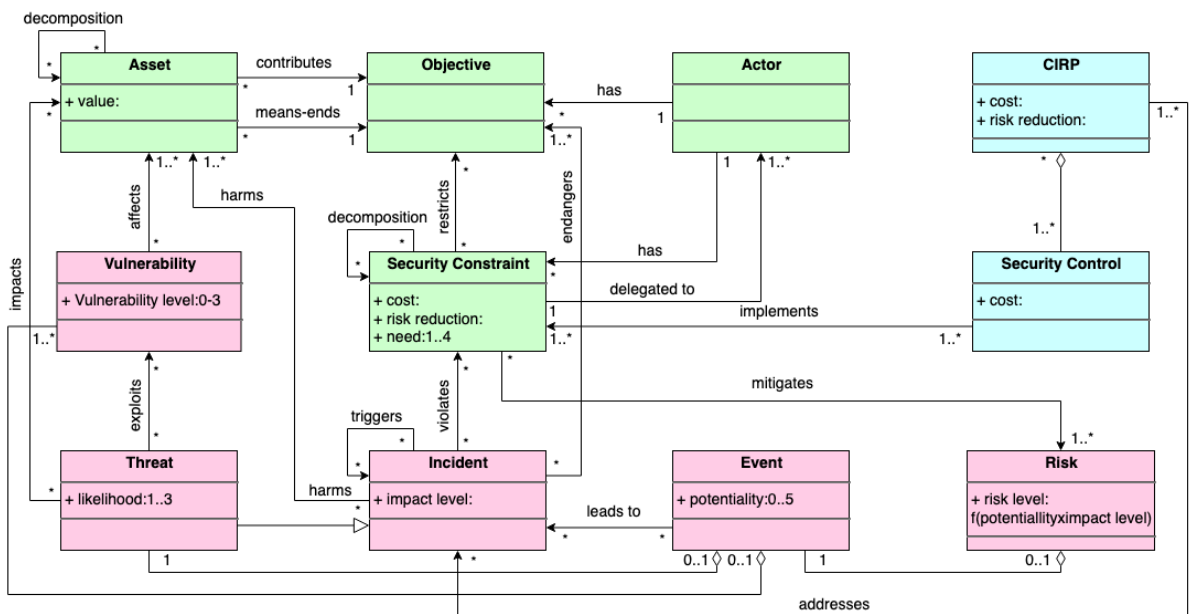


Figure 6.19: Enhanced BINA defensive-related constructs.

6.6.2 Abstract syntax extensions

In Section 6.4, we have not shown the abstract syntax of Secure Tropos due to the necessity for the simple introduction of the language itself. However, to show how the suggested syntactic Secure Tropos augmentations are used, we need to show the abstract syntax elements and the rules based on which they are merged.

The abstract syntax of Secure Tropos consists of a meta-model 6.20. Due to the need to reduce the presentation complexity, the meta-model is discussed in subsections. The first subsection focuses on the actor, the second on the goal and the third on attack scenarios.

Table 6.7: Defensive-related constructs.

BINA Constructs and relationships	Secure Tropos Constructs and relationships	Concrete syntax
Security control	(a) security requirements view (a combination of constructs including actor, goal, security constraint, security control, threat) (b) security attack view (a combination of constructs including actor, goal, security control, threat) (c) security mechanism	
CIRP	-	-
mitigates	mitigates	
implements	implements	
addresses	-	-

Fig 6.20 presents the Secure Tropos abstract syntax. The primary construct we focus at this point is the *actor* who can be a *depender* or a *dependee* in a *dependency* relationship. A *security constraint* is imposed to an *actor* that represents a restriction on a *goal*, *plan* or *resource*. A *security constraint* enriches the language by introducing the conception of secure dependency.

A *secure dependency* proposes one or more *security constraints* that must be satisfied for the dependency to be valid. They exist different types of *security dependency* that are represented using *depender* and *dependee* attributes of *security constraints*.

Moving on with the examination of the Secure Tropos abstract syntax, the second principal component is that of *goal*. *Goals* are achieved through *means-ends* relationships by satisfying other *goals*, *plans* or having available *resources*.

Returning to the *security constraints* that they are *imposed* to *actors*, the *restricts* relationship means that they can also affect *plans*, *resources* and *goals* of an *actor*. From a modelling perspective *security constraints* can be analysed through *decomposition* relationships and *assignment/delegation*. A *security goal* stands for the strategic interest of an *actor* with respect to security. When

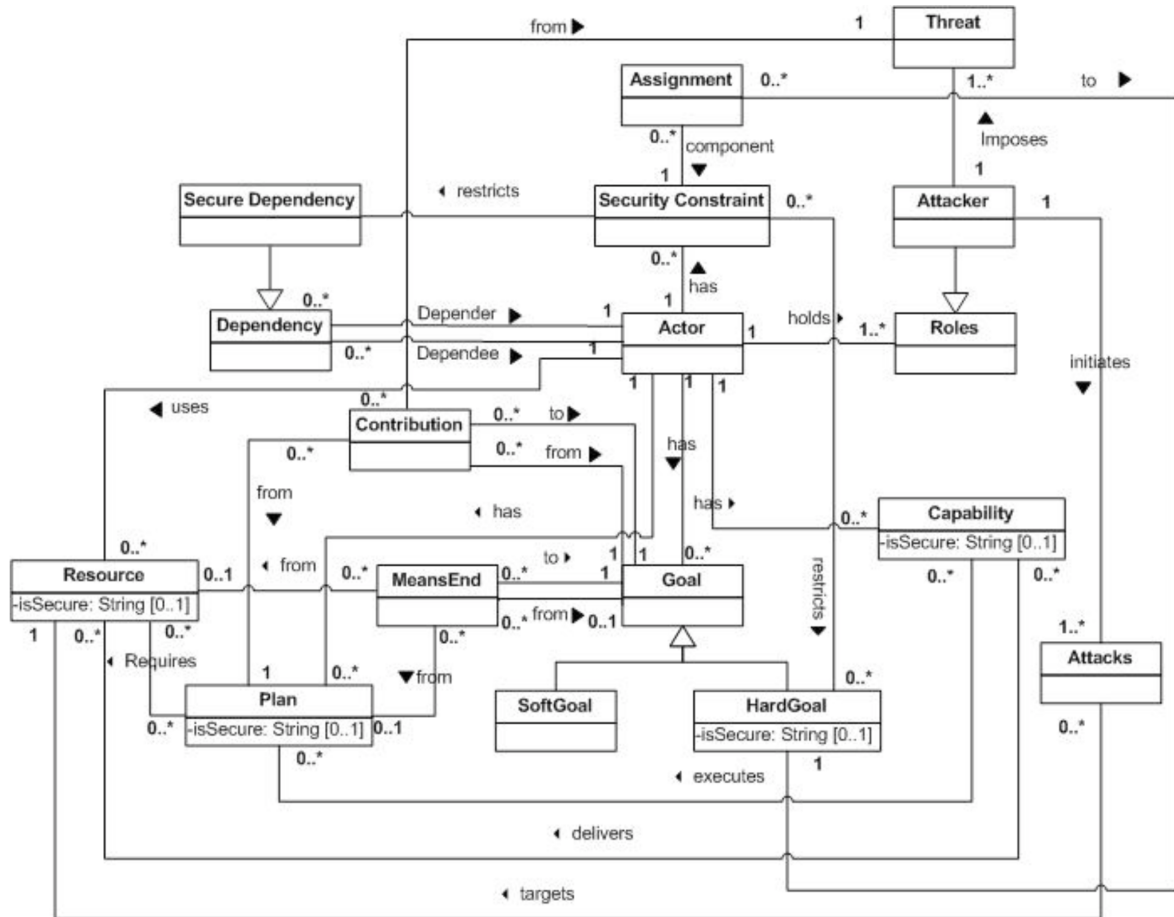


Figure 6.20: Secure Tropos abstract syntax [9]

security objectives are introduced they contribute to the satisfaction of security constraints and can have the form of *soft goals* and use the *satisfies* relationship. If a *plan* is a security-related plan, then it will contribute to the satisfaction of a security goal. For a *resource* when it is secure it means that is critical for the security of the system-to-be.

A *security constraint* is further associated with the *mitigation* of a *threat*. If a *threat* is not mitigated then it can *impact goals, plans* and *resources*. At the same time a *security constraint* can *restrict the goals, plans* and *resources* of an *actor* too.

Moving to **attack scenarios** we refer constructs that relate to cyber resiliency concepts. Here *actors* that are legitimate need to be distinguished from malicious *actors*. Malicious actors can also have *goals, plans* and *resources*. However, they use then to *exploit vulnerabilities* with the use of *threats* and attack methods. The *attacks* relationship indicates the connection of an *attacker* and a *resource*.

It is important to note that Secure Tropos metamodel has been enhanced, and it changes iteratively. Consequently, differences with the representations in the previous subsection might occur. However, they have been derived from the latest version of the Secure Tropos tool, SecTro v.2, and thus, they are equally relevant to our analysis. Overall they do not affect the main aspects of the language as discussed above. In the following subsection, we will present methodological guidelines for the resiliency-aware Secure Tropos application.

6.6.3 Application of resiliency-aware Secure Tropos

The purpose of this subsection is to explain how concrete and abstract syntax augmentations are used in an example. Here, we will use the running example and incrementally provide guidelines for modelling cyber resiliency-aware Secure Tropos models.

Language implementation comprises three main stages. The first stage covers the two first steps of the BINA process, presented in Section 6.1.2: *Determination of context and assets* and *Determination of security goals*. The second stage blends *Assessment and analysis of risks*. Lastly, the third stage matches to *Elicitation of security requirements* coming from *Risk treatment* decisions and leading to new *Selection and implementation of controls*.

Stage 1 - Determination of security objectives

At this stage, the concrete syntax of Secure Tropos deviates only insignificantly from the standard one and used in Section 6.4. As we explained in Section 6.4.3, we need to include the constructs that relate to the BINA domain model. We do this by constructing the organisational view using the constructs of *actor*, *objective*, *asset*, *security constraint* and the dependency relationships. In this way, the Secure Tropos organisational view that represents the organisational requirements in the form of objectives and security requirements in the form of constraints can be instantiated. This view offers a developer an overview of who is expecting what from the system-to-be. More importantly, it also captures the relations between internal and external to the system stakeholders/actors. In this view, we present only objectives (e.g. *Manage pharmaceutical projects*), assets (e.g. *Medical experimentation plans*) and constraints (e.g. *Preserve the integrity of experiments calculation*) related to organisational artefacts.

Based on the steps of the BINA process, we need to model security objectives. In Secure Tropos, it is possible to distinguish general security objectives (e.g., *Establish experiments calculation structure*) using goals and then to refine them using security criteria expressed with security constraints (e.g., *Preserve the integrity of experiments calculation*). This approach is a top-down security objectives identification. However, in Secure Tropos, it is more natural to define implicit security objectives as secure dependencies after defining the actor model. Then identified security constraints can be examined for security objectives of higher level for the system. This is a bottom-up approach.

What follows is the actor specific assets that show how the objectives and security constraints can be fulfilled. Here the main objective is to discover what assets need to be available to support an actor's objectives. The above is illustrated in Fig. 6.21 where a simple instantiation of the organisational view for Pharma Invent is presented. It is worth clarifying that the MHRA abbreviation stands for Medicines and Healthcare products Regulatory Agency, the UK body that gives regulatory approval to vaccines and the associated experimentations.

Stage 2 - Assessment and analysis of risks and incidents

At the second stage, we instantiate possible risks (threat and impacts combinations). We start by determining the security events that are represented as threat exploit vulnerability combinations. Fig. 6.22 focuses on a possible event of the risk to which the information system could be exposed, called *Authentication attack*. It represents a circumstance where a malicious actor mask as a legitimate user, acquires access to a system and damages the data in the *Database server*. The *Authentication attack* impacts the *Influenza vaccine production documentation*. The traceability

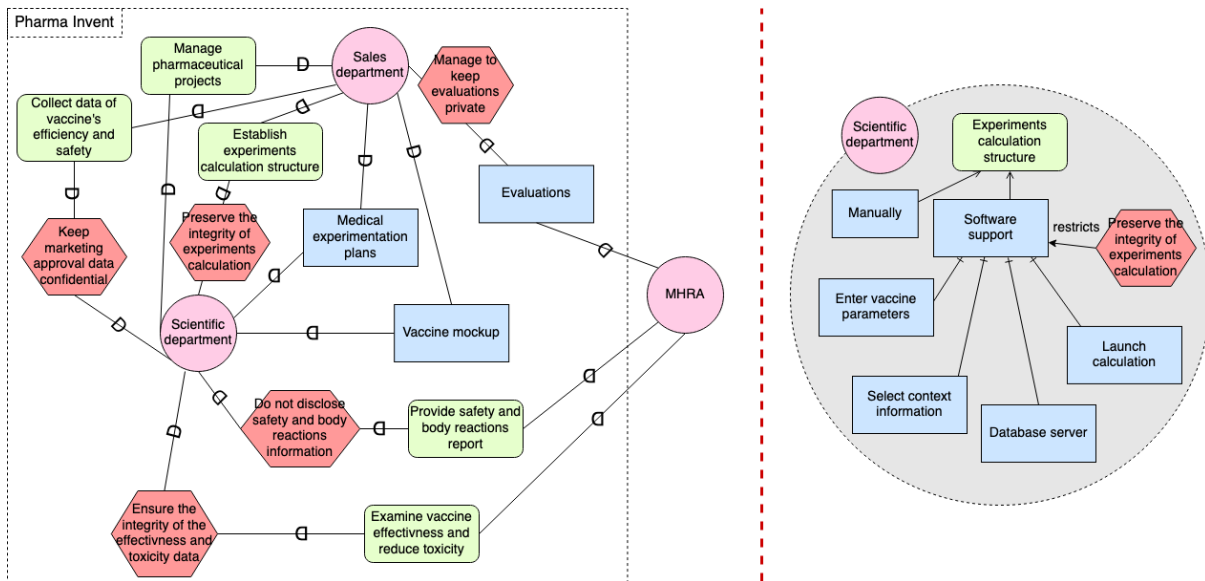


Figure 6.21: Organisational view of Pharma Invent

between *Influenza vaccine production documentation* and *Experiments calculation structure* shows the impact at an operational level. However, in this situation, *Influenza vaccine production documentation* can be interpreted twofold. Firstly, it can represent an *asset*, which is important for Pharma Invent as a business. Then the *impacts* relationship represents harm that the risk causes. Secondly, *Influenza vaccine production documentation* could be viewed as a security criterion, which needs to be represented. In this case, *impacts* defines negation of the security criterion.

After modelling the possible risk, we need to refine it in terms of threat, vulnerability, actor, security constraint and incident. This is done in the security attack scenario (cf. Fig 6.22). Here an *Attacker* has a threat *Social engineering* to an information asset *Software support* which support an objective *Experiments calculation structure*. The *Attacker* attacks *Software support* through exploitation of the vulnerability *Employee not security aware*. Thus the exploits relationship shows a link between a threat *Social engineering* and a *Employee not security aware* vulnerability. The presence of this vulnerability can cause the incident *Inappropriate use*, which subsequently violates the security constraint *Preserve the integrity of experiments calculation*.

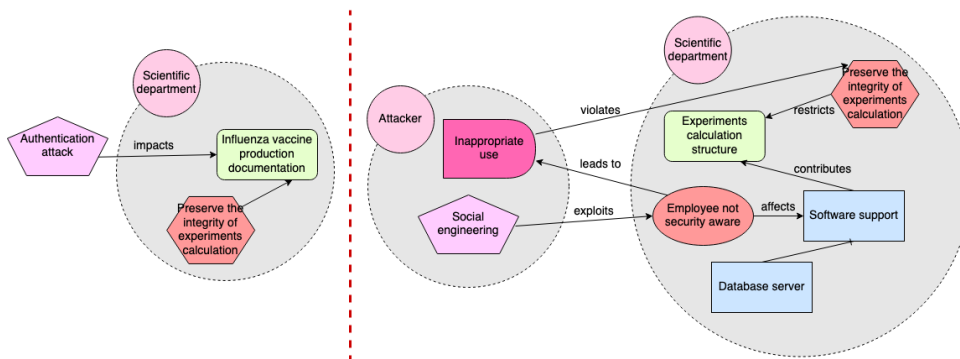


Figure 6.22: Security incident view of Pharma Invent

Stage 3 - Cyber resiliency requirements definition

In order to mitigate the identified risk and become resilient to attacks, such as *Authentication attack*, we have chosen as an example a risk reduction decision. This means we have to design objectives, assets, security controls, and CIRP to mitigate and increase resiliency towards this risk. In this instance, we add the security objective *Make all users security aware* and the security control *Perform security awareness training*. New objectives, assets, security controls and CIRP have a gradient background pattern to indicate that they represent resiliency security requirements in the diagram. In our example, the *Preserve the integrity of experiments calculation* becomes a resiliency security requirement mitigating the risk.

As discussed in Section 6.1.2, the BINA process is iterative. After defining resiliency requirements, one needs to test the system again against new possible risks and incidents. For example, the modeller can now identify internal threats. This will indicate the need for an analysis of new vulnerabilities and CIRP. The first iteration activity assumes new security constraints that become controls and are part of the system-to-be. From there, a risk analysis and resiliency assessment will be performed again using the updated design.

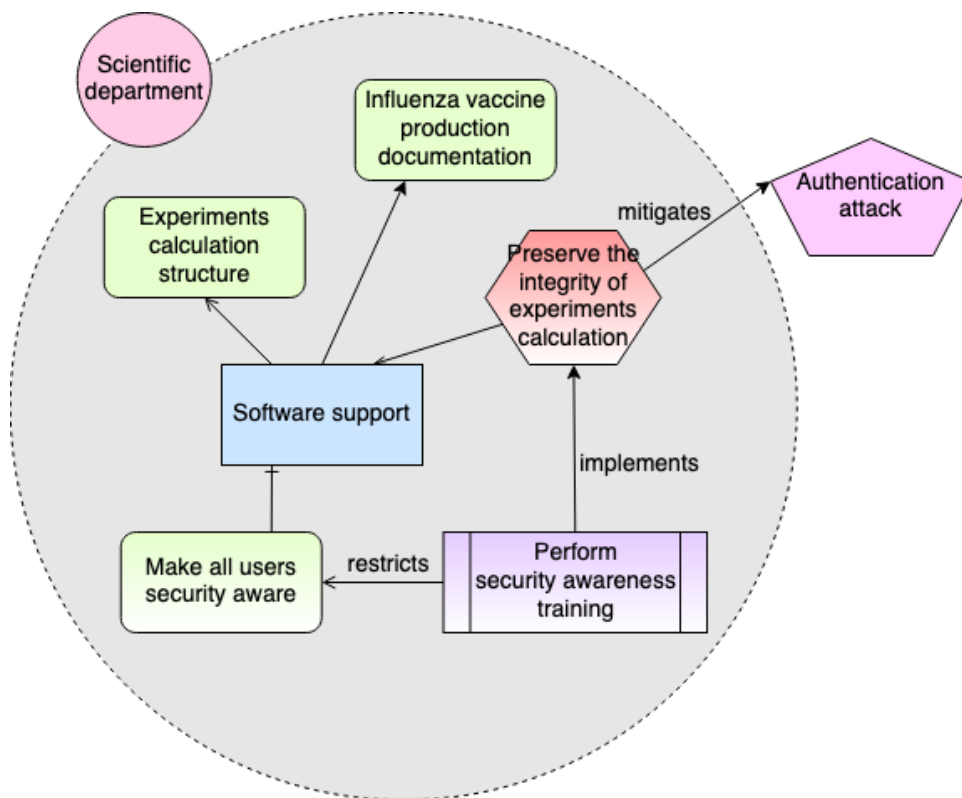


Figure 6.23: Resiliency requirements view of Pharm Invent

6.6.4 Theoretical evaluation

We will evaluate our proposal according to the principle of semiotic clarity [193, 194]. The principle of semiotic clarity defines that there should be a one to one correspondence between syntactic (graphical symbols) and semantic features (constructs). Differently, we need to address language issues, including redundancy, overload, incompleteness and under-definition.

Redundancy

Redundancy expresses that two language constructs have the same or overlapping semantics. Redundancy problems concerning BINA were found in Secure Tropos and discussed in Section 6.4.3. In the cyber resiliency-aware Secure Tropos, we have limited redundancy by proposing different visual constructs to model offensive-related constructs. Redundancy also seems to exist to the same degree within all the constructional groups (domain, offensive, defensive). For example, a BINA *asset* can be represented using Secure Tropos constructs for *actor*, *plan* and *resource*. But, according to the BINA *asset* definition, we need means to show information and processes. That shows that it is not necessarily all the times redundancy a restriction. Similar needs can also be found within the other two constructional groups.

A BINA *security constraint* can be designed either by a Secure Tropos *goal* or a Secure Tropos *security constraint*. This equivalence is not used for the same modelling purpose. We design abstract *security constraints* using *goals* and more specific *security constraints* using the Secure Tropos *security constraints*.

As discussed earlier, the construct of an *event* is represented by a *threat* or by a set of constructs. Expectedly, this division of constructs to varying levels of abstraction give better model analysis opportunities and helps the user to find the information provided in the diagrams. However, this needs validation in empirical contexts.

Overload

Overload is present if the same language construct has several meanings. In BINA, there is a link *impact* which stands for negation impacts and also for actual harm to the constructs of the BINA domain model. We recognise this overload and accept it because it allows the language to remain relatively simple (i.e., without too many modelling constructs). Also, it allows for capturing the semantical difference in the label of the impacted construct (asset).

Incompleteness

Incompleteness arises when a language does not carry data on a specific occurrence. For the incompleteness, we need to examine constructs that, although present in the BINA domain model, are skipped in the cyber resiliency-oriented Secure Tropos. For example, *CCoA* and *residual risk*.

We do not set a visual construct for *CCoA* because this construct does not present any alteration made to the modelled information system. This construct stands as a justification and indicates the modeller's conscious decision. Nevertheless, it needs to be included in the system specification and the generated information system model, using different ways.

In resiliency-aware Secure Tropos, we do not define the construct of *risk*. Instead, we design it as an aggregation of *threat* and *impacts* relationship. This means that the BINA relationship *mitigates* is not explicitly represented by a link. Yet, we can implicitly identify this relationship by analysing connections between *security constraints* and the respecting *risk*.

Because of the overlapping semantic of the relationship of the *impacts*, we can only implicitly define *triggers* relationship. It is defined through multiple uses of the *impacts* link. However, the language alone does not allow modelling, which impact has stimulated which impact. This information needs to be captured utilising other means.

Some constructs included in the cyber resiliency-aware Secure Tropos are viewed conversely than how they are defined in the BINA domain model. For example, when analysing the BINA *threat*, following the principles of Secure Tropos, we set the *actor* as a malicious actor and the *assets* as assets required for an attack.

Besides, the BINA *event* consists of threat and vulnerability. In the case of resiliency-aware Secure Tropos, we model *event* either as a *threat* or a combination of *actor*, *goal*, *asset* and *exploits*. In this case, we are not able to identify the precise *vulnerability*. This means that real vulnerability needs to be specified using other means.

Under-definition

Under-definition occurs when a language construct has no semantics. In BINA, we do not identify any under-definition problems.

Overall, our proposition has few limitations concerning Secure Tropos, from which it was initially derived. In this research, we have emphasised that our objective is to generate a security cyber resiliency management approach suitable for the early stages of a system-to-be. In other words, we do not consider Secure Tropos extensions that address later stages of a system's development. We recognise that these extensions are essential for the later stages of a system's development. Still, for cyber resiliency-aware Secure Tropos, they require additional investigation, time and resources not available within the limitation of this research project.

6.7 Summing-up the Assessment of BINA

This section gives an outline of the outcomes for the various sections of this chapter.

6.7.1 Research method

This chapter aims to evaluate the BINA support of security-oriented modelling languages. Following the research method suggested in Section 6.1, we analyse KAOS, Misuse cases and Secure Tropos. We present which construct for the languages could be used to support one or more BINA constructs and give some reasons for these assumptions. The research method does not include any quantitative assessments of the correlations or non-alignment between BINA constructs and the security-oriented modelling languages constructs, like, e.g., no correlation, marginal, partial, total. However, such a quantitative estimation has considered being too risky in our context. The results we might get would not have been reproducible. The quantitative level of correlation might be indeed inconsistent based on the individuals involved. Moreover, such an evaluation would have been challenging to set up, primarily regarding our time frame.

6.7.2 Assessment of BINA support by security-oriented languages

This section's contribution is that it highlights the coverage level of BINA constructs by security-oriented languages. In most cases, the modelling languages under study have not been initially designed with security in mind. Such aspects have been gradually introduced and have enhanced existing languages because of the growing importance of cybersecurity. Consequently,

such languages have gradually included security and risk constructs without a real systematic language design approach. Moreover, most languages are focused on specific phases of the system design life-cycle. Accordingly, depending on the recognised focus, some languages put more emphasis on the risk management required for the business (i.e., *security goals, security requirements*) like Secure Tropos, while others, more oriented towards late requirements and design, cover constructs like information system assets, vulnerabilities and countermeasures in their scope, like KAOS.

6.7.3 Review of language association

Tab. 6.4 reveals what is missing in term of constructs for the three analytically examined languages to support the BINA domain. The main observation concerning the coverage table is that currently, no perfect correlation for BINA is provided by any existing requirements engineering modelling language. Although the languages include some risk constructs, their approaches are not complete regarding BINA and cyber resiliency. The coverage table assists in picking the most suitable language, considering the modelling scope of the analyst as well as the demanded constructs and related activities. For example, Misuse cases seem sufficient for obtaining threats, malicious actors and cyber attacks, whereas Secure-Tropos will be more suitable for identifying assets and associated security constraints of the design.

This table can also show interoperability between security-modelling languages. Since some languages are better suited to support some resilience-related activities than others, they can be used in a complementary manner during information system development. The coverage table provides a reference for connecting different languages at the BINA conceptual level. Moreover, a satisfied language user would not be pleased if he must change this language for another to be able to perform BINA at the requirements engineering level.

6.7.4 A cyber resiliency-aware Secure Tropos

During the assessment of the language, suggestions for improvement were made. Based on them, we have extended both language syntax and semantics in order to comply with the BINA. These extensions have resulted in the cyber resiliency-aware Secure Tropos. In addition to the language itself, we have defined methodological guidelines for applying the language illustrated through the running example.

It is generally a challenging task to define a helpful modelling language, producing models in the sense that they help to communicate effectively [195]. A trade-off needs to be found between extending a language to enhance its expressive power and keeping it simple. Cyber resiliency-aware Secure Tropos should thus be evaluated through additional criteria [195]. The outcomes are discussed in a theoretical evaluation for semiotic clarity. An experiment in a real environment should complement this discussion. Such an experiment would provide evidence of the effectiveness of this extension to support BINA and highlight its weaknesses.

6.7.5 Discussion and Closing Remarks

In this chapter, security-oriented languages were compared to the BINA domain model. The goal was to assess their coverage level for BINA constructs.

Initially, a research method was introduced. This research method explains how we proceeded to examine a language concerning the BINA domain model. The languages analysed

were KAOS, Misuse cases and Secure Tropos. Then, a summary of language comparison and ways of enhancement for a better coverage level was proposed, and some preliminary remarks were suggested for (PCySeMoL)-Cy-2, CySeMoL and the Tropos Goal-Risk framework, based on our current knowledge of these languages.

The identified ways of enhancement were then examined for Secure Tropos. We proposed a concrete and abstract syntax extension of Secure Tropos. This extension was applied to the running example. Finally, an evaluation of this extension was performed based on the principle of semiotic clarity. The chapter ends with relevant conclusions.

Chapter 7

BINA Process and Tool

This chapter outlines our systematic approach to model the alignment of organisational needs with security concepts in resilient computing systems. This approach can guide developers by capturing resilient computing systems through modelling techniques, defining stakeholder requirements and security needs. Each step of the process assembles a holistic view of the system-under-design, represented through models comprising system needs and resiliency-specific security properties from a security requirements engineering perspective. The approach outlines the types of analysis supported and the developer's requirements to perform semi-automated reasoning. We also indicate where input from security requirements engineers or incident response teams are required.

7.1 Overview of the BINA process

Before we present the BINA process, it is essential to clarify that the BINA process was designed based on the literature and the specific constructs of the BINA domain model. More precisely, we reviewed existing methodologies' steps to determine and analyse cybersecurity requirements. Then we formulated a series of common steps as identified in the literature and presented them in Section 6.1.2. From there, we looked at the constructs of the BINA domain model and its purpose for designing. We used small scale case studies to apply alternative ways to instant the constructs and generate new information. After trials and errors, we reached the understanding that it is more meaningful to express what we aim for resiliency-wise and find ways to achieve it under various circumstances, rather than designing everything that might go wrong and attempting to establish in that way what we need as system-to-be to have as requirements. Based on that assumption and existing practices in the domain, we designed the BINA process.

We present an iterative process that supports developers to systematically capture and refine resilient systems relationships, security properties and organisational needs. Each activity represents a step that contributes towards defining and constructing a resilient environment model representing the system-under-design. For each activity, we also specify the steps and relevant artefacts. These activities are placed after the requirements elicitation and before the requirements specification. We use the Software and Systems Process Engineering Metamodel (SPEM) specification (SPEM 2.0) to specify the process, the activities, the steps, the artefacts and the roles involved. An overview of the BINA Process is shown in Fig 7.1 with the following activities:

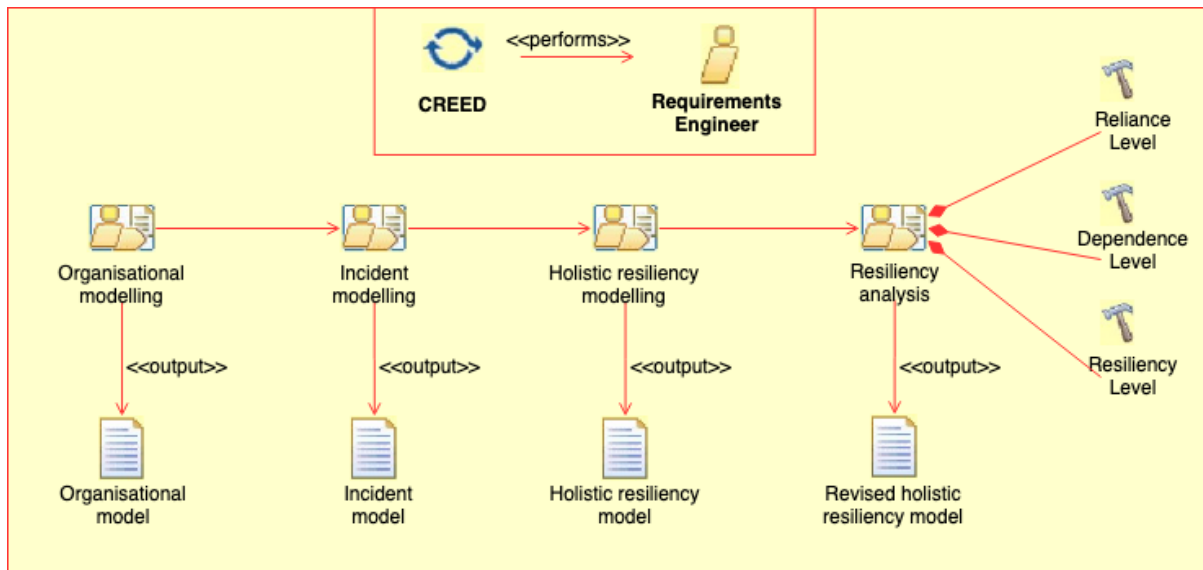


Figure 7.1: BINA process.

- **Organisational modelling:** identify organisational objectives, stakeholders, assets, security constraints and relationships, producing an organisational model as output.
- **Incident modelling:** identify and configure incidents and CIRP, generating a list of incident response services as output.
- **Holistic resiliency modelling:** refinement of incident-specific constructs focusing on the system-under-design to output a resilient environment model.
- **Resiliency analysis:** performing analysis techniques from the resilient security analysis, incident management and transparency to support developers identify and understand the resiliency security requirements of the system-under-design.

7.1.1 Activity 1: Organisational modelling

The cyber resiliency analysis of the system-to-be begins with the modelling of the organisational context. The main focus of this activity is to understand the organisational and system requirements. It contains four steps: actor identification, goal identification, security constraints identification and dependencies identification. Fig. 7.2 depicts the organisational modelling activity with its steps and relevant artefacts.

In the first step, the security engineer identifies the actors of the system-to-be, including the technical assets, the human actors of the system environment, and other technical actors of the system environment. Human actors are usually the system's stakeholders, while the other technical actors are systems utilised under development. The developer can identify such information in organisational documents and interviews with the stakeholders and models produced by security engineers.

In the second step, stakeholders sometimes explicitly state goals or in preliminary material available to requirements engineers. However, if they are implicit, the goal elicitation will have to be undertaken. Goals can also be identified systematically by searching for intentional keywords in the preliminary documents and interview transcripts. The preliminary analysis of an existing system is an essential source of goal identification. Such analysis usually results in

a list of problems and deficiencies. Negating those issues yields a list of goals to be achieved by the system-to-be. Once an initial set of goals and requirements is obtained and validated with stakeholders, many other goals can be identified by refinement and abstraction. For instance, by asking 'how' and 'why' questions about the goals and requirements available.

In the third step, the security engineer refines or introduces the security requirements with security constraints that restrict goals. The security engineer can identify them from the high-level goals of the stakeholders and, at this step, refine them as security-specific goals and model them as security constraints to specific goals. Moreover, the security engineer can also use security policy documents as an input for this stage of modelling, inheriting to the system-to-be more generic organisational security requirements.

In the fourth step, the requirement engineer models the dependencies. The actors cannot consistently achieve goals by themselves. For these goals, the security engineer has to seek actors that can achieve them and specify the correspondence between the goal that the depender cannot achieve and the corresponding goal of the dependee. Based on the correspondences between goals, the dependencies are then specified. Therefore the relationships where an actor depends on another actor for a goal can be identified.



Figure 7.2: Organisational modelling activity.

Overall, organisational modelling is an activity of the cyber resiliency process, where we assume that the input is either an existing goal model or constructed by the developer based on existing requirements. In the latter case, we assume that security requirements engineers have carried the process of eliciting system needs, analysis and production of requirements, and the developer has access to the requirements of the system-under-design. We make this assumption that the process for producing goal models of existing software systems or from initial requirements falls out of the scope of this thesis. Due to the maturity of established work in requirements engineering, we do not attempt to redefine the existing process of goal modelling. Instead, we focus on extending the existing work to capture security requirements issues in resilient computing, building upon goals models to represent these concepts. In this case, we use the SecTro modelling tool to design organisational models from existing requirements because the Secure Tropos methodology provides a goal-oriented approach in security requirements engineering. Consequently, the output of this step would be the organisation goal model.

7.1.2 Activity 2: Incident modelling

The purpose of the second activity of the secure resiliency process is to identify a list of incidents and Cyber Incident Response Plan (CIRP) based on the requirements of the system-under-design. We input an organisational goal model from Activity 1 and produce, as output, a list of incident response services and an incident model. The incident modelling activity consists of two steps: model the incidents and model the CIRP that the incident response team may introduce and resolve them as well until no further incidents are introduced (cf. Fig. 7.3).

1	Activity {kind: phase}: Organisational modelling
2	ProcessPerformer {kind: primary}
3	RoleUse: Requirements engineer
4	WorkDefinitionParameter {kind: in}
5	WorkProductUse: List of organisational processes
6	WorkDefinitionParameter {kind: out}
7	WorkProductUse: List of actors
8	WorkProductUse: List of goals
9	WorkProductUse: Goal models
10	Steps
11	Step: Study organisational processes
12	Step: Identify actors
13	Step: Identify high level actor goals
14	Step: Model actors
15	Step: Model high-level goals
16	Step: Refine actors' goals
17	ProcessPerformer {kind: primary}
18	RoleUse: Requirement engineer
19	WorkDefinitionParameter {kind: in}
20	WorkProductUse: List of high-level goals
21	WorkProductUse: Goal models
22	WorkDefinitionParameter {kind: out}
23	WorkProductUse: List of dependencies
24	WorkProductUse: Organisational model
25	Steps
26	Step: Model system and actors
27	Step: Refine goals
28	Step: Identify security constraints
29	Step: Model security constraints
30	Step: Identify dependencies among actors
31	Step: Model dependencies among actors

In the first step, the requirement engineers identify past and possible incidents. Next, the engineer must consider the different types of incidents, i.e., experiential, reported, normative, internal and external, and the impact level they can have on the system-to-be. This activity will enable the requirement engineer to decide if there is an impact and the reason behind this incident by modelling the appropriate 'harms' relation.

In the second step of this activity, the requirements engineer models the suitable incident responses reported by the organisation. Reported resolutions introduce a way to address one or more incidents. The overall activity is iterative and ends when there are no incidents left without suitable incident response or if there are any unresolved incidents, no suitable incident response could be found. In the former case, the engineer can move on to the next activity. In the latter case, however, the resiliency analysis activity should be followed.

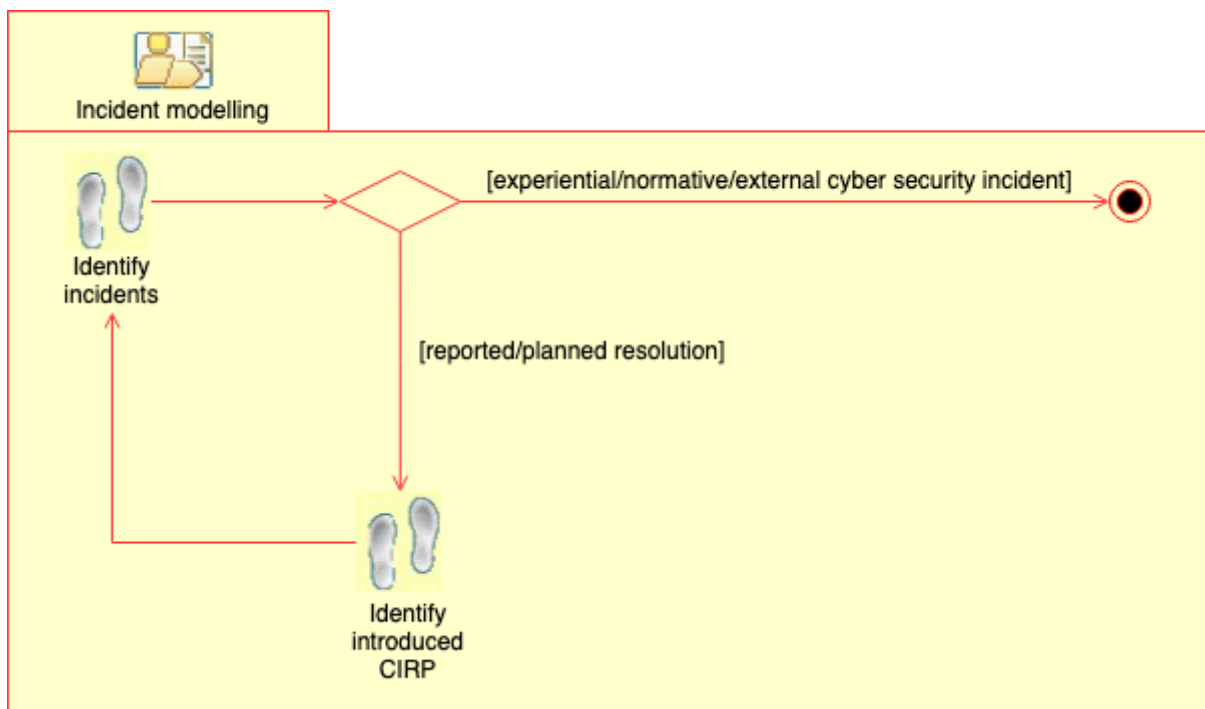


Figure 7.3: Incident modelling activity.

1	Activity {kind: phase}: Incident modelling
2	ProcessPerformer {kind: primary}
3	RoleUse: Requirements engineer
4	WorkDefinitionParameter {kind: in}
5	WorkProductUse: Organisational model
6	WorkProductUse: List of dependencies
7	WorkDefinitionParameter {kind: out}
8	WorkProductUse: List of incident response services
9	WorkProductUse: Incident model
10	Steps
11	Step: Identify system-related cybersecurity incidents
12	Step: Model incident
13	Step: Identify type of incident response and cyber resiliency
14	Step: Model incident response and cyber resiliency
15	Step: Identify new system-related cybersecurity incidents
16	Step: Model possible new incident response and cyber resiliency

7.1.3 Activity 3: Holistic resiliency modelling

In the third activity, the Cyber Incident Response Plans (CIRPs) is specified and validated. The Cyber Incident Response Plans (CIRPs) represent the resiliency assumptions that underlie the system under development. This activity starts with the specification of related security

controls and the collection of evidence to examine the validity of the Cyber Incident Response Plans (CIRPs) (cf. Fog. 7.4).

In the first step, the requirements engineer will specify the security controls that relate to Cyber Incident Response Plans (CIRPs). In the second step, the security engineer collects evidence related to threats, vulnerabilities, events and risks. This information derives from experience, reports, regulations, agreements with third parties and lists of existing controls.

In the third step, the requirements engineer examines the validity of Cyber Incident Response Plans (CIRPs) because if not valid, then there will be a potential weakness to the system-to-be that can affect its resiliency. The validity property of a Cyber Incident Response Plan (CIRP), named risk reduction, takes Boolean values true or false. If the Cyber Incident Response Plan (CIRP) is valid, then the risk reduction is set to true; otherwise, it is set to false.

Based on the results of the Cyber Incident Response Plans (CIRPs) validation, the requirements engineer can calculate the resiliency level of the Cyber Incident Response Plan (CIRP). Ideally, it should be 100%, but it is up to the requirements engineer to decide the level upon which he considers that the incident is contained and eradicated. If the resiliency level is 100%, then there is the reliance that the system-to-be will indeed contain and eradicate the incident as expected. Otherwise, there is no reliance that the resiliency will be helpful, and additional Cyber Incident Response Plans (CIRPs) is required by the system-to-be to enforce the desired resiliency.

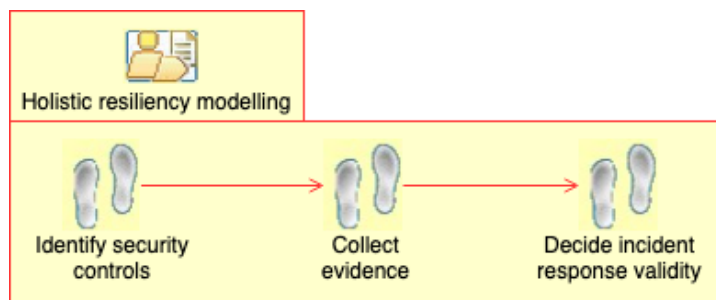


Figure 7.4: Holistic resiliency modelling activity.

1	Activity {kind: phase}: Holistic resiliency modelling
2	ProcessPerformer {kind: primary}
3	RoleUse: Requirements engineer
4	WorkDefinitionParameter {kind: in}
5	WorkProductUse: List of incident response services
6	WorkProductUse: Incident model
7	WorkDefinitionParameter {kind: out}
8	WorkProductUse: Resiliency model
9	WorkProductUse: List of valid incident response services
10	WorkProductUse: List of invalid incident response services
11	Steps
12	Step: Identify security controls based on incident response services
13	Step: Collect evidence related to threats, vulnerabilities, events and risks
14	Step: Check the validity of the incident response services

7.1.4 Activity 4: Resiliency analysis

The fourth activity of the BINA process measures the resiliency of the system-to-be. The measurement can be applied for all the actors of the information system, but we believe the most helpful approach is to measure the resiliency of the technical system-to-be. Assessing the system under development at the requirements stage is beneficial to identify potential resiliency vulnerabilities or implementational bottlenecks and address them as early as possible. Oth-

erwise, any possible fix at a later stage will cost more resources, such as time and money. Moreover, if potential incidents are left unidentified and resolved adequately if the system is implemented, it may fail to meet its goals, and users will not accept it. This activity contains four steps: assignment of importance level to the top-level Cyber Incident Response Plans (CIRPs), assignment of confidence levels to the bottom level Cyber Incident Response Plans (CIRPs), calculation of the resiliency levels, calculation of the system resiliency (cf. Fig. 7.5).

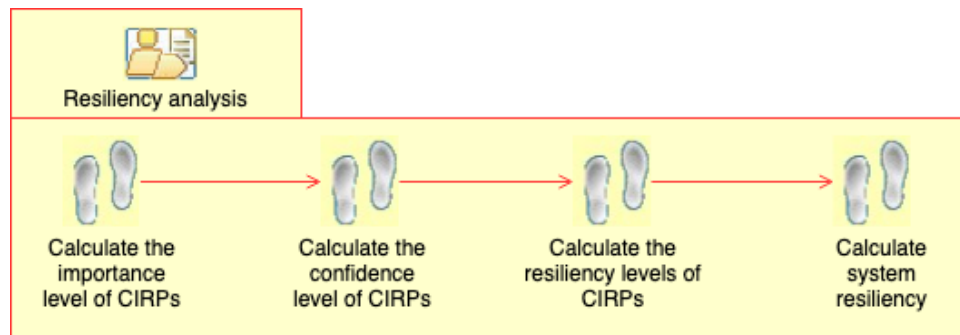


Figure 7.5: Holistic resiliency modelling activity.

In the first step of this activity, the top-level Cyber Incident Response Plans (CIRPs) of the system-to-be are assigned an importance value. The stakeholders are responsible for providing essential values to the top-level Cyber Incident Response Plans (CIRPs) of the system-to-be. The range of importance is from zero (not important) to one (important).

During the second step, the lowest level Cyber Incident Response Plans (CIRPs) are assigned with reliance levels. The reliance level is one of the actors can achieve the Cyber Incident Response Plans (CIRPs) by himself; zero is the actor cannot achieve the Cyber Incident Response Plans (CIRPs) by himself. The reliance values will be propagated to the higher-level Cyber Incident Response Plans (CIRPs) until the top-level Cyber Incident Response Plans (CIRPs). In case the actor cannot implement the Cyber Incident Response Plan (CIRP) by himself and depends upon another actor for this Cyber Incident Response Plan (CIRP)'s implementation, the reliance level takes the value of the dependence level. The dependence level of a dependency shows the degree of reliance in the fulfilment of dependency, is calculated as:

$$D = \left(\frac{\text{ValidCIRPs}}{\text{TotalCIRPs}} \right) \times \text{RelianceLevel} \quad (7.1)$$

Where the RelianceLevel is the reliance level of the corresponding of the Cyber Incident Response Plan (CIRP) dependee actor.

SR is the system resiliency level, which shows how reliable the system is, i.e., how certain we are that the system will meet its resiliency requirements. I is the importance of the high level Cyber Incident Response Plan (CIRP) to the overall system resiliency, and the requirement engineer defines it. If n is a set of direct system dependencies, then the system resiliency is calculated using the following formula:

$$SR = \left(\frac{\sum_{x=1}^n I_x \times R_x}{\sum_{x=1}^n I_x} \right) \times 100 \quad (7.2)$$

7.2 Tool description

The design of modelling languages aims to a shared understanding and the support of automation. We decided to design a tool that supports the BINA framework implementation

because

- learning the graphical syntax and using it manually can be challenging for users; a tool simplifies that and allows testing from third parties.
- it allows supporting the framework's application by allowing us to encode the automation we propose.
- we used the tool as a first test into the applicability of the theoretical components of our research.
- We wanted a tool to act as a graphical editor to instantiate models meaningful for cyber-resilient healthcare systems.

For those reasons, we designed the BINA tool to capture and connect graphical notation with the meta-modelling rules ensuring validity. We also wanted the BINA tool to instantiate the context within which incident response occurs, along with the risks and dependencies among sociotechnical system components. Based on the above, the tool also needs to capture the relevant resiliency metrics and allow adjustments based on the new information acquired.

For implementing the BINA tool, we used C# to run as an independent application initially. Hence, in early versions, the tool was built using the Electron library. Electron [196] uses Chromium and Node.js to allow developers to built apps with HTML, CSS, and JavaScript. Practically the tool is a web application that uses Electron to operate as both a desktop and web application. As a web application, we wrote it using the Microsoft framework Blazor [197]. All of the tools, applications and frameworks used are Open-source.

The main graphical user interface (GUI) consists of the drawing canvas, the menu bar, the toolbar, and the properties panel. The drawing canvas is where the developer is incrementally constructing the BINA model, while the menu bar has the standard functions, such as creating a new model, opening the model, saving, and so on. Finally, the toolbar contains elements and links that correspond to constructs in the BINA metamodel.

We developed the BINA tool based on the principles of agile software development. In other words, we discovered requirements and solutions, gradually collaborating with users. We remained flexible to changes based on adaptive planning and continual improvement.

To download the tool, using Windows as your operating system, please download the software from https://mega.nz/file/8hwgEY4R#SeSVmuuSFc2sSN030Qkva7xEe8fCEBrLJNfeEhmI_Z0. After you unzip the file, open the application. When the tool asks for credentials, enter for user: admin and for password:123456. Then click the *Designer* from the list on the left-hand side.

7.2.1 Constructs graphical notation

There is the inherent difficulty associated with grasping new constructs and learning new notations. The development of a tool and its artefacts support the increase of familiarity and applicability with a methodology. Using a tool should not require more cognitive overhead than learning how to use the techniques associated with the BINA methodology. We need to introduce new notations, and we need to do it so that the visual complexity does not increase. Therefore, we designed the new graphical notation in resemblance to the existing graphical notations of the actor and goal of Secure Tropos. Fig. 7.6 shows the notations of the constructs used in the BINA methodology.

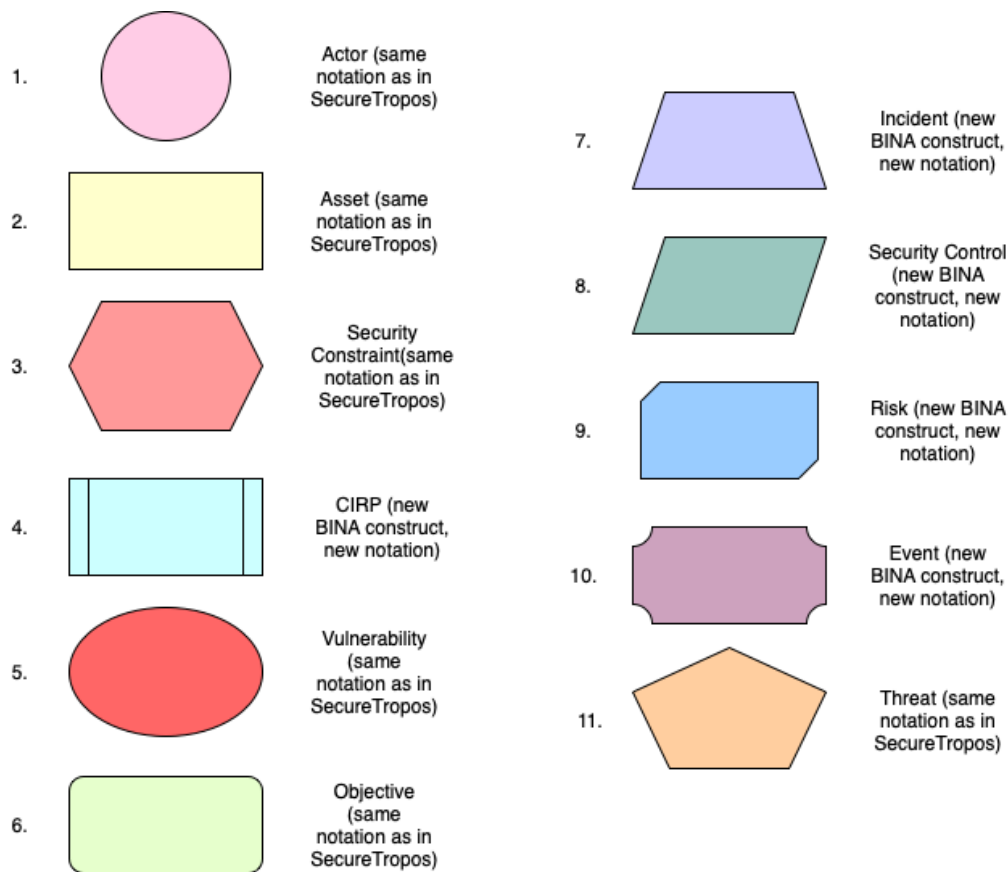


Figure 7.6: Constructs notation.

Each construct has relevant properties, and some of these properties have specific values, such as in cases where they take a Boolean value. These properties are critical as they enable tool-assisted automation of the resiliency analysis. Fig. 7.7 shows these properties and some of the values they take based on lists in the form of enumerations, Boolean values and manual input.

An essential part of automation is related to the relations among constructs, expressed graphically as links between nodes. These links determine how constructs relate to each other. This is the base for the validation of a model that a designer creates. It allows validating if a model has been designed based on the meta-model. Fig. 7.8 shows these relations along with the constructs that they connect.

7.2.2 BINA tool functionality

Researchers design modelling languages to enhance understanding through graphical representations and automate part of the process for the user of a relevant tool. This section presents the semi-automated analysis that a requirement engineer can perform on BINA models. The analysis uses the enumerated values of the metamodel's constructs and the metamodel's rules to produce results. The requirements engineer's input is partially part of the process. The effort that the security engineer puts into created these models will inform him about:

1. the validity of the models based on the metamodel rules;
2. the applicability of the Cyber Incident Response Plans (CIRPs) within the specific context

List of Properties

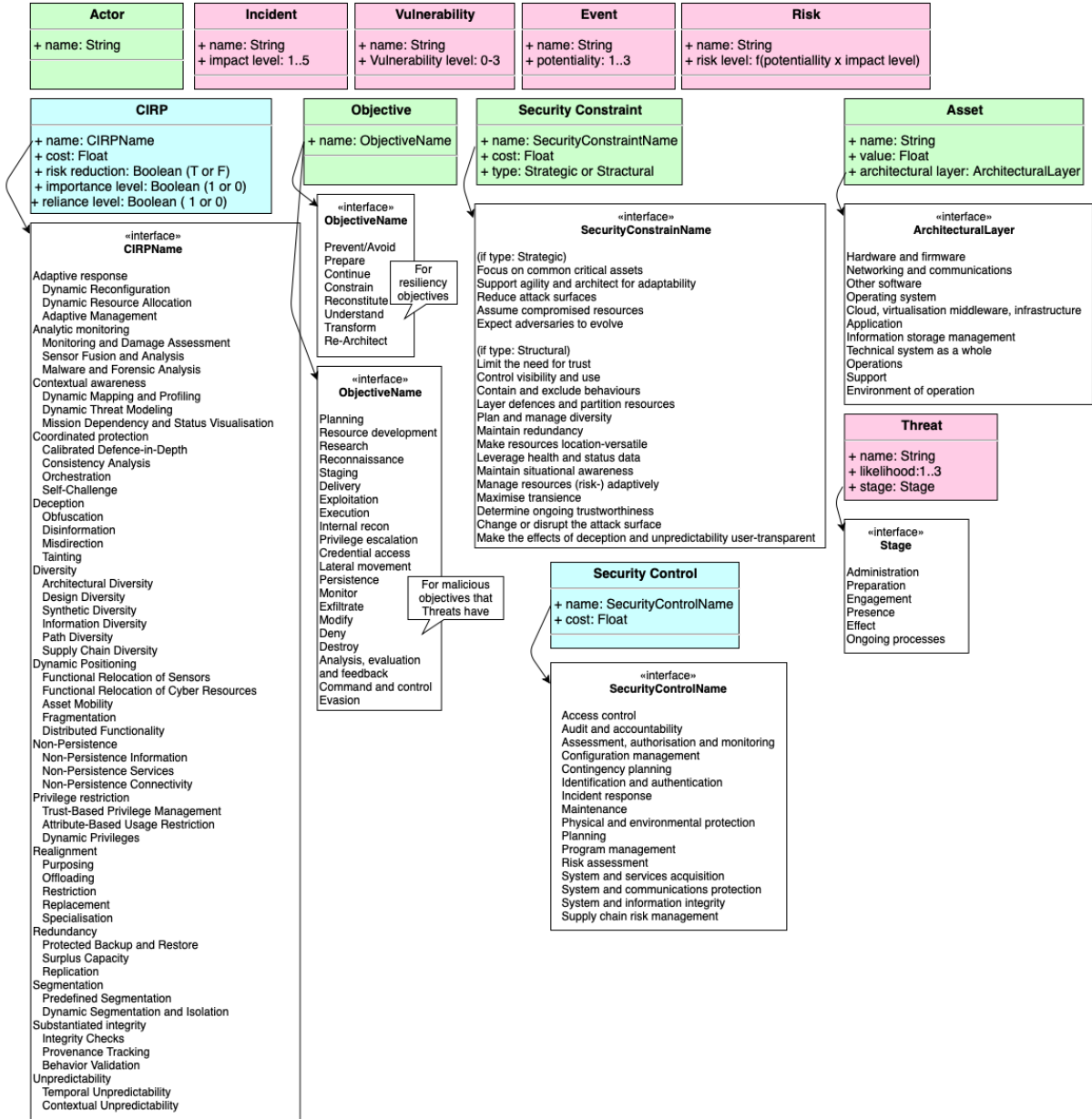


Figure 7.7: Constructs properties.

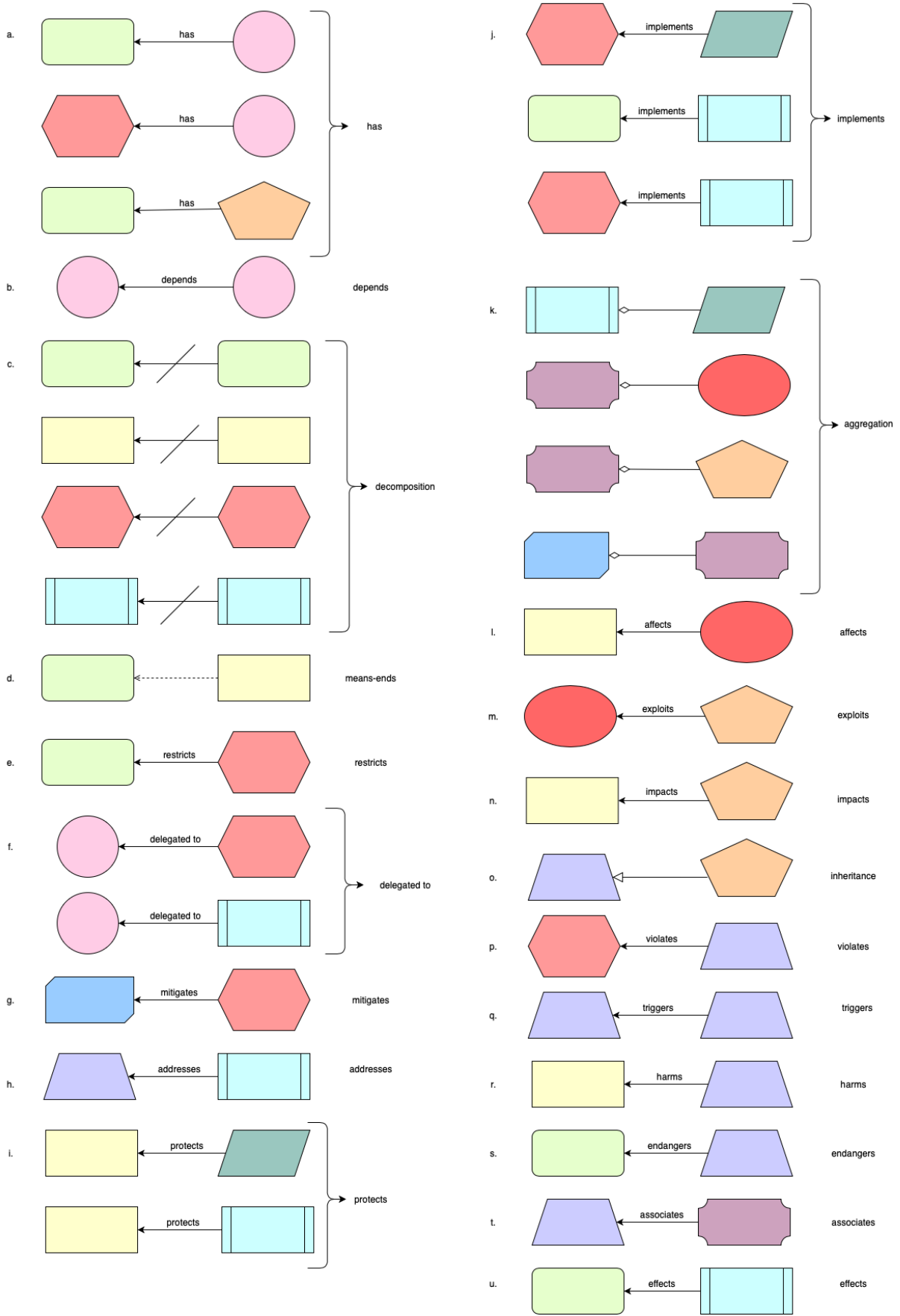


Figure 7.8: Relations among constructs.

s/he is analysing;

3. the risk that has not been managed at a satisfactory level based on the requirements engineer's choices;
4. the overall dependence and system resiliency.

Model validation based on metamodel rules

The Build In iNcident response Analysis (BINA) tool is a tool for constructing and analysing BINA models as part of the cyber resiliency analysis of the system under development. The main functionalities of the BINA tool are to support the modelling activities of the cyber resiliency process. The tool allows developers to draw BINA graphical models using a pallet of shapes. Standard features such a saving, zoom, cut, copy, and paste is provided as well. The tool also checks the syntactical correctness of a model through the validation button. For example, if the developer attempts to connect two constructs that cannot be connected with a relation, the tool will show that that action follows the metamodel. The implementational metamodel is shown in Fig. 7.9.

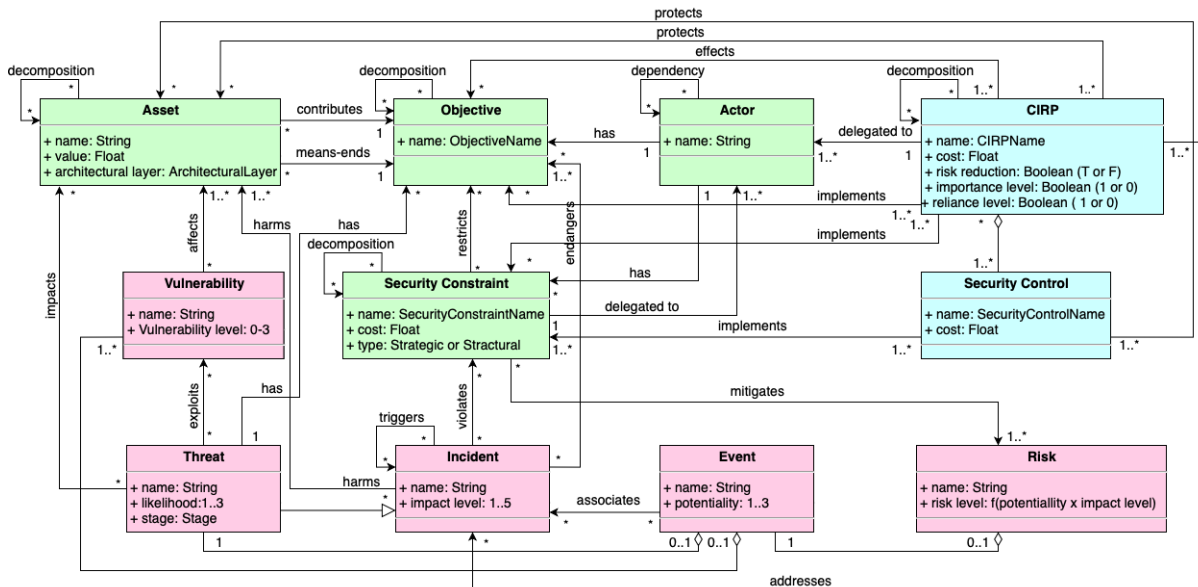


Figure 7.9: Implementational metamodel.

Analysis of CIRP

After the incident and resiliency modelling activities, the developer might want to assess the actual correlations among potential Cyber Incident Response Plans (CIRPs) and the other constructs that can affect each other in different ways. The BINA tool allows the analysis among the various Cyber Incident Response Plans (CIRPs) as well as their relations with objectives, security constraints, assets and security controls. More specifically, the tool analyses:

- if and how the modelled CIRPs implement the recovery-related objectives;
- if and how the modelled CIRPs implement the structural security constraints;
- if the modelled assets' architectural level corresponds to the introduced CIRPs;

- security controls aggregate to form the modelled CIRPs;
- how CIRPs effect malicious objectives of threats;
- what are the effects of CIRPs decomposition relations among their own (i.e., they support, depend, use or conflict with each other).

For these analyses to be possible, the designer needs to define specific properties of the constructs from a list of options. These options are following the NIST SP 800-160v2 [10]. This publication focuses on *“achieving the identified cyber resiliency outcomes based on a systems engineering perspective”* [10, ?]. Based on NIST SP 800-160v2 and the constructs of BINA, the tool functions are shown below.

Fig. 7.10 shows an algorithm that is mapping the implements relationship between the modelled CIRPs and recovery-related objectives. Based on the designer’s input and following the relations between these constructs and their specific properties values, the algorithm assesses the correctness of the modelled constructs.

```

1  for every cirp(implements) -> notEmpty()
2    and objective.name -> notEmpty()
3    and cirp.name -> notEmpty() then
4    if cirp.name -> 'Dynamic reconfiguration' and objective.name -> 'Prevent/avoid' then
5      cirp(implements) -> correct
6      maintain cirp(implements) link
7    else if cirp.name -> 'Dynamic reconfiguration' and objective.name -> 'Prepare' then
8      cirp(implements) -> wrong
9      delete cirp(implements) link
10     insert exclamationmark to the objective
11  ...
12  repeat until all the implements relations are assessed
13  generate a report of corrections

```

Figure 7.10: Assessment of implementation of recovery objectives from CIRPs.

Structural security constraints guide the applicability of CIRPs within a specific organisation or system. Fig. 7.11 shows how CIRPs implement structural security constraints as required by the designer. The consistency of that implementation is assessed based on the relevance between the specific CIRPs and the modelled structural security constraints.

```

1  for every cirp(implements) -> notEmpty()
2    and securityConstraint.name -> notEmpty()
3    and cirp.name -> notEmpty() then
4    if cirp.name -> 'Coordinated protection' and securityConstraint.name -> 'Limit the limit for trust' then
5      cirp(implements) -> correct
6      maintain cirp(implements) link
7    else if cirp.name -> 'Deception' and securityConstraint.name -> 'limit the need for trust' then
8      cirp(implements) -> wrong
9      delete cirp(implements) link
10     insert exclamationmark to the security constraint
11  ...
12  repeat until all the implements relations are assessed
13  generate report of corrections

```

Figure 7.11: Assessment of implementation of security constraints from CIRPs.

CIRPs can be applied at various architectural layers or system assets, including assets of the technical system (e.g., hardware, networking, software, and information storage) and system elements that are part of the more extensive socio-technical system—operations (e.g., people and processes). Fir. 7.12 indicates, for a representative asset architectural layers, CIRPs that are

suitable for the application. It is noticeable that some CIRPs (e.g., Calibrated Defense-in-Depth and Consistency Analysis) can involve working across multiple layers and/or locations.

```

1 for every cirp(protects) -> notEmpty()
2   and asset.architecturalLayer -> notEmpty()
3   and cirp.name -> notEmpty() then
4     if cirp.name -> 'Dynamic reconfiguration' and asset.architecturalLayer -> 'Hardware and firmware' then
5       cirp(protects) -> correct
6       maintain cirp(protects) link
7     else if cirp.name -> 'Dynamic reconfiguration' and asset.architecturalLayer -> 'information storage management' then
8       cirp(protects) -> wrong
9       delete cirp(protects) link
10      insert exclamationmark to the asset
11    ...
12  repeat until all the protects relations are assessed
13  generate report of corrections

```

Figure 7.12: Assessment of protection of assets from CIRPs.

Cyber resiliency is essentially about ensuring the continuation of pursuing organisational objectives even though an adversary has established a foothold in the organisation’s systems and cyberinfrastructure. Security controls are largely focused on keeping the adversary out of systems and infrastructure. They are not generally resiliency controls, represented in BINA as CIRPs. For example, identification and authentication controls are generally not focused on combating an adversary after achieving a foothold in an organisational system. Similarly, physical access controls are generally considered necessary information security measures, not cyber resiliency measures.

In some instances, cyber resiliency capabilities are reflected in security control enhancements. In those situations, it is required that a parent control be selected if one or more of its control enhancements are selected. This is expressed through an aggregation of security controls under a parent CIRP. This allows for any cyber resiliency control enhancement selected, and the associated CIRP is also selected, modelled and included in the resiliency analysis for the system’s security plan.

Fig 7.13 identifies the security control enhancements that support CIRPs. For each of the selected cyber resiliency controls or security control enhancements, the algorithm specifies the corresponding CIRP. In many instances, more than a single CIRP is provided. That is because many of the controls and enhancements support more than one CIRP. There are multiple corresponding CIRPs listed in a prioritised order where the technique with the most robust linkage is listed first.

```

1 for every securityControl(aggregates) -> notEmpty()
2   and securityControl.name -> notEmpty()
3   and cirp.name -> notEmpty() then
4     if securityControl.name -> 'Account management/dynamic privilege management' and cirp.name -> 'adaptive response' then
5       securityControl(aggregates) -> correct
6       maintain securityControl(aggregates) link
7     else if securityControl.name -> " and cirp.name -> " then
8       securityControl(aggregates) -> wrong
9       delete securityControl(aggregates) link
10      insert exclamationmark to the security control
11    ...
12  repeat until all the aggregates relations are assessed
13  generate report of corrections

```

Figure 7.13: Assessment of security controls aggregation to CIRPs.

Fig. 7.14 allows the identification of the effects that CIRPs can have on threat objectives. By seeing which effects a CIRP could potentially have on a threat, the designer can determine

which CIRPs (and corresponding controls) could maximise the system’s chances of mitigating the adversary’s actions. Thus, using the relevant algorithm for analysis, it may reveal to a designer that the CIRPs (and correspondingly, the controls) that they are planning to implement are largely focused on detecting an adversary, containing an adversary’s assault, shortening the duration of a successful adversary attack, and reducing the damage from such an attack. Correspondingly, such an assessment would reveal to the designer that the organisation’s resiliency plans may lack CIRPs that have other effects, such as diverting or deceiving the adversary or preempting or negating the adversary’s attempted assault. Such information can help the designer and other stakeholders reconsider their resiliency investments to be more balanced.

Also, the algorithm reveals which CIRPs have multiple potential effects on the adversary’s objectives and have only a few potential effects on the adversary’s objectives. Such information might help guide investment decisions by guiding stakeholders to CIRPs with multiple effects, including those in which the organisation has not previously invested. However, not all threat objectives are affected by all CIRPs. Indeed, some objectives are affected only by one or two CIRPs. This is generally the case for threat objectives in the early stages (e.g., Administration, Preparation), which mainly involve adversary actions before accessing a system.

```

1 for every threat(has) -> notEmpty()
2   or threat objective.name -> notEmpty() and cirp(effects) -> notEmpty() then
3 from effects.value = [contain, deceive, degrade, delay, detect, deter, divert, exert, expunge, negate, no effect, preempt, reduce, reveal, scrutinise, shorten]
4 put a value in effects link based on rules
5   if cirp.name -> 'Dynamic reconfiguration' and objective.name -> 'Execution' then
6     effects.value -> negate, delay and exert
7   else if cirp.name -> 'Dynamic reconfiguration' and objective.name -> 'Reconnaissance' then
8     effects.value -> exert, shorten
9   else if cirp.name -> 'Dynamic reconfiguration' and objective.name -> 'Privilege escalation' then
10    effects.value -> no effect
11 ...
12 repeat until all the effects relations are specified
13 generate report of effects relations

```

Figure 7.14: Analysis of CIRPs effects on threat objectives.

Fig 7.15 lists each CIRP and identifies potential interactions (e.g., synergies, conflicts) between CIRPs. Based on these interactions, a CIRP can support (S) another CIRP, as one is made more effective by implementing the other. A CIRP might depend (D) on another if it is ineffective if not used in conjunction with another CIRP. A CIRP can also use (U) another CIRP if a CIRP can be implemented effectively in the absence of another CIRP; but, more options become available if the other CIRP is also used. Finally, a CIRP can conflict/complicate (C) the implementation of another CIRP, which means that some or all implementations of a CIRP could undermine the effectiveness of another CIRP.

```

1 for every cirp(decomposition) -> notEmpty() and cirp.name -> notEmpty()
2 from decomposition.value = [supports, depends, uses, conflicts/complicates]
3 put a value in decomposition link based on rules
4   if cirpA.name -> 'Adaptive response' and cirpB.name -> 'Analytic monitoring' then
5     decomposition.value -> depends
6   else if cirpA.name -> 'Adaptive response' and cirpB.name -> 'Contextual awareness' then
7     decomposition.value -> uses
8   else if cirpA.name -> 'Adaptive response' and cirpB.name -> 'Coordinated protection' then
9     decomposition.value -> supports
10  else if cirpA.name -> 'Adaptive response' and cirpB.name -> 'Diversity' then
11    decomposition.value -> uses
12 ...
13 repeat until all the decomposition relations are specified
14 generate report of decomposition relations

```

Figure 7.15: Analysis of effects among different CIRPs.

The aim of a cyber resiliency analysis, especially in a requirements engineering tool, is to

determine what is applicable for each organisation's objectives. In this respect, organisations can select, adapt, and use some or all of the cyber resiliency constructs (e.g., objectives, CIRPs, security constraints) presented in the implementation metamodel and apply the constructs to their own technical, operational, and threat environments for which systems-to-be need to be engineered.

The tailorable quality of the engineering activities and tasks and the analysis that takes place at the early stages of a system's development and in particular the requirements stage ensure that systems resulting from the application of BINA, have the level of resiliency deemed sufficient to guard stakeholders against experiencing unacceptable impacts on their assets and associated consequences. Cyber resiliency is pursued, in part, by the rigorous application of the security and cyber resiliency design principles and constructs within a structured set of processes that provide the necessary traceability of requirements, transparency, and evidence to support risk-informed decision-making and trade-offs as presented above.

Generation of risk level

After the designer has specified the impact level of an incident and the potentiality of an event, then the risk level can be calculated. Moreover, the designer can determine the level of risk value a warning can be inserted into the model. The warning alert indicates that new CIRPs or security controls need to be inserted into the model.

```

1  if incident.impactLevel -> notEmpty() and event.potentiality -> notEmpty() then
2  calculate risk.riskLevel = incident.impactLevel x event.potentiality
3  if user.riskWarning determined then
4  if user.riskWarning > risk.riskLevel then
5  generate alert
6  else
7  move to next risk
8  end if
9  else
10 ask user to determine user.riskWarning
11 send the new user.riskWarning to determine if need to generate alert
12 end if
13 else
14 ask user to determine incident.impactLevel and/or event.potentiality
15 send the new incident.impactLevel and/or event.potentiality to determine risk.riskLevel
16 endif
17 generate riskLevel

```

Generation of resiliency metrics

Once the risk reduction of CIRPs has been defined as valid or invalid by the developer and the importance and reliance level, there is an automatic calculation of the dependence level and the system resiliency level. The following algorithm implements formula 7.1.

7.3 Discussion and Closing Remarks

In this chapter, we have proposed a process for reasoning about resiliency relationships, analysing Cyber Incident Response Plans (CIRPs) and assessing the resiliency of the system-to-be. Section 7.1.1 presented the initial activity that focuses on modelling the organisation context of

```

1 if cirp.riskReduction -> notEmpty() then
2   sum(cirp.riskReduction = total)
3   sum(cirp.riskReduction = true)
4   sum(cirp.riskReduction = false)
5 else if cirp.riskReduction -> isEmpty()
6   ask user to determine cirp.riskReduction
7   send the new cirp.riskReduction to count it
8   endif
9 endif
10 if cirp.importanceLevel -> notEmpty() then
11   collect(cirp.importanceLevel = 1) -> sum(cirp.importanceLevel = 1)
12 else
13   ask user to determine cirp.importanceLevel
14   send the new cirp.importanceLevel to summation
15 end if
16 if cirp.relianceLevel -> notEmpty() then
17   collect(cirp.relianceLevel = 1) -> sum(cirp.relianceLevel = 1)
18 else
19   ask user to determine cirp.relianceLevel
20   send the new cirp.relianceLevel to summation
21 endif
22 calculate cirp.dependenceLevel = (sum(cirp.riskReduction = true) / sum(cirp.riskReduction = total)) x sum(cirp.relianceLevel = 1)
23 calculate cirp.systemResiliency = (sum((sum(cirp.importanceLevel = 1) x sum(cirp.relianceLevel = 1)) / (sum(cirp.importanceLevel = 1)) x 100
24 generate cirp.dependenceLevel
25 generate cirp.systemResiliency

```

the system-to-be and especially capturing the relationships among organisational constructs. In Section 7.1.2 the incident modelling activity was described. It concerns the identification of experiential, reported, normative, and external incidents and Cyber Incident Response Plans (CIRPs). In Section 7.1.3 described the activity of holistic resiliency modelling. Besides, it is pointed out that the validity of the Cyber Incident Response Plans (CIRPs) needs to be examined by collecting relevant evidence. The resiliency analysis was described in the following Section 7.1.4. The analysis consisted of the reliance and dependence level of Cyber Incident Response Plans (CIRPs). It also presents the formulas for measuring the resiliency of the technical system-to-be. The BINA process is part of the requirements engineering phase of system development. It can be applied along with the elicitation and analysis of other functional and non-functional requirements. It leads to the identification of the system-to-be resiliency that enhances the requirements specification of the system under development.

Chapter 8

Evaluation of BINA methodology by case study research in the health care domain

Validation is the process of checking whether or not a specific design artefact is appropriate for its purpose, meets its requirements and constraints and performs as expected. This chapter validates the strengths and weaknesses of the proposed Build-In Resiliency Analysis (BINA) methodology. This part of the research is empirical and includes the following questions:

- How well does the methodology support modelling and reasoning about cyber resiliency relationships?
- How well does the methodology support resiliency requirements' modelling and analysis?
- How well does the methodology assess the cyber system resiliency at a requirements level?

We adopted two methods of validation for the BINA methodology (cf. Fig. 8.1). The first validation method is a confirmatory qualitative case study that tests the developed theory. It is a confirmatory case study because we can use it to generate and test hypotheses [198] and to build a convincing body of evidence to support the propositions of this thesis. Moreover, qualitative because the assessment was based on the required features that the BINA methodology provided [199].

We selected the Brighton and Hove Digital Health Living Laboratory as the main case study. The Digital Health Living Lab is a unique test-bed of digital devices and applications. It homes 50 families and is used as an arena for testing and developing prototypes or more mature products and services that can improve welfare services. They are testing different digital devices and applications to reduce social isolation and remotely monitor the community's older members' vital signs, activities, and emotions.

Case study research is suitable for situations where the context can play a role in the phenomena. The confirmatory case study was selected because we can observe the benefits of the BINA methodology on a single system. Moreover, software engineering is a multidisciplinary field involving areas where case studies typically are conducted, such as psychology and sociology. As software engineering combines elements from these areas, this means that many research objectives in software engineering research are suitable for case study research [200] and

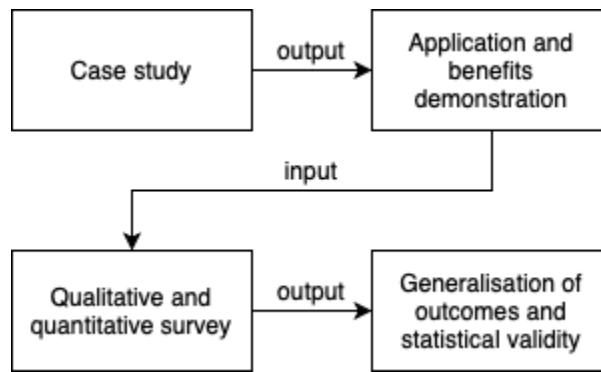


Figure 8.1: Validation approach.

that there was the need to investigate not only methods and tools but also the social and cognitive processes surrounding them [201]. In these areas, the objectives are to increase knowledge about personal and social phenomena in their context, which is similar to our objectives to increase knowledge regarding the practitioner’s ability, knowledge, understanding, and capture of cyber resiliency relationships during information systems development.

The second validation method is a quantitative survey [202]. The subjects were practitioners and researchers that used the methodology and tool on a small scale case study. Then they were asked to provide information about their experience of applying the methodology through the BINA tool to investigate the quantitative impact of our proposal. This validation included a questionnaire-based survey that provided multiple instances of observation for the statistical validity of the results. We analysed the collected information using standard statistical techniques, and we focused on the methodology’s perceived usefulness and ease of use as experienced by the participants.

The overall results were subject to a combination of quantitative and qualitative analysis. The quantitative and qualitative survey methods were selected because the available participants had experience using methodologies and tools and were interested in learning about any consequent methodologies and tools that could arise. Additionally, this is a suitable means of validation instead of a simple review of the methodology by the participants. In particular, we used the survey for qualitative evaluation, which was a feature-based evaluation. We developed a BINA tool prototype that helped us identify features that participants perceived as useful or not. This analysis was beneficial for identifying design flows and practical problems with the methodology, such as ambiguities or missing conditions.

8.1 Proof of Concept for BINA by case study research in the health care domain

A Proof of Concept (POC) is a small exercise to test the design idea or assumption. The primary purpose of developing a POC is to demonstrate the functionality and applicability of the BINA design artefacts. The expected outcome from the POC is to show that that the BINA methodology is practicable in the healthcare context.

This section considers a case study on the application of BINA methodology in the health care domain. We examine if BINA efficiently enables practitioners to model and reason about incident response relationships and assess the system’s-under-development resiliency at a requirements stage. To demonstrate BINA in action, we used a confirmatory qualitative case

study. We choose two healthcare systems that were of engineering interest at the time and relevant to penetration testers. We monitored and collected data from existing experiments to demonstrate the applicability and the advantages of BINA. These case studies also served as the first test for BINA before a more formal validation.

Based on the taxonomy of Zelkowitz and Wallace [202] for validating new methodologies, this study is utilising historical data collection methods. It can also be characterised as a literature search-based validation method, as there was a collection of data from completed projects and analysis of papers and other publicly available documents. More specifically, we based some attack scenarios on experiments available in the literature and documents related to the selected case study.

Our case study follows the steps listed below [203, 204, 205]:

- Research initiation - This phase included defining the research objectives and determining the appropriate case study. We based the suitability of the case study on the research objectives and the literature review.
- Case study management - which dealt with ethical approval, publishing rights, and scheduling issues. It was an "ad hoc" phase that took place in parallel with all the other phases.
- Case study context - identification of the case study boundaries and selection of feasible case scenarios. We selected case scenarios that were likely to be typical, critical, and/or relevant to health care system designers. Further, we chose the documents and information needed to make the scenarios as realistic as possible.
- Case study plan - determining the strategy for data validity and minimisation of the confounding factors. We also defined the data collection strategy and how the results would be analysed.
- Data collection - selection of methods for data collection during the development of the case studies. Including the collection of data from multiple sources, such as literature searches of previously published studies, legacy data from completed projects, static analysis considering the structure of the developed product.
- Data analysis - the evaluation and the conclusion resulting from the case study. As case study methodology is a flexible design strategy, there are many iterations over the steps, and the data collection and analysis were conducted incrementally. During the whole process, there was constant updating of research notes, and the structure of the case study report was in the form of a single case study narrative report.

8.2 Case study design

8.2.1 Case study objectives

The objectives of the case study are confirmatory and/or identify areas of improvement. They were defined in a way to provide answers to the evaluation research questions. Therefore the objectives of the case study were to:

- **O1:** Apply the BINA methodology in the health care domain.

- **O2:** Evaluate the applicability of BINA methodology for modelling and reasoning of resiliency and relevant requirements in the health care domain.
- **O3:** Evaluate the applicability of BINA methodology for assessing the resiliency of the system under development at a requirements stage.
- **O4:** Evaluate the efficiency of BINA methodology.
- **O5:** Overall consideration of the BINA methodology and any potential areas of improvement.

8.2.2 Case selection/context

We returned to the literature searching for cyberattacks against healthcare infrastructures that we could use as case studies to evaluate BINA applicability. We found attacks against MRIs where an attacker can tamper with the control commands and trap or injure a patient with rapidly accelerating objects like an oxygen tank or burning a patient by overriding the strength of the magnetic field. We found attacks against X-rays that an attacker manipulates photons to expose a patient to harmful radiation. We found attacks against infusion pumps that could administer or not pain medication and give different indications to the user. We found attacks against PET scans that their files were kept locked due to ransom or CT scanners that the display information did not correspond to the actual radiation delivered to the patient. We found attacks against medical ventilators that had maliciously altered patient-related parameters. Similar attacks against anaesthetic machines, heart-lung machines, dialysis machines and medical lasers were also found.

It became clear that attacks were occurring against medical devices operating within healthcare premises and devices that are used remotely. In 2013 the first hacking against medical devices was targeting a Brain-Computer Interface (BCI), so for symbolic and historical reasons, we used this example for one of the case studies covering devices used within healthcare premises and can be used remotely. For the second case study, we chose a Teleoperated Robotic Systems (TRSs) because it is used in hostile environments and cover cases where medical devices operate within unsafe contexts. Also, some of the cases mentioned above clarified that we needed more knowledge of physics and biomedical sciences, so we felt that the two examples above were better understood and analysed than the others that seemed to require input from healthcare professionals and engineers.

Two case studies were selected. The first case study concerned the resiliency of Brain-Computer Interface (BCI) against cyber attacks [206]. The second case study considered attacks against Teleoperated Robotic Systems (TRSs). TRSs have widespread use. In particular, they are helpful where remote intervention is required by scaling the size and motion of a human operator's intended actions, such as handling explosive and radioactive material, warfare zones and underwater research [207, 208]. In healthcare, TRSs are also used to perform operations, reducing the size of incision or from a distance, in areas where there might not be doctors available [209].

8.2.3 Unit of analysis

To judge the effectiveness of a system's resiliency, we applied the resiliency-based constructs and process into two critical healthcare systems: a Brain-Computer Interface (BCI) and a Teleoperated Robotic System (TRS). Then we identified resiliency relationships and examined

whether the resiliency assumptions were justified. If not, then additional functionality was proposed to ensure the system’s resiliency. The aim is to make the system as resilient as possible.

The healthcare systems under development, namely BCI and TRS, will be interacting with other components of a whole information system, either human or technical. These interactions constitute dependencies between the system and the other components and vice versa. The unit of analysis is the dependency between the technical system and other components of the information system. As there were multiple dependencies, there were multiple instances of this unit of analysis. Another unit of analysis will be the identification of resiliency requirements. Similarly, there were multiple instances of this unit of analysis. The last unit of analysis was the assessment of the resiliency of the system under development.

8.2.4 Data collection and analysis methods

Fig. 8.2 shows the data acquisition methods used for the case study. The developed models using the BINA methodology were collected, along with qualitative notes derived from the models. Additionally, we collected documents related to the existing development of BCI and TRS systems and documents related to the cybersecurity of these technologies.

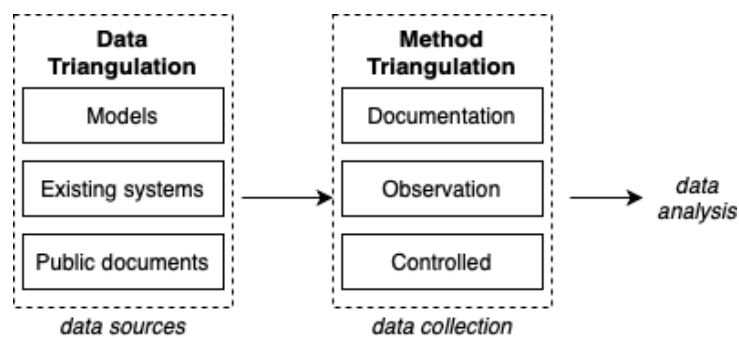


Figure 8.2: Case study acquisition methods.

Then we compared the existing functionalities of the BCI and TRS with the identified functionalities using the BINA methodology. Then, there was an evaluation of the non-quantifiable benefits of the BINA methodology by gathering qualitative information from the comparison.

8.2.5 Case study validity

There are various aspects of validity that are discussed below [201, 198, 205].

Construct validity focuses on whether the operational measures for the concepts are **suitable**. Therefore, to improve construct validity, the operational measures regarding the confidence in the fulfilment of a system’s resiliency were developed by using multiple sources of evidence, such as literature and expert opinion.

Our case study was, by nature, comparative. We tried to reduce the expectation bias on the case study results by identifying a valid basis for assessing the results. To this end, we compared the actual implementation of the BCI and TRS systems developed with another method and the potential implementation of the BCI and TRS systems developed with our proposed method. Therefore, we improved the internal validity as we compared our proposed method while using the same medical systems. We base the comparison on identifying the

systems' resiliency. More specifically, we compare whether there has been any reasoning about resiliency requirements fulfilment.

External validity concerns whether our claims for the generality of the results are **justified**. To ensure external validity, we used data triangulation. Triangulation allows us to limit the effects of one interpretation from one single data source by gathering data from multiple sources. In terms of gathering information about the BCI and TRS systems, various data was collected from the UK Department of Health and research publications. Based on this data, the BINA models were constructed and used as another data source. This way, the conclusions reached were stronger than conclusions based on a single source. Data triangulation ensured the external validity of our case study, which justified the generalisation of our results.

Another validity concern is the **representativeness** of the selected case study, which ensured the external validity of our case study. The BCI and TRS systems were selected, as they are increasingly critical medical systems, and their resiliency depends a lot on other interacting entities such as a remotely located doctor. Also, its resiliency is of paramount importance because any variations can have severe consequences on peoples' health. Furthermore, when we chose the systems' resiliency aspects of our case study, we applied theoretical sampling to capture all possible variations of a resiliency resolution and gain a deeper understanding. Among the selected resiliency aspects, some were resolved by control or by a process and some unresolved. In the last case, we identified and analysed resiliency requirements. A theoretical sampling of the systems' resiliency was also a way to ensure data triangulation of our case study and ensured its external validity.

Reliability focuses on whether the case study yields the same results if another developer replicates it. Triangulation, developing and maintaining a detailed case study protocol, spending sufficient time with the case ensured a certain level of similarity of results and improved the study's validity. However, as the developer performs the resiliency analysis, the results can probably differ in certain aspects. In particular, when reaching the stage to decide the type of resolution of a resiliency requirement, a different developer can have different preferences and priorities. As a result, another developer might not resolve a resiliency issue in the same way and vice versa; for example, another developer might identify a resiliency resolution while we did not because we did not have any direct experience or our priorities were different.

Also, we used method triangulation to improve external validity. The first data acquisition method was a documentation analysis of research data. It included the analysis of work artefacts that were already available. One disadvantage of this type of data collection technique was that the documents were created for another purpose than that of the research study, so it is unclear if the requirements on data validity and completeness were the same. A second acquisition method was an observation, a direct method, where there was direct contact and real-time data collection. We conducted an observation to investigate how a practitioner conducts a specific task. The advantage of the observation data collection technique was that it provided a deep understanding of the studied process. However, some of the data was controlled because they could be identifiable and thus liable to disclosure. These data have been considered in the resiliency analysis but are not presented directly in the case studies.

In the next section, we apply the BINA methodology. Again, we performed the role of the requirements analyst to carry out the BINA process of the methodology.

8.3 Brain-Computer Interfaces

Brain-computer interfaces (BCIs) denote a communication and control technology that facilitates communication between the brain and the external world through various electrophysiological signals. BCIs were developed for medical reasons and mainly to provide essential communication capabilities to people suffering from neuromuscular disorders [210]. Currently, BCI-enabled communication has also non-medical applications, such as advertising, fiction and gaming [211, 212, 213].

As the expansion in BCIs capabilities and applicability continues, it is critical to assess potential risks associated with them. Based on recent neuroscientific results [214, 215], BCIs can be misused to extract private information about users. For example, memories, biases, religion and political beliefs, and possible neurophysiological disorders. For example, memories, biases, religion and political beliefs, and possible neurophysiological disorders. In order to improve the security of emerging BCI technologies, their resiliency by design needs to be assessed.

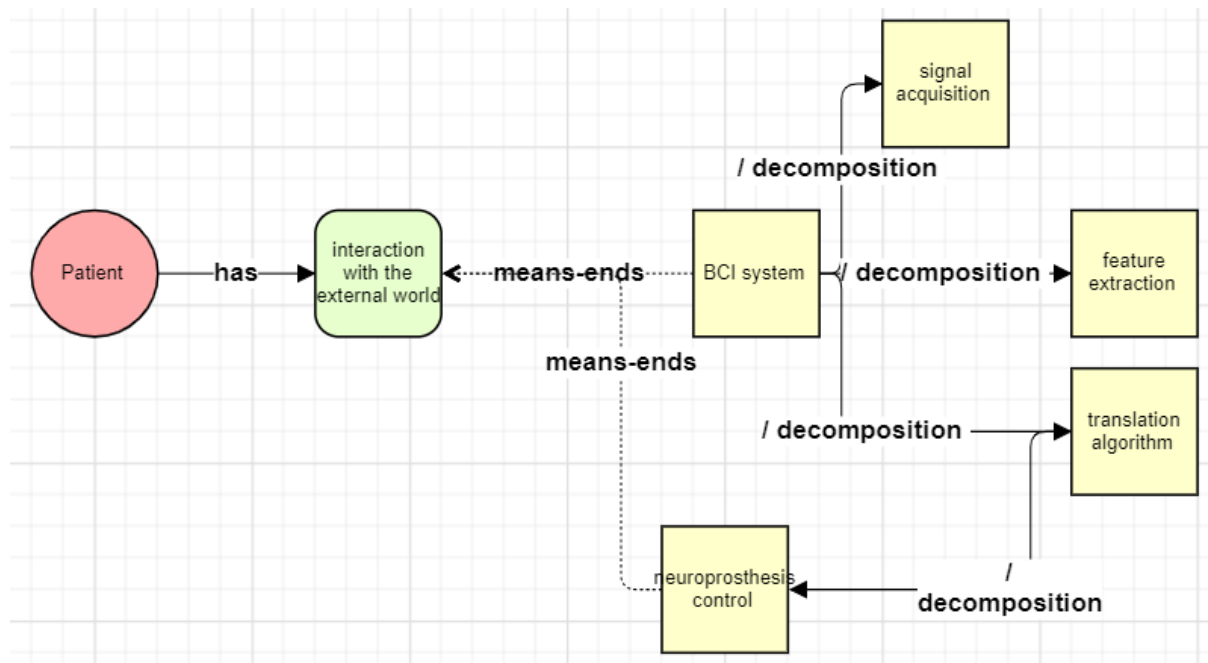


Figure 8.3: A simple Brain-Computer Interface.

Fig. 8.3 shows a simple depiction of a BCI system that translates electrophysiological signals, reflecting the activity of the central nervous system, into a patient’s intended messages that act on the external world [210]. As can be seen, a BCIs is essentially a communication system consisting of inputs (patient’s neural activity), outputs (outside environment commands), and components that translate inputs to outputs.

Activity 1: Organisational modelling

From the scenario, we identify the following main actors, BCI manufacturer, user as the people using BCI for medical reasons, incident response team (IRT) and BCI attacker. Furthermore, we carried out discussions with domain experts and studied publicly available organisation documents. These documents were describing the structure of BCI and healthcare policies.

Once we had gathered as much information as we could from the domain, we constructed the system under the development organisational model. By system, we mean the BCI and the environment in which it operates. In this way, we model the goals of the system under development. Further, we identify which of them can be accomplished by the system itself and which ones are accomplished by other entities that the system depends on. It was vital to examine this, as these dependencies are a potential source of issues for resiliency planning. For example, fig. 8.4 depicts the BCI system organisational model that we constructed using the BINA tool.

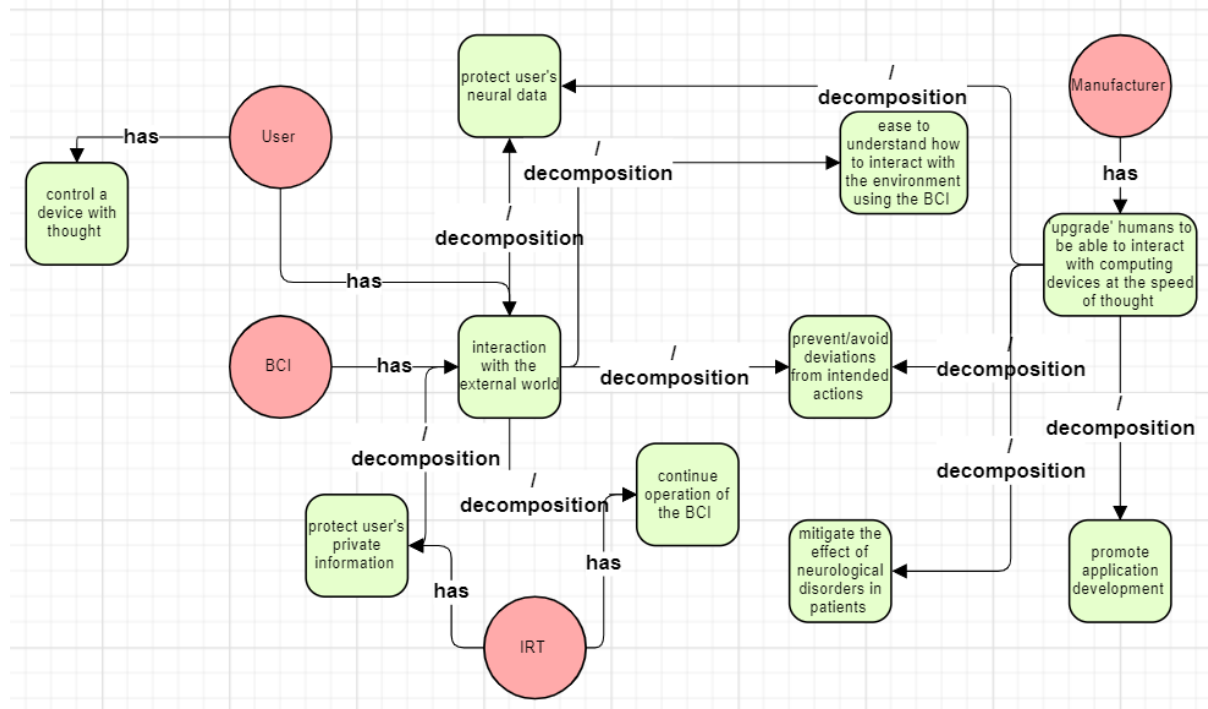


Figure 8.4: Partial BCI system goal-dependency model.

The high-level goal of the BCI system is *interaction with the external world*. We decompose this high-level goal into smaller and more specific subgoals, such as *prevent/avoid deviations from intended actions*, *continue operation of the BCI*, *ease to understand how to interact with the environment using the BCI*, *protect user's neural data* and *protect user's private information*.

Constructing the system goal diagram is vital to identify the goals that can be achieved solely by the system itself and those that cannot. The next step is to examine each goal and decide whether the system itself can achieve the goals or it requires interacting with other actors of the system domain. We identify the goals that the system itself cannot fulfil unless it interacts with other entities of the system domain, such as a *user*, a *manufacturer* and an *incident response team (IRT)*. The rest of the goals are considered as goals that the system can fulfil without depending on other actors.

The BCI system's goals that the system itself cannot accomplish were modelled as dependencies on other interacting actors. Fig. 8.4 depicts the modelled dependencies by the BINA tool. These are the following:

- The BCI system depends on the *user* to *interact with the external world* using the system appropriately.
- The BCI system depends on the *manufacturer* to develop a system that *protect user's neural data* and *prevent/avoid deviations from intended actions* with a secure-by-design approach.

- The BCI system depends on the *manufacturer* to develop a system that *protect user's neural data* and *prevent/avoid deviations from intended actions* with a secure-by-design approach.
- The BCI system depends on the *IRT* to *continue operation of the BCI* and *protect user's private information*.

The modelled dependencies represent how the BCI system can fulfil its goals and be resilient for the stakeholders. Nevertheless, they represent just assumptions; hence they require further study.

The modelled dependencies of the system on other entities of the system domain constitute a potential threat to the BCI system's resiliency. The system must be resilient, but if the dependencies are not fulfilled when the system is put in operation, it will not be resilient. In particular, if the *user* does not use the BCI appropriately to interact with his/her environment, then the system is not resilient in terms of inappropriate use. For example, if the user is tampering with the hardware. If the *manufacturer* does not include security controls to protect the users' neural data, then the system will not be able to protect the users from malicious actors; thus, the system is not resilient in terms of cyber-attacks. If the *incident response team (IRT)* does not support the continuation of the operations of the BCI and does not protect the users' privacy, then the system will not be secure; thus, the system is not resilient. Moving on and implementing the system without investigating further these dependencies by identifying ways to remove the uncertainties at this stage will result in a system that has the risk of not being resilient.

Ultimately, we need to find resilience and control resolutions of the modelled dependencies to build assurance that the BCI system dependencies are fulfilled, and the BCI system is resilient. In order to define appropriate resolutions for the specific context, we first need to model the security constraints that the BCI system and its dependencies impose on the system design. In particular, a *user* of a BCI system needs to *evaluate their network security and protect their critical systems*, a *manufacturer* can pursue corporate goals that comply with his responsibility to produce systems that offer *protection against unauthorised access and control of BCI functions*, and thus he needs to *identify risks and hazards associated with their BCI systems and the processing of neural data* remaining vigilant. Additionally, the *IRT* needs to operate in a way that *prevent distraction or degradation of the BCI operations* and *prevent an attacker from gaining access to the user's private data*.

Activity 2: Incident modelling

Denning et al. [216] in 2009 recognised that "*standard engineering practices, medical trials, and neuroethical evaluations during the design process*" [216] generate safe systems, but not secure as "*none of these disciplines currently ensure that neural devices are robust against adversarial entities trying to exploit these devices to alter, block, or eavesdrop on neural signals*" [216]. The authors classified potential security threats that can be used against implanted neural devices and introduced the term "neurosecurity" as "*the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will*" [216].

It was demonstrated in 2012 by Martinovic et al. [206] that malware can be used against a BCI. They used a commercially available BCI to present a user with visual stimuli and record his/her electroencephalogram (EEG) neural signals. In that way, the authors analysed the recorded signals and detected successfully a user's chosen digit, banking information, the month of birth, location of residence, and if a user recognised the presented set of faces. From

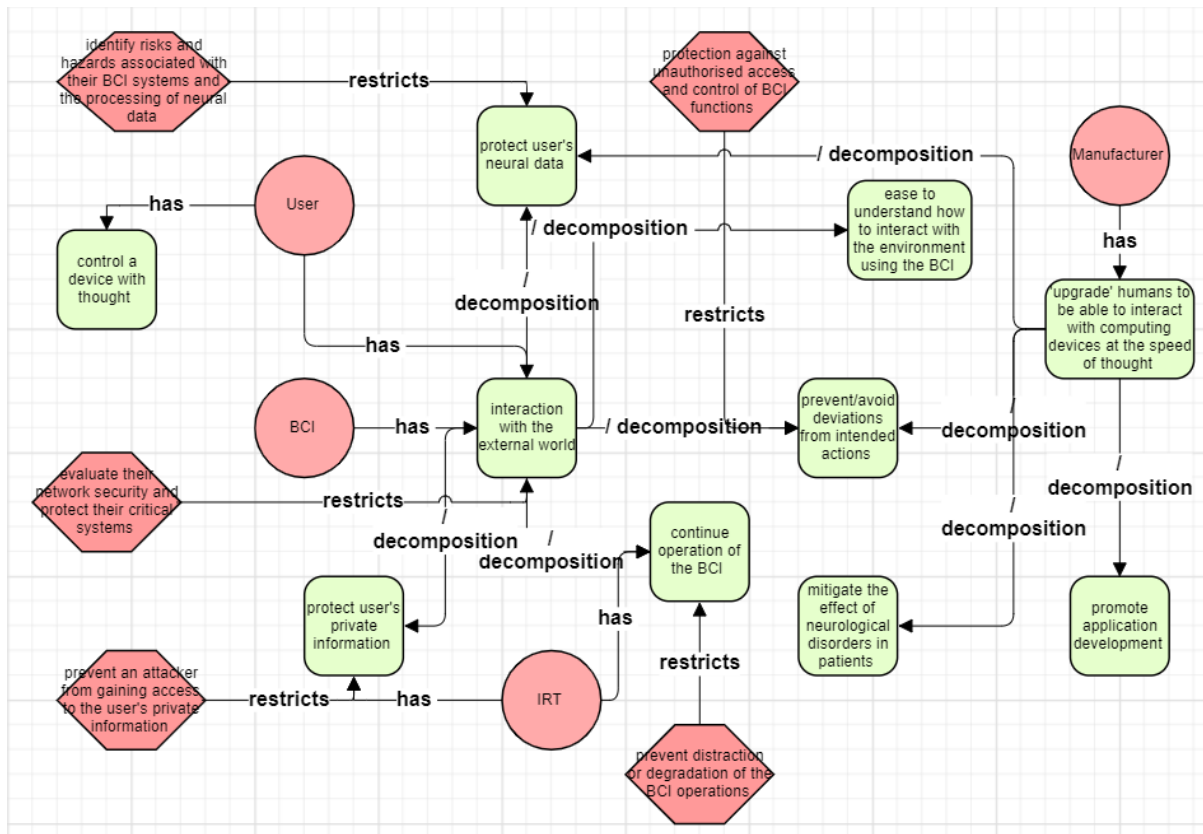


Figure 8.5: Partial BCI system organisational model.

a security perspective, it is essential to protect users from the extraction of their private information about their memories, prejudices, and beliefs and their potential neurophysiological disorders. Currently, cybersecurity concern does not seem to be part of the design and development of such systems.

In this incident modelling activity, we consider an attacker who uses non-invasive BCI devices, mainly intended for consumer use, to obtain private information about users. Manufacturers of non-invasive EEG-based BCIs currently often distribute software development kits with their products, as well as technical support [206]. Manufacturers aim to promote application development, but such "open-development" platforms may compromise users' privacy and security. There is currently no review process, standards and guidelines in place to protect users, nor technical protection to restrict inappropriate or malicious BCI use.

Fig. 8.4 depicts a typical BCI system that is decomposed to an acquisition system, a feature extraction application, and a signal processing system. There is also modelled the *manufacturer* of the BCI that offers "open development" platforms that grant every application developer complete control over all of these components. We, therefore, assume that an *attacker* has access to all of these resources and examine scenarios where an attacker can use these resources to develop malicious applications.

As we have discussed in section 4.4.2, an *incident* construct represents a single or a series of violations or imminent threat/s of violation of security constraints. In other words, it is the effect of intentional and malicious behaviour. For example, possible observable occurrences in a BCI system are: *affect on user's reputation*; *violation their right "to be left alone."*; *maliciously extract private and sensitive information about a user*; *failed user deidentification*.

In a build-in approach to resilient design and development of BCI systems, a Cyber Inci-

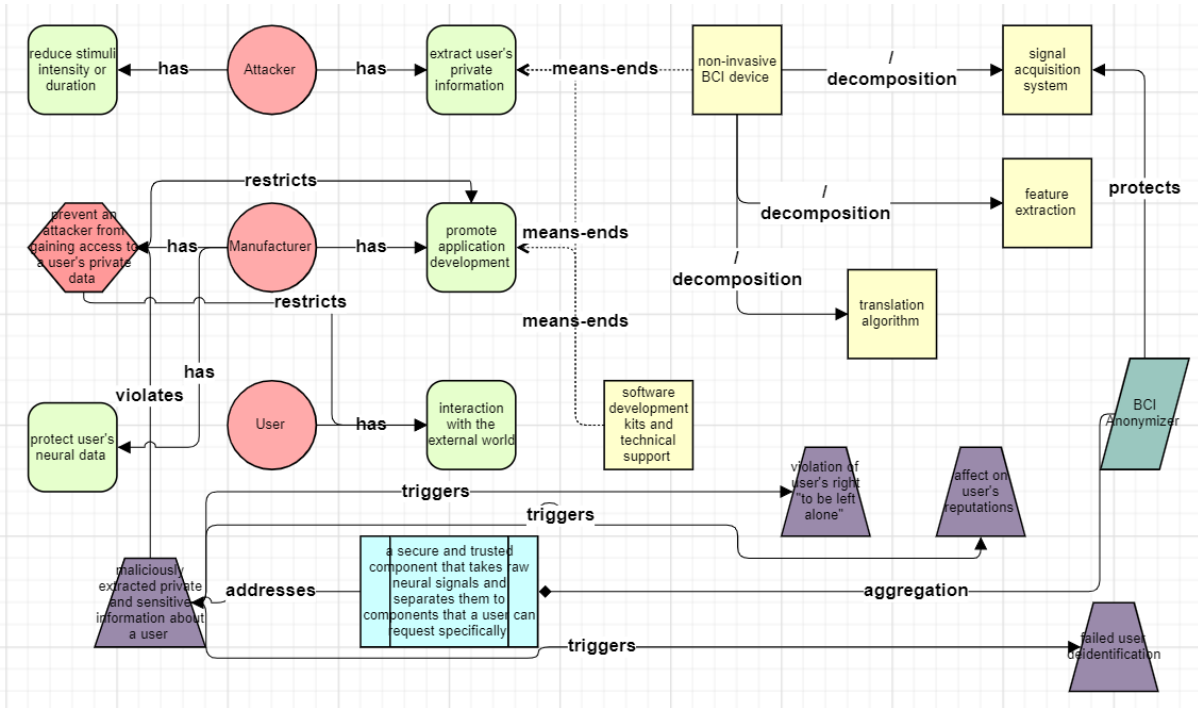


Figure 8.6: An incident scenario against a Brain-Computer Interface.

dent Response Plan (CIRP) suitable to the incidents identified above will be *a secure and trusted component that takes raw neural signals and separates them to components that a user can request specifically*. This approach has been proposed in [217] where the appropriate security control is identified under the name “BCI anonymiser”. However, in order to be able to analyse the resiliency of a BCI system, we need to identify possible causes of such incidents.

The second step of the analysis focuses on effects (incidents) and not causes (threats) because the designer knows what is unwanted to occur from technical errors and malicious behaviours but does not necessarily know at that stage what may be the possible causes. By analysing causes in the next activity, we can go more in-depth with how a BCI system is penetrated and identify ways to prevent and recover from these preidentified unwanted occurrences.

Activity 3: Holistic resiliency modelling

The identified resolutions point out the underlying resiliency relationships. From the incidents and responses, we need to identify possible causes, representing the existing resiliency assumptions about the BCI and its socio-technical system underlying our analysis.

In both experiments in regards to the security of BCI systems, researchers used a batch processing method to extract private information about a user [206, 217]. Hence, in Fig. 8.7 we model an attacker that aims to extract users’ private information by *hijacking* the legitimate components of a BCI (feature extraction and decoding algorithms) or by adding or replacing the legitimate BCI components. Such an attacker implements additional feature extraction and decoding algorithms and either substitute or complements the existing BCI components with additional *malicious code*.

More specifically, an attacker presents to a user a random sequence of stimuli that s/he has tampered. An attacker can interact with a user by presenting them with a malicious set of

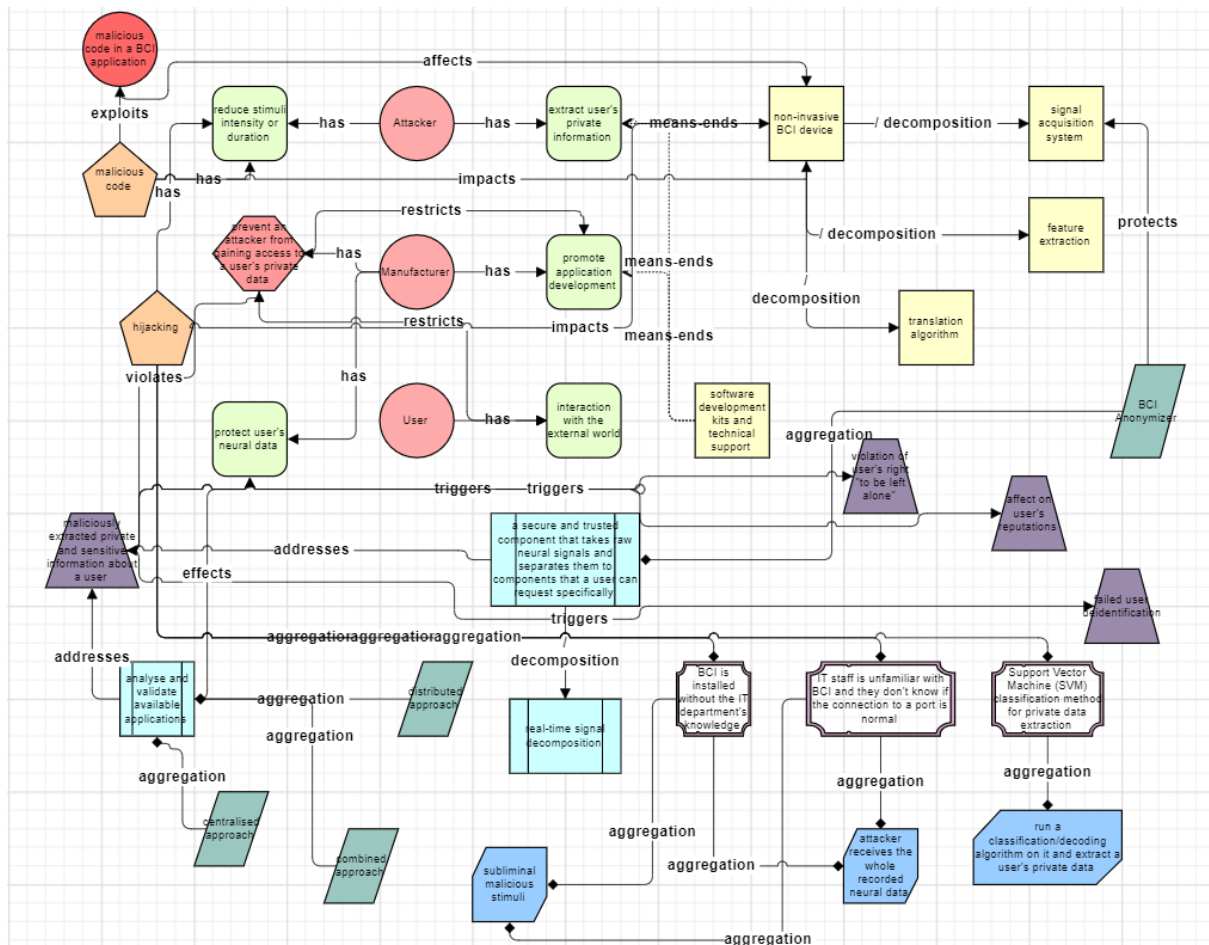


Figure 8.7: A partial resiliency model for BCI.

stimuli in an overt (conscious) fashion or in a subliminal (unconscious) way. We specifically focus on private and sensitive data extraction when stimuli are being presented to a user subliminally. This means that the stimuli are presented to the user in a manner where s/he is not consciously aware of the presented stimulus, but s/he may still be reacting to it. This will allow an attacker to conceal his/her presence and any changes in the BCI functions. Subsequently, the attacker will record the user's responses to the whole sequence of presented stimuli and process the recorded signals to infer information about the user.

Consequently, we model potential risks from the threats present in the model. The first risk is the potential exposure of the user to *subliminal malicious stimuli*. If the attacker is successful into compromising the BCI system, by controlling the application and the signal processing component of the system, s/he exposes the BCI to two main risks. Firstly the *attacker can receive the whole recorded neural data* and secondly s/he can *run a classification/decoding algorithm on it and extract a user's private data*.

Then we identify the relevant events that stand for any observable occurrence in a system that has not risen to the level of a violation of security constraints. Based on that, the associated events are: *BCI is installed without the IT department's knowledge; IT staff is unfamiliar with BCI, and they do not know if the connection to a port is normal; and Support Vector Machine (SVM) classification method for private data extraction*.

The Support Vector Machine (SVM) classification method is a standard classification method in Event-Related Potential (ERP) research. ERP is the measured brain response that is the di-

rect result of a specific sensory, cognitive, or motor event. The main idea behind this non-probabilistic binary classification method is to find the separating hyper-plane between two classes so that the distance between the hyper-plane and the closest set of points from both classes is maximised.

This leads us to identify how to enhance the resiliency of a BCI. It seems possible that the same approach, first to record neural signals and batch-decompose them into components before giving them to a BCI application, may also be used to mitigate some of the privacy attacks on BCI-enabled communication. This seems to be depicted already as *BCI Anonymiser* that is mitigating the vulnerability *malicious code in a BCI application*. However, the batch approach leaves vulnerable stored neural data, their transmission and manipulation by a BCI system. that means that we need to enhance the *BCI Anonymiser* with a *real-time signal decomposition*. In this way, we mitigate privacy attacks that might occur during these stages of the neural data.

Moreover, the vulnerability *malicious code in a BCI application* can be tackled having a way to *analyse and validate available applications*. In a *centralised approach* a centralised entity will scrutinise every application, and only allow those applications deemed as appropriate to become a part of the app store. Whereas in a *distributed approach*, every application can freely be added to the app store. There anyone can freely use, analyse and report findings of the application for everyone else to view. A combination of the two is also possible.

The designer also needs to determine the importance level of the CIRPs as well as the reliance level. S/he can do that using the properties and changing the relevant value accordingly, as shown in Fig. 8.8. Similarly, we fill in the information for the other CIRPs in the model.

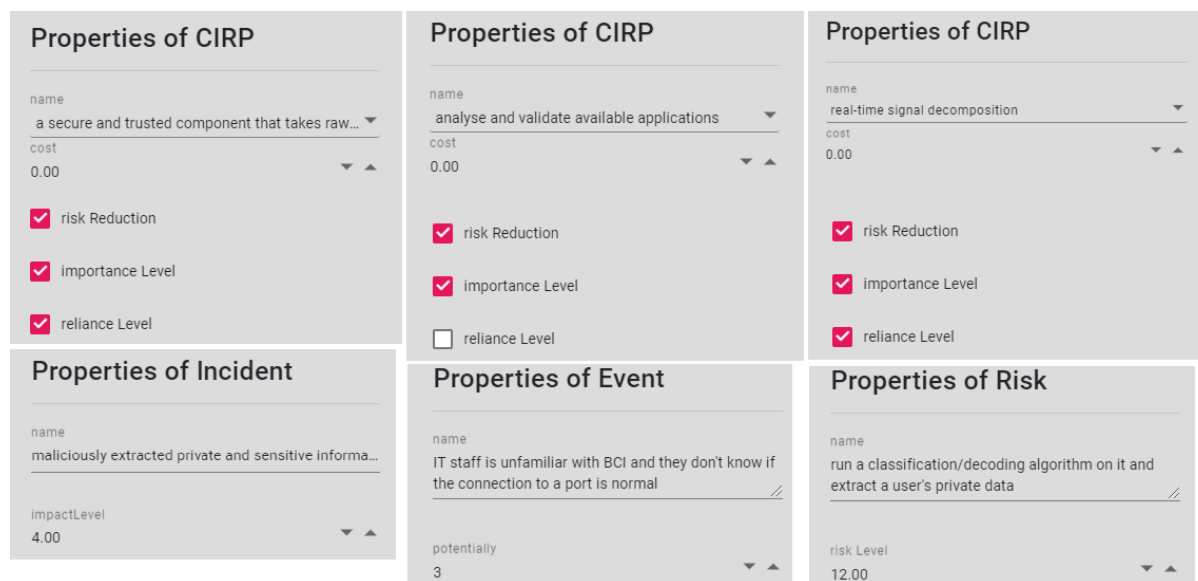


Figure 8.8: CIRP properties determination.

The next step was to justify if the CIRP were valid or not and to modify their "risk reduction" property accordingly. For the *secure and trusted component that takes raw neural signals and separates them to components that a user can request specifically* previous studies have shown that this approach is applicable and experimental evidence exists that supports this assumption.

However, for the *analyse and validate available applications*, the environment norm has not been established yet. Therefore this is not a valid CIRP, and as a consequence, the system's objective *protect a user's neural data* may not be fulfilled. The invalid effects relation represented resiliency assumptions of objectives on which the further development of the BCI system would have been based. Eventually, they would have become potential vulnerabilities of the system.

Thus, additional requirements need to be added to the functionality of the system to ensure the fulfilment of objectives and the system's resiliency.

The designer also needs to determine the importance level of the CIRPs as well as the reliance level. S/he can do that using the properties and changing the relevant value accordingly, as shown in Fig. 8.8. Similarly, the designer can fill in the information for the properties of the modelled *incidents*, *events* and *risks* (cf. Fig. 8.8).

The designer can enrich the model with constructs and relations until the central security objectives have been addressed sufficiently. That will generate a more detailed model as the one depicted in Fig. 8.9. This diagram is the holistic resilience model for a BCI system.

Activity 4: Resiliency analysis

Using the BINA tool, the designer can firstly validate the correctness of the model created based on the metamodel. This analysis happens automatically when the user designs with the BINA tool. If a link between nodes (concepts and relationships) is invalid then the tool shows a relevant message and does not allow the connection.

After the correctness of the designed model is assessed from the tool and the designer, further analysis can take place that can raise several critical implementational issues.

Firstly, at any stage, the BINA tool automatically assessed the BCI system's resiliency. Before the resiliency analysis, the 'System Resiliency' (SR) was at 66.66667%. When the analysis progressed, and the designer addressed the relevant issues, the BCI's resiliency became 100%.

Potential interactions between CIRPs: CIRPs can support (S), depend (D), use (U) and conflict or complicate (C) each other. The relations among CIRPs are in accordance with the cyber resiliency techniques presented in NIST SP 800-160v2 [10]. Fig. 8.10 depicts an example of this type of analysis for a BCI. More specifically, the implementation of *segmentation* supports *coordinated protection* and conflicts *analytic monitoring*. If the designer wants to have an implementational model, then all three CIRPs cannot be implemented as there is a conflicting *effects* relationship between *segmentation* and *analytic monitoring*. Also, *analytic monitoring* conflicts with *non-persistence*. As the rest of the CIRPs do not conflict with each other, the designer might choose to remove from the model the CIRP *analytic monitoring*.

Assessment of the implementation of objectives using the selected by the designer CIRPs: CIRPs can also further be analysed in relation to the *security objectives* that they *implement*. Objectives motivate the definition of security requirements and the selection and tailoring of CIRP. A designer can use objectives as a starting point for eliciting restatements of objectives and analysing how CIRPs meet these objectives or not. Using the objectives suggested in NIST SP 800-160v2 [10] and focusing on the BCI system, the designer through the BINA tool derives the relations shown in Fig. 8.11. The designer can see in that way that some CIRPs implement the same objectives, such as the *understand* objective that is implemented from both the *sensor fusion and analysis*, the *consistency analysis* and *integrity checks*. Based on this information and a limited security budget, s/he might choose to remove the CIRP *sensor fusion analysis* as the other two CIRPs achieve the same objective and simultaneously other objectives (i.e., *reconstitute*, *constrain and continue*).

Analysis of the CIRPs effects on malicious objectives: The designer, by incorporating CIRPs as part of the model, wants to effect malicious objectives that an adversary can have. Using the BINA tool, these *effects* relationships became more specific as shown in Fig. 8.12. Assuming that the adversary does not have prior knowledge of the system-to-be, a set of ob-

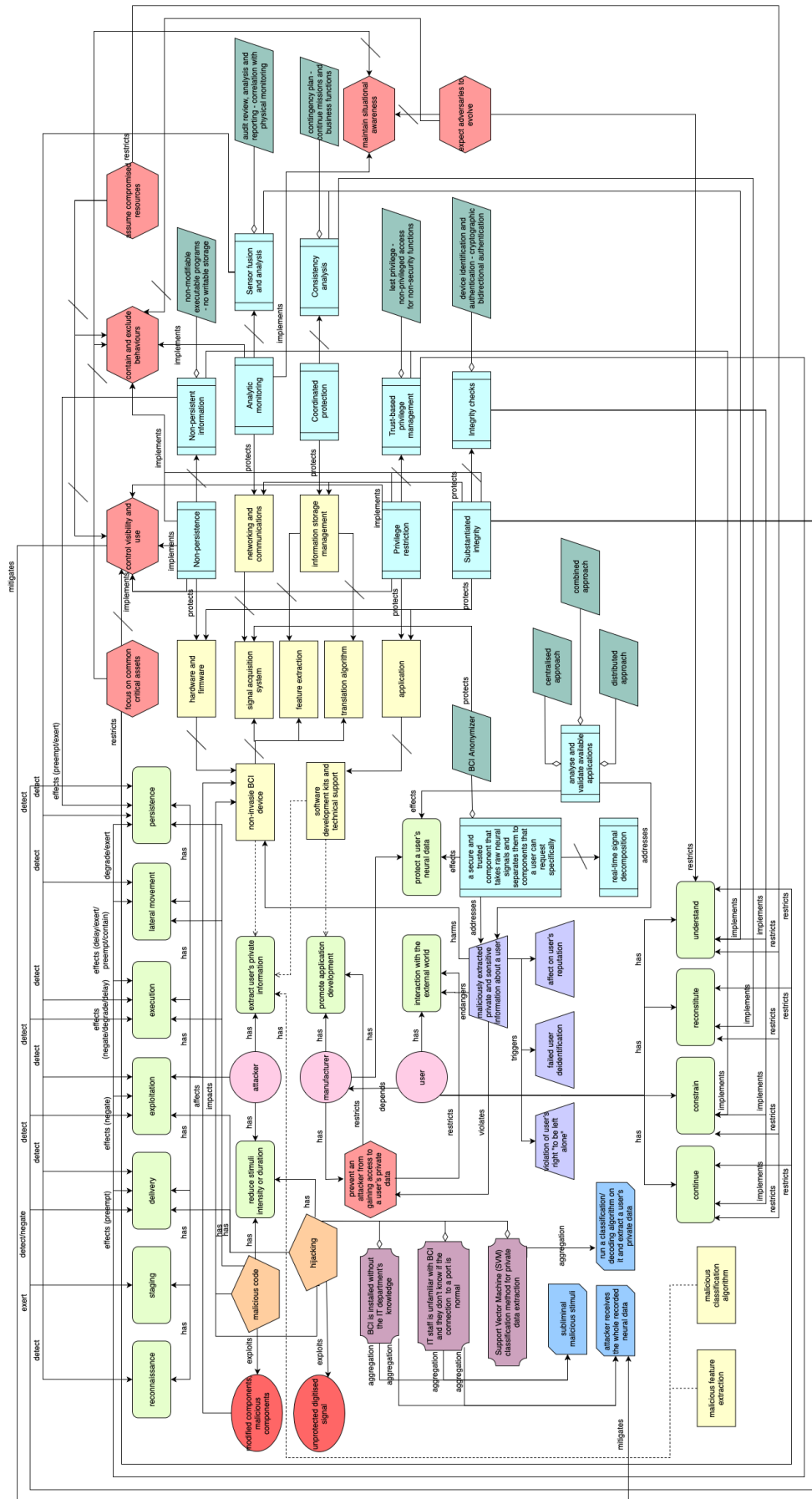


Figure 8.9: Holistic resilience model for BCI.

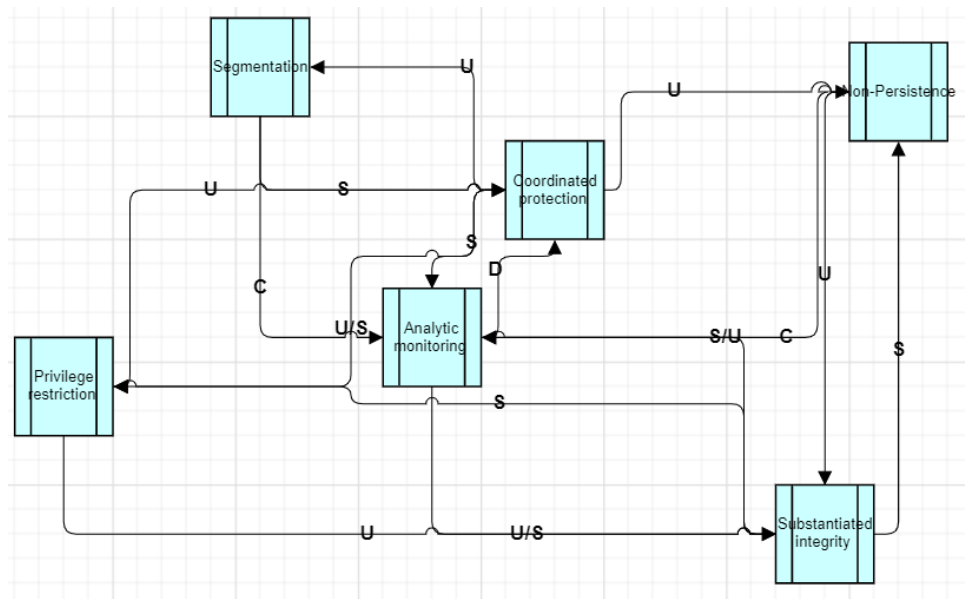


Figure 8.10: Potential interactions between BCI's CIRPs.

jectives can be selected from the designer and modelled using the BINA tool. Then the tool analysis these relationships and characterises them. Assuming that the adversary does not have prior knowledge of the system-to-be, a set of objectives can be selected from the designer and modelled using the BINA tool. Subsequently the tool analysis these relationships and characterises them. For instance, the CIRP *trust-based privilege management* negates the adversarial objective *exploitation* and *execution*. The same CIRP delays exert, preempts or constraints the objective *lateral movement*.

Examination of coverage of structural security constraints with the implementation of CIRPs: Based on NIST SP 800-160v2 [10] CIRPs implement structural security constraints. Structural security constraints guide and inform the design and implementation decisions throughout the BCI system life cycle. Many of the structural design principles are consistent with or leverage the CIRPs. If CIRPs are not sufficient, then the designer will need to add more, or if the model has redundant CIRPs the designer will need to remove them. This type of analysis is facilitated by the BINA tool that offers the capability to define structural security constraints and examine the coverage of the CIRPs that initially the designer has modelled. Fig. 8.13 shows that whereas most modelled CIRPs implement structural security constraints such as *control visibility and use* is implemented with the use of the CIRPs *non-persistence* and *privilege restriction*. However, one of the CIRPs does not meet any structural security constraints, and hence the designer can justify its removal from the model.

Assessment of CIRPs specification with security controls: When the designer might wish to analyse the means through which the CIRPs will be implemented. CIRPs aggregate security controls. The designer using the BINA tool can identify gaps in his/her analysis. For instance, in Fig. 8.14, the designer can see that s/he has not specified a security control for the CIRP *consistency analysis*. In this case, the designer has also instantiated the security control *contingency plan - continue missions and business functions*. However, this control is not suitable for the model to meet the CIRPs modelled that meet the desired objectives for the BCI. The designer can improve his/her design by removing that control and finding one suitable for the CIRP that lacks control (i.e., consistency analysis).

Examination of the restrictions that strategic security constraints restrict objectives: Strate-

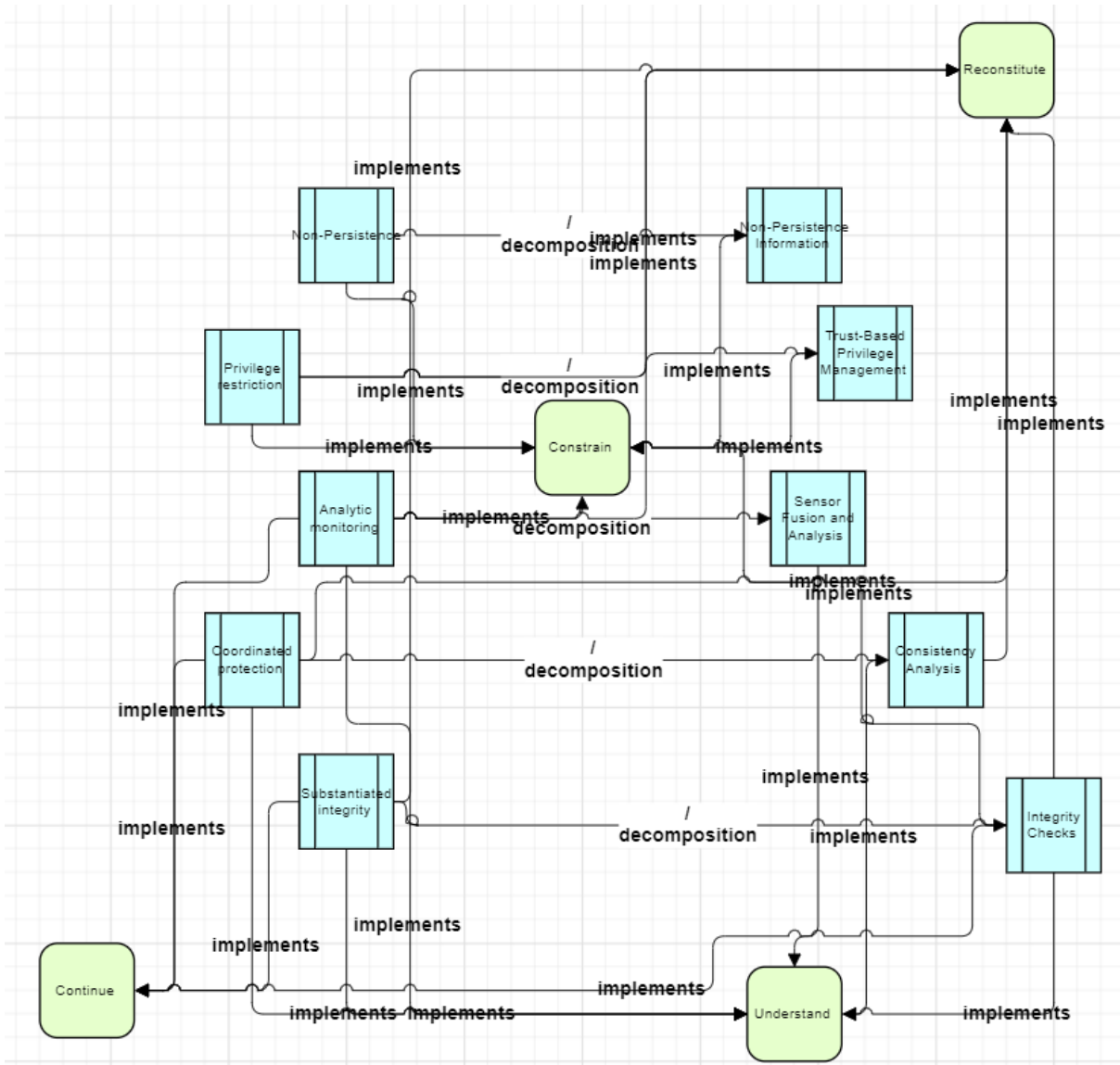


Figure 8.11: CIRPs implementing BCI objectives.

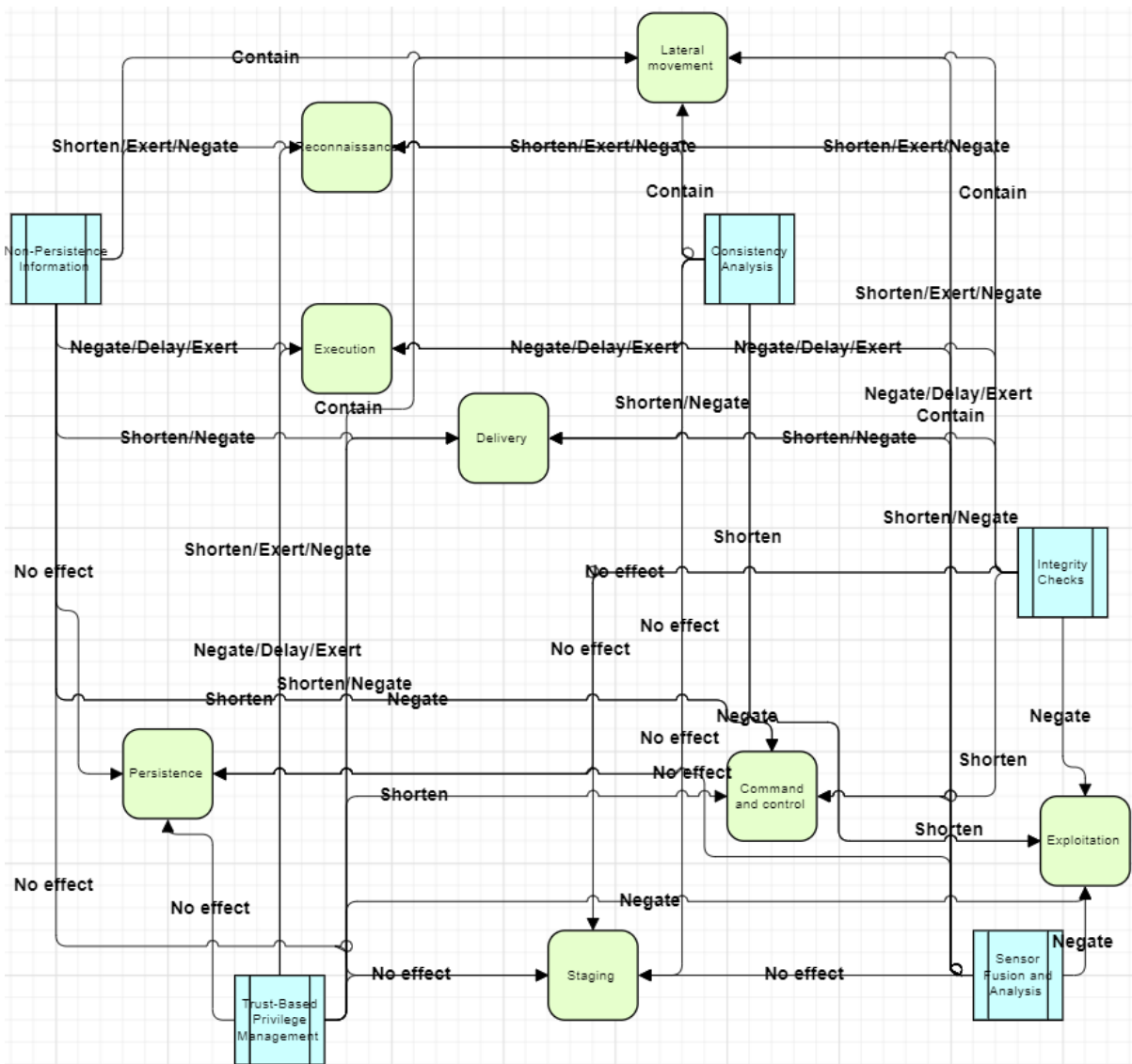


Figure 8.12: Analysis of the CIRPs effects on objectives for the BCI system.

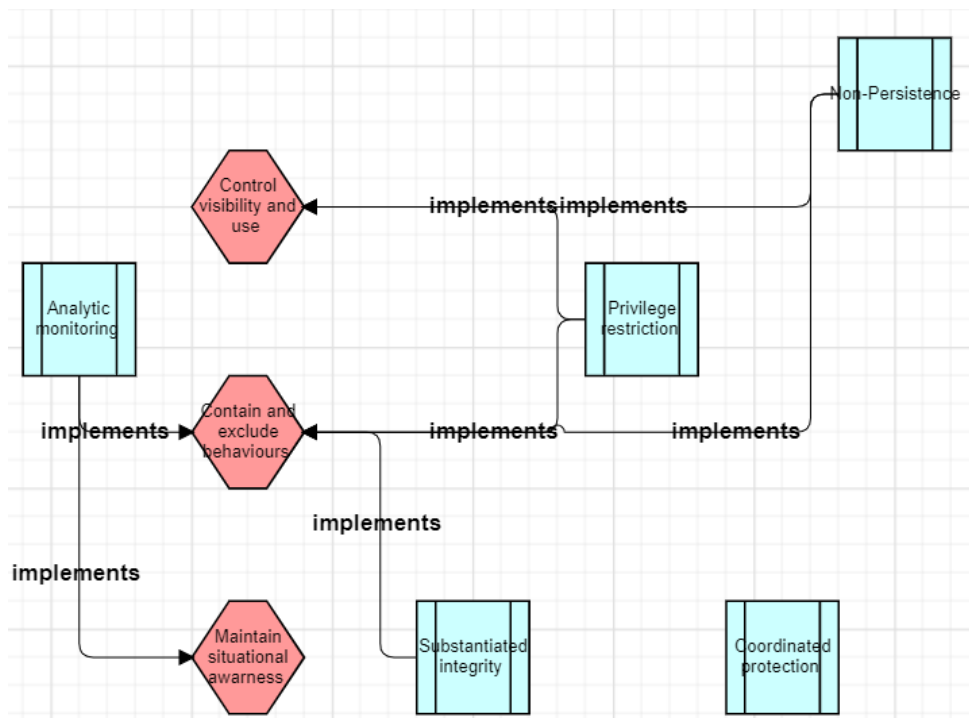


Figure 8.13: Structural security constraints implementation through CIRPs for the BCI system.

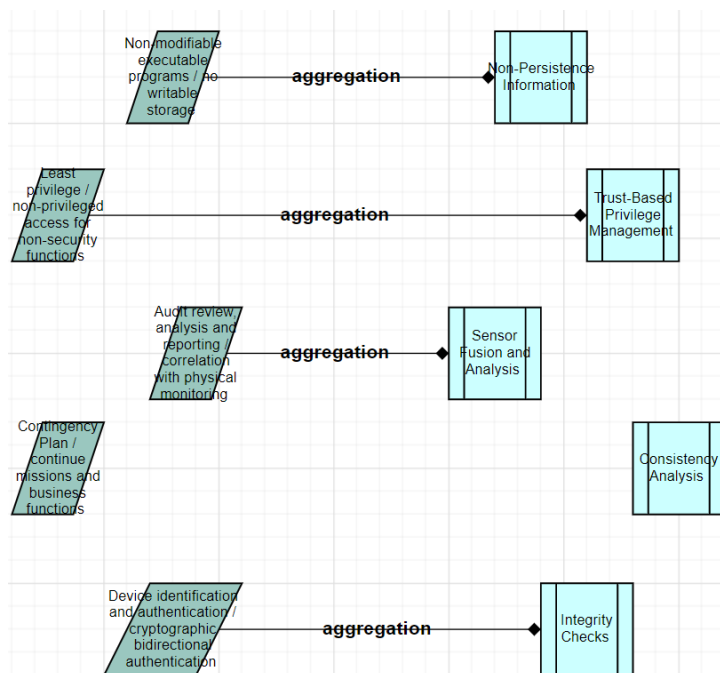


Figure 8.14: BCI security controls that aggregate to CIRPs.

gic security constraint guide and inform security analyses and resiliency analyses throughout the system life cycle and highlight different cyber resiliency techniques, and approaches to applying those techniques. *Strategic security constraints* restrict *objectives*. Security constraints indicate the type of incidents and risks the designer incorporate in his/her plan. One way to express priorities for cyber resiliency is through objectives. Each strategic security constraint supports the achievement of one or more cyber resiliency objectives. The BINA tool allows the designer to assess if the resiliency priorities are expressed through the restrictions that strategic security constraints impose on objectives. An example is shown in Fig. 8.15 where a designer can see through the BINA tool automation that most of the strategic security constraints restrict more than one objectives and that the strategic security constraint *expect adversaries to evolve* only restricts the objective *understand* that is already covered from the other constraints. Consequently, the designer can consider this restriction as redundant for the BCI resiliency model.

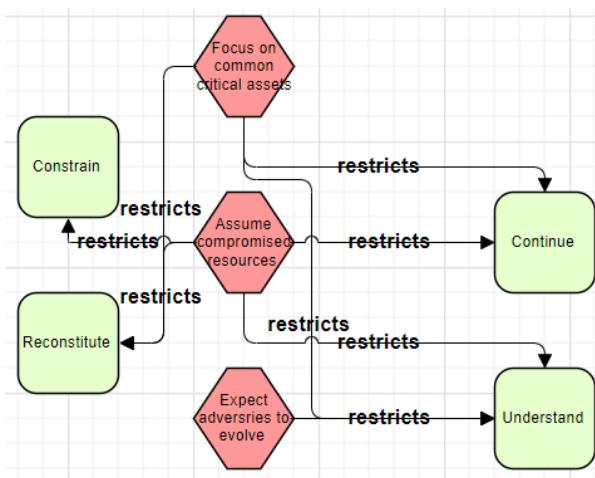


Figure 8.15: Strategic security constraints that restrict BCI objectives.

Analysis of compatibility between strategic and security objectives: Strategic objectives drive the selection of structural objectives. The decomposition relation can be used here to showed how strategic objectives link with the choices of structural objectives. A designer can use the tool to examine if the structural objectives shas modelled are justified by the strategic objectives or need to be amended. For example, in Fig. 8.16 it seems that all the strategic objectives can be decomposed to the modelled structural objectives and hence no amendments are required. Noticeable is that the strategic objective *focus on common critical assets* can be decomposed to all three of the structural objectives, namely *control visibility and use, contain and exclude behaviours* and *maintain situational awareness*.

Coverage examination of threats and correspondent objectives: The modelled threats have objectives that need to be examined further. Threats have objectives. A designer of a system-to-be wants to make sure that the threats model corresponds to adversarial objectives that need to be managed for the specific system-to-be. Fig. 8.17 shows the two threats *malicious code* with property 'stage' having the value presence and *hijacking* with property 'stage' having the value of engagement and their corresponding objectives. However, two of the objectives *reconnaissance* and *staging* do not have a corresponding threat. That means that the designer needs to either remove them from the model or find a corresponding threat that will allow him/her to expand his/her analysis.

The above resiliency analysis steps result in an updated model that can be analysed again after the changes to ensure that it is consistent with the design goals.

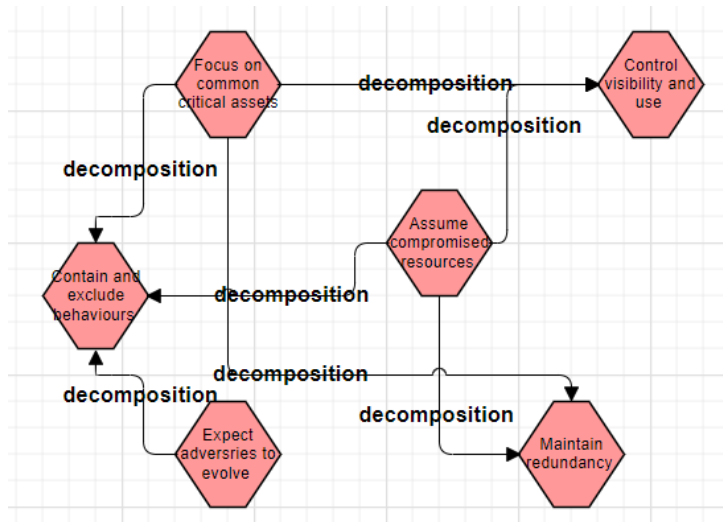


Figure 8.16: Decomposition of strategic objectives to structural objectives.

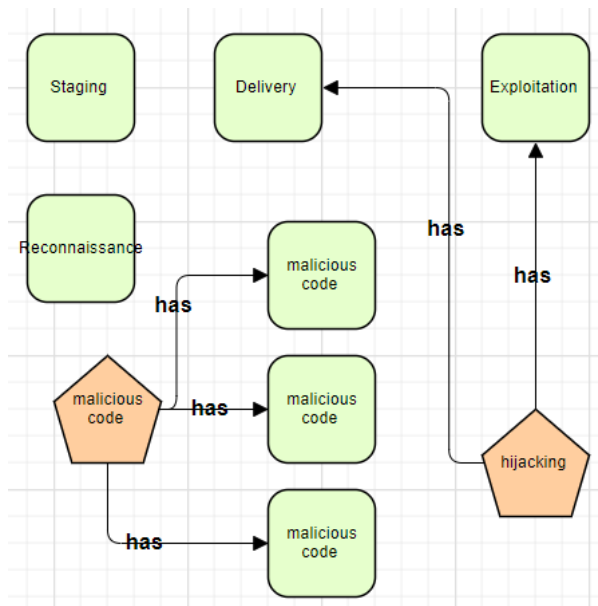


Figure 8.17: Threats and malicious objectives.

8.4 Teleoperated Robotic Systems

Teleoperated Robotic Systems (TRSs) allow human operators to control remote robots through a communication network. These robotic systems are designed to be used in areas of natural disasters, in combat zones, in underwater missions, in space. In such conditions, robots' portability and ability to operate with limited power resources becomes essential as the necessary healthcare infrastructure may not exist. Moreover, in these circumstances, operator-robot communication over available networks may be targeted by attackers, exposing the whole system to cybersecurity threats. Hence, the cyber resiliency of these systems is critical to be analysed by design.

The need for the resilient design of TRSs derives from the literature and the fact that they are used in healthcare environments. Testing the TRS NEEMO 12 in mission 16 [218], Lum et al. identified the critical network factors that need to be resilient for the TPR's performance. Such factors were communication latency, jitters, packet delays, out-of-order arrivals and packet losses [219]. Most of the issues seem to occur within the communication networks that are open and have an uncontrollable nature. Hence, malicious actors can jam, disrupt, or take over the communication between a robot and an operator.

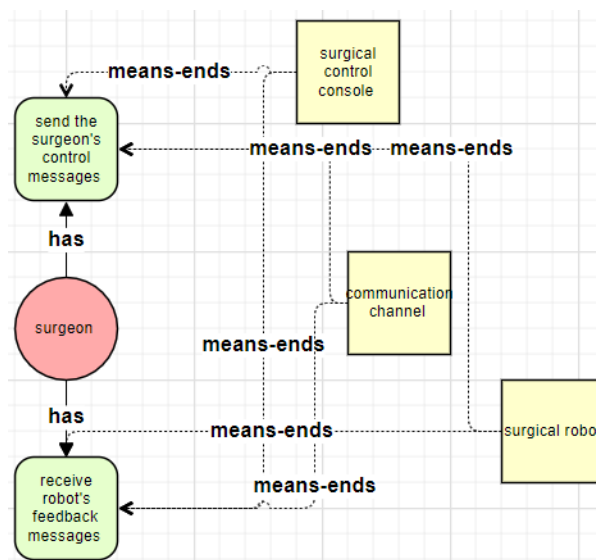


Figure 8.18: A typical interaction between a surgeon and a Teleoperated Robotic Systems.

Fig. 8.18 depicts a typical TRS where a surgeon sends and receives messages from a robot that is located remotely. It shows a surgical control console used from a surgeon to command and control through a communication channel the surgical robot. This simple depiction indicates that there can be endpoint and communication threats for TRSs that need to be analysed further. In the following sections, we use the BINA approach for that.

Activity 1: Organisational modelling

We follow a simple scenario where the actors are a *TRS*, a *patient*, *surgical manipulators* and a *surgeon*. Here the TRS is used to perform surgical operations in isolated and hostile areas.

This scenario derived from discussions with domain experts and studied publicly available organisation documents in regards to the structure of TRSs and healthcare policies. Once we had gathered as much information as we could from the domain, we constructed the system

under development organisational model. By system, we mean the TRS and the environment in which it operates. In this way, we model the goals of the system under development. Further, we identify which of them can be accomplished by the system itself and which ones are accomplished by other entities that the system depends on. It was vital to examine this, as these dependencies are a potential source of issues for resiliency planning. Fig. 8.19 depicts the TRS system organisational model that we constructed using the BINA tool.

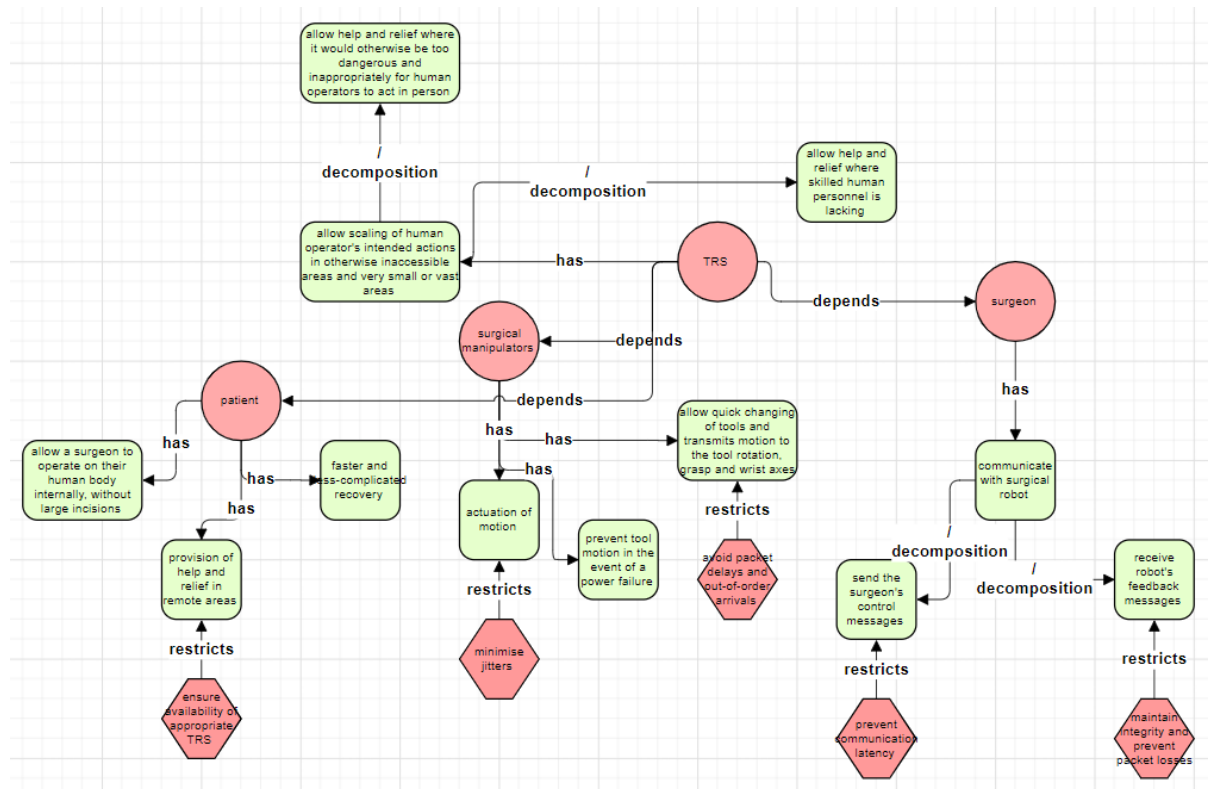


Figure 8.19: Partial TRS organisational model.

The high-level goal of the TRS system is *allow scaling of human operator's intended actions in otherwise inaccessible areas and very small or vast areas*. We decompose this high-level goal into smaller and more specific subgoals, namely *allow help and relief where it would otherwise be too dangerous and inappropriately for human operators to act in person* and *allow help and relief where skilled human personnel is lacking*.

Constructing the system goal diagram is vital in order to identify the goals that can be achieved solely by the system itself and the ones that cannot. The next step is to examine each goal and decide whether the system itself can achieve the goals or it requires interacting with other actors of the system domain. The goals that cannot be fulfilled by the system itself unless it interacts with other entities of the system domain such as a *surgical manipulators*, a *surgeon* and a *patient*. The rest of the goals are considered as goals that can be fulfilled by the system.

The TRS's goals that cannot be accomplished by the system itself were modelled as dependencies on other interacting actors. Fig. 8.19 depicts the modelled dependencies by the BINA tool. These are the following:

- The TRS system depends on the *patient* to provide *help and relief where skilled human personnel is lacking* using the system on them.
- The TRS depends on the *surgical manipulators* to *actuate motion* and *allow quick changing of*

tools and transmits motion to the tool rotation, grasp and wrist axes with a secure-by-design approach.

- The TRS depends on the operator, here the *surgeon* to *communicate with the surgical robot* with the secure-by-design.

The modelled dependencies represent the means with which the TRS can fulfil its goals and be resilient for the stakeholders. Nevertheless, they represent just assumptions; hence they require further study.

The modelled dependencies of the system on other entities of the system domain constitute a potential threat to the TRS's resiliency. The system is required to be resilient, but if the dependencies are not fulfilled when the system is implemented, then it will not be resilient. In particular, if the *patient* does not interact with the TRS appropriately, then the system is not resilient in terms of inappropriate use. For example, if the patient is tampering with the hardware. If the *surgical manipulators* does not include security controls to prevent jerky movements, then the system will not be able to serve the purposes for which it has been designed for, and instead of being resilient, it will be exposed to cyber threats. If the *surgeon* does not communicate with the TRS then the patient's safety is susceptible to attacks. Moving on and implementing the system without investigating further these dependencies by identifying ways to remove the uncertainties at this stage, will result in a system that has the risk of not being resilient.

Ultimately, we need to find resilience and control resolutions of the modelled dependencies, in order to build assurance that the TRS dependencies are fulfilled, and the TRS is resilient. In order to define appropriate resolutions for the specific context, we first need to model the security constraints that the TRS and its dependencies impose to the system design. The constraints are: *ensure availability of appropriate TRS; minimise jitters; avoid packet delays and out-of-order arrivals; prevent communication latency and maintain integrity and prevent packet losses.*

Activity 2: Incident modelling

In the current TRS experimental implementation, the operator communicates with the surgical robot over publicly available networks. This communication channel exposes teleoperated robotic procedures vulnerabilities. Due to the open and uncontrollable nature of communication networks, it becomes easy for malicious actors to affect the communication between a robot and an operator maliciously.

Attacks against cyber-physical systems, such as programmable logic controllers [220] show that security threats can affect such systems. Examples also can be seen from the vulnerabilities identified in the relevant literature [221]. Additionally, relevant proposals on private communication [222], and verification of the code on a robot's side [223] indicate that the scientific community recognises the need to make TRS resilient against cyber-physical threats.

In this incident modelling activity, we consider an attacker who aims to intercept the existing network traffic, inject new malicious traffic, or both. Communication is assumed to be wireless. That means that an on-the-field attacker will be able to disrupt the link or manipulate traffic contents. Hence, we focus on disruption and manipulation attacks against teleoperation communication links.

Fig. 8.20, depicts a typical TRS that consists of a *surgical control console*, a *communication channel* and a *surgical robot* that has the surgical manipulators. From the perspective of a legitimate operator, in this case, a *surgeon* a TRS is used in order to *send the surgeon's control messages* and to *receive robot's feedback messages*. In the core of every healthcare service is also the aim to

protect humans and the environment in the vicinity of the robot from possible injuries/damage. This goal indicates that security-oriented goals are fundamental for TRSs. These type of goals are in this case the goal *prevent robotic arms from moving too fast or in jerky motions due to malicious commands sent to the robot* and *prevent potential damage to a robot from attackers*.

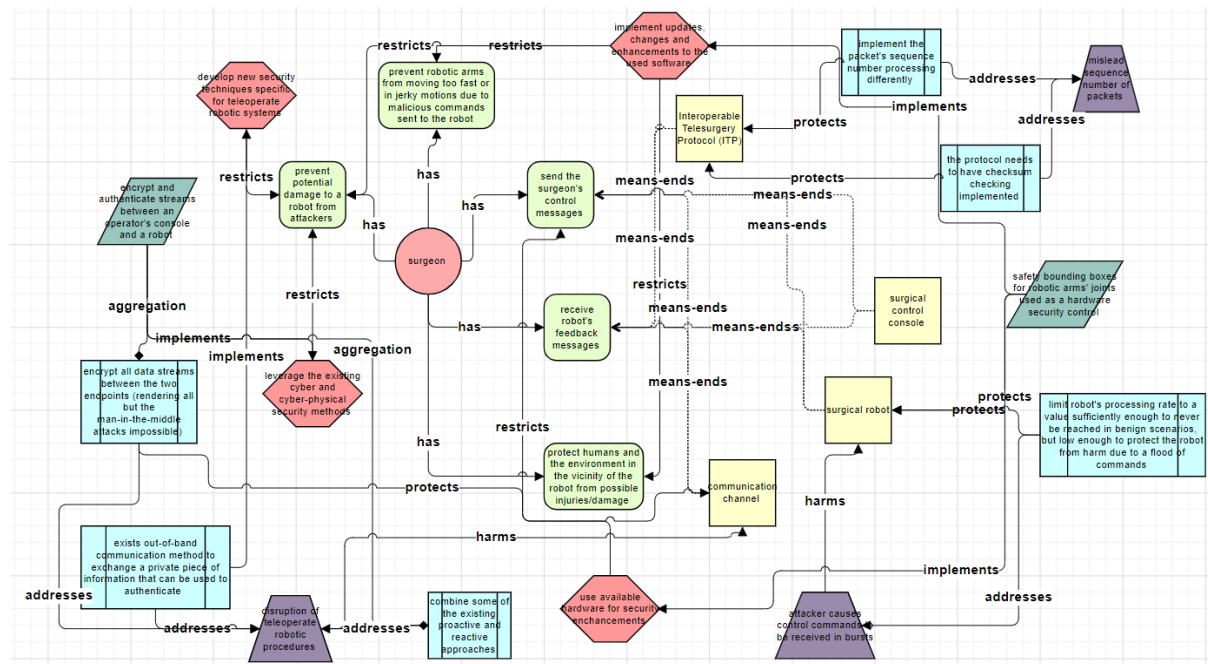


Figure 8.20: An incident scenario against a surgical TRS.

As seen in section 4.4.2, an *incident* represents a single or a series of violations or imminent threat/s of violation of security constraints. The constraints in this case study are *implement updates/changes and enhancement to the used software*; *develop new security techniques specific to teleoperate robotic systems*; *use available hardware for security enhancements* and *leverage the existing cyber and cyber-physical security methods*. The incidents that violate one or more of these security constraints or present imminent threats of their violation are *disruption of teleoperate robotic procedures*; *attacker causes control commands to be received in bursts* and *mislead sequence number of packets*.

Using BINA we take a build-in approach to resilient design and development of TRS. For that reason, we identify within this activity, possible Cyber Incident Response Plans (CIRPs) that address the incidents mentioned in the previous paragraph. The suitable CIRPs are many in this case, and some examples are *implement the packet's sequence number processing differently* and *the protocol needs to have checksum checking implemented*. Moreover, specific security controls that can be implemented are modelled at this stage. Such controls are *safety bounding boxes for robotic arms' joints used as a hardware security tool* and *encrypt and authenticate streams between an operator's console and a robot*.

Nevertheless, to be able to analyse the resiliency of a surgical TRS, we need to identify possible causes of such incidents. During this activity, we are aware of what occurrences are unwanted given to a surgeon's goals. In the following activity, we will examine possible threats that can impact a TRS in previously mentioned unwanted ways, modelled in this activity as incidents. At this stage, we have also modelled possible ways to protect critical TRS assets from these incidents. In order to examine in more detail their resiliency, we move to the third activity.

Activity 3: Holistic resiliency modelling

We identify two potential attack vectors for a surgical TRS. In the first case, the attacker targets either the surgical control console or the robot. This type of compromise will require physical access. However, we expect that either side will have monitoring controls in place to prevent such scenarios. In the second case, the attacker targets the communication channel. Since surgeon and robot communicate most likely through a wireless network, the attacker can attempt to disrupt or manipulate the communication. An attacker's goals, in that case, will be the surgeon's *intention modification*, *intention manipulation* or *hijacking*. These malicious intentions can be modelled through BINA, as shown in Fig. 8.21.

If an attacker aims to modify the surgeon's intentions when using the surgical TRS, then he/she/they will modify the surgeon's messages while the packets are in-flight. This can be seen in Fig. 8.21 as the attacker's goal *intention modification*. If an attacker aims to modify feedback messages from the robot to the surgeon, then a valid surgeon's actions can be harmful to the patient and the environment as the surgeon is operating with a distorted representation of the patient's health status and overall situation. This scenario is captured from the goal *intention manipulation*. Finally, an attacker can target the surgical robot and make it to ignore the surgeon's commands completely. Depending on what actions the attacker who has successfully hijacked the surgical robot executes the consequences will be determined. These scenarios are modelled with the generic attacker's goal *hijacking*.

The *attacker* needs to assume a role within the system to mount the different attacks. He/she/they can initially eavesdrop on information exchange between an operator and a robot, and based on the collected information, starts inserting false messages into the network, while still allowing both innocent parties to communicate directly. This type of attacker is modelled as *network observer*. Alternatively, an *attacker* assumes the role of an intermediary between a robot and an operator, thus wholly preventing the innocent parties from communicating directly. This type of attacker is modelled as *network intermediary*.

From a security perspective, a TRS can have to operate in severe conditions and uncertain environment. The main objectives for the TRS as identified in the literature [224, 225, 226] are *secure delivery of control inputs to a robot, and force and video feedback to an operator; steady operation under large communication latencies, jitter and packet losses; and resilience to communication delays, device failures and unexpected events* (cf. Fig. 8.21). Security constraints restrict these goals. For example, *privacy/confidentiality*; *data integrity*; *signature*; *message authentication*; *authorisation and identity authentication* restrict the objective *secure delivery of control inputs to a robot, and force and video feedback to an operator*. The meaning of each security constraint is further analysed below.

Privacy/confidentiality stands for the requirement to keep information secret from authorised operators and remote robots. *Data integrity*, secures that messages to and from an operator are not corrupted by events (e.g., communication errors) or incidents (e.g., unauthorised entities). *Signature* ties control commands to an operator and feedback data to a robot. This objective will be important when multiple operators collaboratively control a remote robot. *Message authentication* undeniably confirms the origin of each message. *Authorisation* ensures that only authorised operators can control robots. *Identity authentication* confirms the unique identities of an operator and a robot.

Time-stamping records the times that control and feedback information are created. *Receipt* is the acknowledgement of receiving information. *Confirmation* acknowledgement of services provided through force and video feedback. *Revocation* withdraws authorisation at any point in time, which is an essential requirement for manipulators with limited times of use.

In this activity so far, we have been updating and reviewing the existing model of the TRS. Doing so is very important because when mounting an attack against TRSs, an adversary may exploit a specific system property, and disrupt an ongoing procedure by invalidating any of these security constraints.

The attacker uses an *attacking machine*, which runs Kali Linux, and s/he/they write attack implementations in Python with the Scapy framework. The attacker targets the following assets *the surgical control console, the communication channel and the surgical robot*. The attacker establishes communication between the surgical control console and the surgical robot through a communication channel hub (cf. Fig. 8.21). This communication allows the attacker to connect an external computer to the same subnetwork. S/he/they then use that computer to observe and modify the communication between the surgeon and the robot. This simplified example allows us to abstract the communication between the surgeon and the surgical teleoperated robotic systems into a layer common to all communication systems, and a layer-specific to teleoperated robotic systems. We then focus on the resiliency of the layer-specific to teleoperated robotic systems, instead of focusing on known and well-analysed threats that penetrate communication networks (c.f. [227, 228]).

Examining the layer-specific to teleoperated robotic systems, an attacker can modify a surgeon's intended actions changing the original messages while packets are in-flight. The *intent modification* threat models this malicious attempt. Another attack approach can be to manipulate a robot to cause harm, modelled as *hijacking* threat. An attacker might also attempt to make a TRS or a communication channel unavailable to their intended and legitimate users, modelled as a *denial-of-service* threat. Finally, an attacker can negatively impact a teleoperated procedure by intentionally and maliciously delaying the exchange of messages between a surgeon and a remote robot, modelled as the threat *delay*.

For each of the analysed classes of threats, we seek to model an informed understanding of risks, events, incidents and vulnerabilities. For example, the threat *intent modification* relates with the incidents *surgeon's intent loss; surgeon's intent modification and surgeon's intent reordering*. These incidents can be observed as the events *robot's motion becomes delayed and jerky; difficult to use if grasping becomes challenging or almost unusable; the robot's safety mechanism clips the currents, resulting in a noticeably slower robot motion and jerky motion of robot's arms*.

In the case of *surgeon's intent loss*, the attacker poses the risk of *randomly dropping individual surgeon's packets or groups of packets*. As a result, the event *robot's motion becomes delayed and jerky* occurs. Depending on the packets' dropping rates, the robot can be operable but challenging to use as grasping becomes challenging or almost unusable, especially if the surgery requires small and precise movements.

In the case of the *surgeon's intent modification*, the attacker poses the risk of *modify surgeon's packets on-the-fly before forwarding them to the robot through his/hers/theirs malicious proxy*. The attacker can do so by leveraging knowledge about a surgeon's packets' structure, from the Interoperable Telesurgery Protocol [229]. The attacker's modifications can affect the robot's position, rotation, grasping of robotic arms, invert left and right robotic arms to name a few. These events have a noticeable impact on the robot. Once the attacker's modifications require very large or fast changes in robotic arms positions, requiring too high currents, the robot's safety mechanism will clip the currents, and the robot will be noticeably slow.

In the case of the *surgeon's intent reordering*, the attacker instead of forwarding a surgeon's packets to the robot, s/he/they *adds the surgeon's packets to a queue on the attacking machine, that pops items out in random order once it reaches the maximum length*. That means that the surgical robot receives these packets with delay and skips those with sequence numbers received out of order. This threat results in the event of *jerky motion of the robot's arms*.

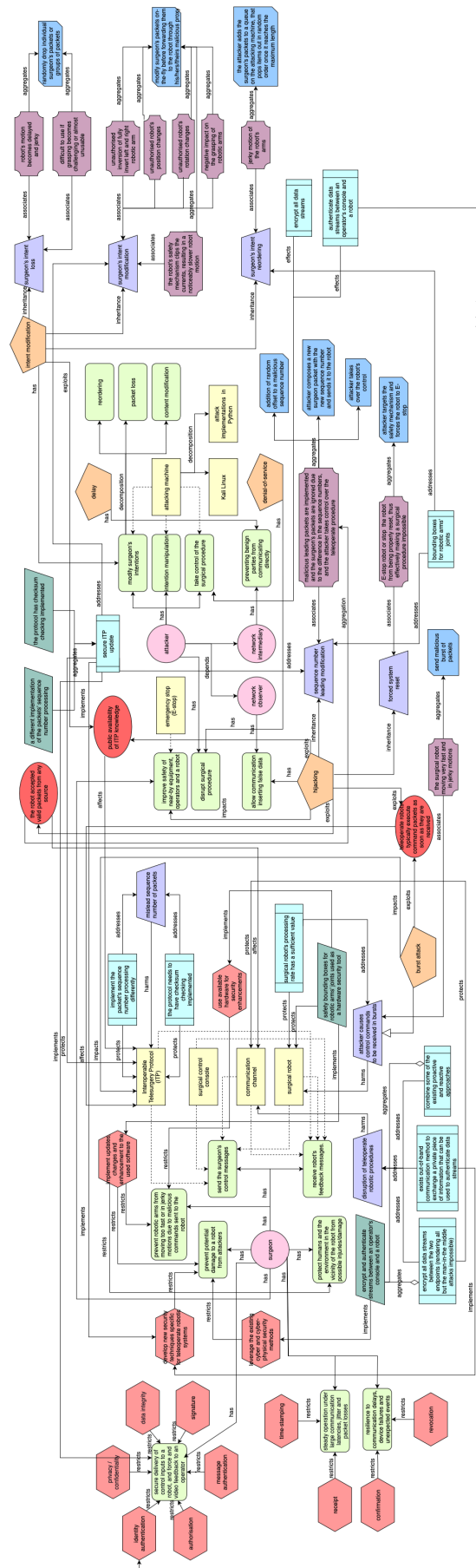


Figure 8.21: Holistic resilience model for a surgical TRS.

For the threat *hijacking*, an attacker becomes a *network observer*. S/he/they can eavesdrop on packets between a surgeon and a robot, without modifying them. Here the attacker is interested in the current packet's sequence number. After sufficient reconnaissance, s/he/they inject new, malicious packets into the network to impact the surgical procedure. S/he/they do that either using a *sequence number leading modification* or *forcing the robot to reset*.

In the first case, the attacker having knowledge about the structure of a surgeon's packet [229], first reads a single surgeon's packet, and extract its sequence number. Then *adds a random offset to a malicious sequence number*. Then the attacker composes a new surgeon packet with the new sequence number and sends it to the robot. The attacker takes over the robot's control, since the robot attributes the large jump in sequence numbers to packet drops, and as long as the system does not lose more than a second worth of data, the operation continues. The malicious packets are implemented, and the surgeon's packets are ignored due to the difference in the sequence numbers, which means that the attacker has taken control of the teleoperated procedure.

In the second case, extending the previous threat, the attacker targets the robot's inherent safety mechanism. The attacker sends a packet to the robot that commands the robot's arms to move very fast or go to an unsafe position. This type of commands activates the robot's safety software that imposes a system-wide halt called software emergency stop (E-stop). The E-stop stops the system from operating, protecting electrical, mechanical components and most importantly humans from harm. However, the attacker sends on purpose packets modifying the position or rotation of the robotic arms above the safety threshold. That causes the robot to either go too fast or go to an E-stop.

If the attacker continues to send malicious packets of that type (that violate safety requirements) the robot will stop from ever correctly resetting. Hence, the attacker can make, in this case, a surgical procedure impossible. This case introduces to the model the *emergency stop (E-stop)* asset and the surgeon's goal *improve the safety of near-by equipment, operators and a robot*. Initially, the surgeon might not have listed this goal as one of the resiliency aims to the surgical robot's designer. This process though helps the security engineer to extract such goals of the stakeholders.

The security engineer can similarly analyse denial-of-service threats and delays. Modelling the threats, vulnerabilities, incidents, events and risks, we can now identify ways to make the TRS resilient. For that purpose, we introduce a couple of CIRPs to the BINA model.

An essential first step for a secure and resilient system is the implementation of updates. More specifically we add the CIRP *secure ITP update*. By introducing this CIRP, we can avoid some of the incidents that occur when a TRS is under attack. More specifically, if this CIRP is implemented with the security control *a different implementation of the packets' sequence number processing*, then the incident *sequence number leading modification* can be avoided. Whereas if the same CIRP is implemented with the security control *the protocol has checksum checking implemented* then the incident *surgeon's intent modification* can be avoided.

Another vulnerability that the threats exploit seems to be that *teleoperate robots typically execute command packets as soon as they are received*. In this case, the event of *the surgical robot moving very fast and in jerky motions* can be observed. Moreover, an attacker can deliberately cause control commands to be received in bursts. To protect against the threat of *burst attacks*, we introduce the CIRP *surgical robot's processing rate has a sufficient value*. That value needs to be large enough, so it is not reached in benign scenarios and low enough to guard the surgical robot against harm due to a burst of commands.

As we can observe in the BINA model for the surgical TRS, safety mechanisms to protect the system's physical aspect already exist. Such physical security controls can be extended to

cybersecurity controls to make TRSs resilient. One such CIRP is the *bounding boxes for robotic arms' joints*. This safety mechanism can also make the robotic arms resilient to malicious commands that aim to make them move too fast or in jerky motions.

Another vulnerability is that *the robot accepted valid packets from any source*. A CIRP that can be used is to *encrypt all data streams* between the two endpoints. This CIRP will render most threats impossible, except man-in-the-middle threats. Also, surgical robots are expected to have dedicated staff at one end of the system. Consequently, an out-of-band communication method can be used for the exchange of private information for authentication. This can also be modelled as the CIRP *authenticate data streams between an operator's console and a robot*. These CIRPs will make the robotic surgical system *intention modification, manipulation, and hijacking* threats and consequent incidents more difficult to occur and hence the TRS will be more resilient.

After modelling CIRPs and security controls, the designer determines the importance level of the CIRPs and their reliance level. S/he/they can do so using the 'properties' and changing the relevant value accordingly (c.f. Fig. 8.22). For example, for the CIRP *secure ITP update* the importance and resilience level are 1. Similarly, we fill in the information for the other CIRPs in the model.

We define these properties by first justifying if the CIRPs were valid or not and modify their "risk reduction" property, respectively. For the CIRP *encrypt all data streams* previous studies have shown that this approach is applicable and experimental evidence supports this assumption. Consequently, the property "risk reduction" takes the value 'true'. However, for the CIRP *secure ITP updates*, there is no sufficient published work on the subject, and there are not established updates yet. Therefore this is not a valid CIRP, and as a consequence, the system's objective *secure delivery of control inputs to a robot, and force and video feedback to an operator* may not be fulfilled. Eventually, these CIRPs would have become potential vulnerabilities of the TRS. Thus, additional requirements need to be added to the system's functionality to ensure the fulfilment of objectives and the system's resiliency.

Moving to the "importance level" property, the designer determines if the modelled CIRPs are essential or not for the surgical TRS's overall resiliency. If they are they take the value 1, alternatively they take the value 0. For example, the CIRP *secure ITP update* takes the value 1 as if not included in the TRS resiliency design might mean that the objective *secure delivery of control inputs to a robot, and force and video feedback to an operator* might become unattainable. We do that for the rest of the CIRPs and then move to the next property.

It is crucial here to mention that the property "risk level" is automatically generated from the designer's inputs in the rest of the constructs' properties. More specifically, as we have seen in Section 5.5, the risk level is generated from the function:

$$\text{Risk level} = f(\text{Potentiality} \times \text{Impact level})$$

Activity 4: Resiliency analysis

Using the BINA tool, the designer can firstly validate the correctness of the model created based on the metamodel. This analysis happens automatically when the user presses the 'analysis 1' in the BINA tool. After the designed model's correctness assessment takes place from the tool and the designer, further analysis can take place that can raise several critical implementational issues. For example, if the constructs are connected with the appropriate relations.

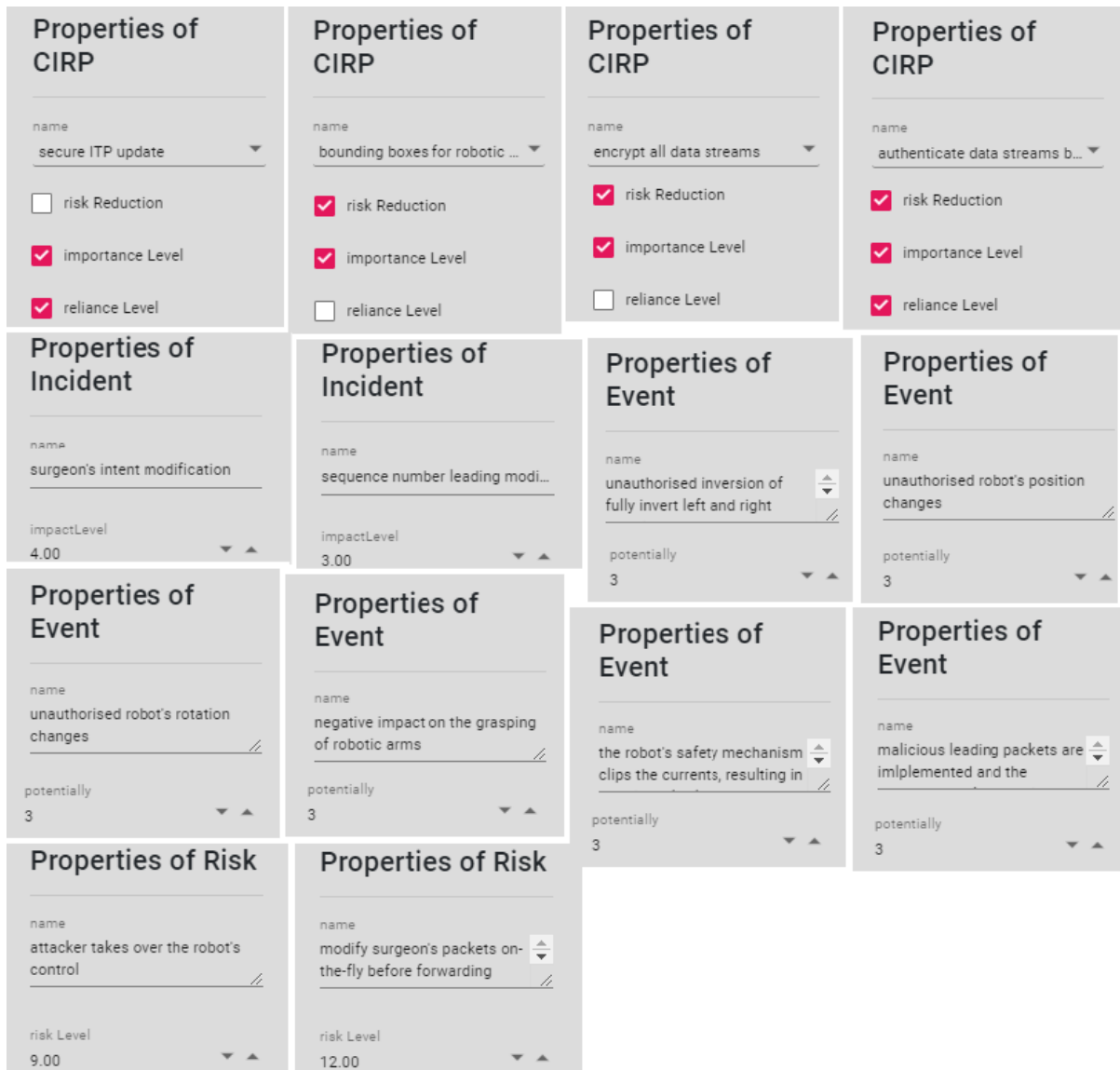



Figure 8.22: TRS Properties determination.

System resiliency before and after the resiliency analysis: Firstly, at any stage, the BINA tool automatically assessed the BCI system's resiliency. Before the resiliency analysis, the trustworthiness was at 50%, as shown in Fig. 8.23. When the analysis progressed, and the designer addressed the relevant issues by adding resiliency requirements, the BCI's resiliency became 100%.

Potential interactions between CIRPs: For the surgical TRS, the designer introduces six new CIRPs based on newly modelled resiliency objectives. The surgical TRS needs to *monitor and analyses the TRS's ongoing properties and behaviours*. This objective can be implemented, introducing the CIRP *analytic monitoring*. The designer models also the resiliency objective *maintain the posture of surgical operations considering threats*. The CIRP *contextual awareness* implements this objective. The designer also models the objectives *ensure the security controls operate in a coordinated manner and as intended; hide critical assets; limit privileges of users, system elements and environmental factors* and *reduce the risk of teleoperated surgeries aligning TRS resources*. The relative CIRPs that implement these objectives are *coordinated protection; deception; privilege restriction* and *realignment*.

 TRS	
Property	Value
Dependence level	0.375
System resiliency	50%


 TRS	
Property	Value
Dependence level	
System resiliency	

Figure 8.23: System resiliency before and after the resiliency analysis.

The introduced CIRPs can support (S), depend (D), use (U) and conflict or complicate (C) each others implementation. The relations among CIRPs are in accordance with the cyber resiliency techniques presented in NIST SP 800-160v2 [10]. Fig. 8.24 depicts an example of this type of analysis for a surgical TRS. For example, *analytic monitoring* **supports** the CIRP *contextual awareness* whereas *contextual awareness* **uses** the *analytic monitoring* as that gives more options available, even though the first CIRP can be implemented effectively in the absence of the second CIRP. The CIRP *deception* **conflicts** but in some instances, it might support *contextual awareness*. For example, if the *deception* stands from hiding critical assets, it complicates the implementation of *contextual awareness*. However, if *deception* stands for exposing covertly tainted assets to the attacker, it supports the implementation of *contextual awareness*. The implementation of the CIRP *analytic monitoring* **depends** on the CIRP *coordinated protection*, differently it will be ineffective. These examples sum up the different relations between CIRPs (cf. Fig. 8.24).

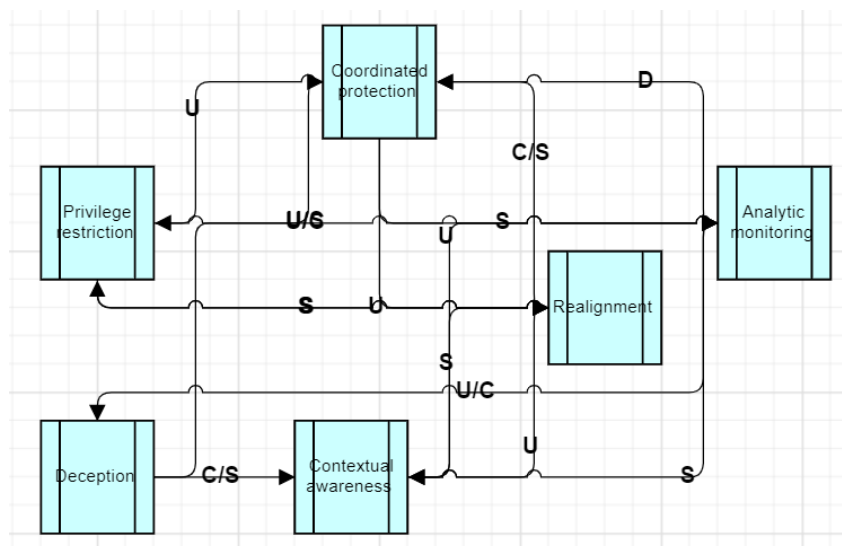


Figure 8.24: Potential interactions between TRS's CIRPs.

Assessment of the implementation of objectives using the selected by the designer CIRPs: CIRPs can also further be analysed in relation to the *security objectives* that they implement. Objectives motivate the definition of security requirements and the selection and tailoring of CIRP.

For example, the objective *prepare* implies that a CIRP needs to support and maintain a set of appropriate courses of action that thwart adversity. The objective *continue* indicates that a CIRP is needed to extend the duration and reliability of a surgical procedure in the presence of a threat. The objective *constrain* requires to model a CIRP that limits the impact of an adversarial attack. The objective *understand* expresses the need for a CIRP that offers situational awareness of the resources necessary for a surgical procedure under siege. Finally, the objective *transform* asks for a CIRP that support surgical processes continuation under adversarial and environmental changes.

Consequently, a designer can use objectives as a starting point for eliciting restatements of objectives and analysing how CIRPs meet these objectives or not. Using the objectives suggested in NIST SP 800-160v2 [10] and focusing on the TRS system, the designer through the BINA tool derives the relations shown in Fig. 8.25. The designer can see in that way that some CIRPs implement the same objectives, such as the CIRPs *malware and forensic analysis*; *dynamic threat modelling* and *consistency analysis* implement the objective *understand*. Based on this information and a limited security budget, the designer might choose to remove the CIRPs *malware and forensic analysis*; *dynamic threat modelling* as the other CIRP *consistency analysis* achieves the same objective and simultaneously the objective *prepare*.

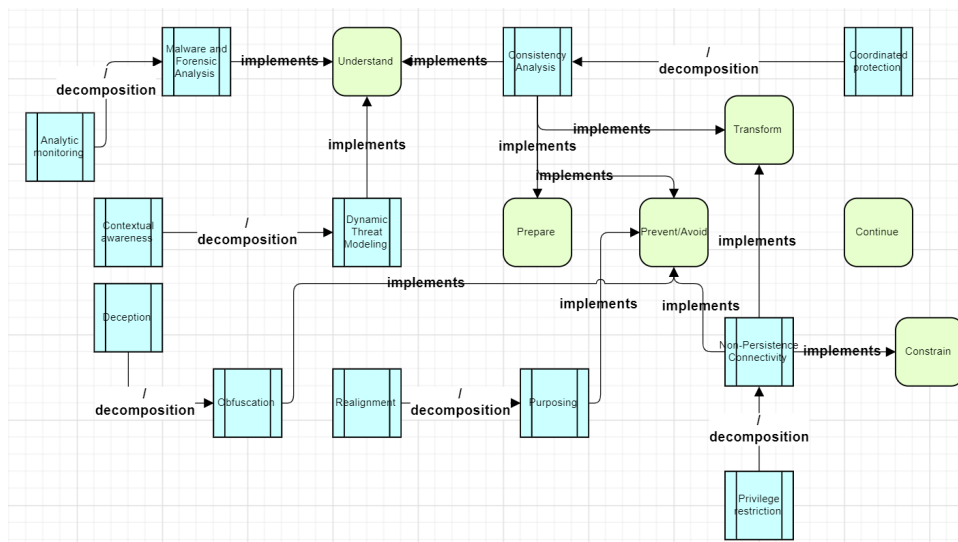


Figure 8.25: CIRPs implementing TRS objectives.

Analysis of the CIRPs effects on malicious objectives: The designer wants to effect malicious objectives that an adversary can have. S/he/they can do so by incorporating CIRPs as part of the model. Using the BINA tool, these *effect* relationships became more specific as shown in Fig. 8.26. Assuming that the adversary does not have prior knowledge of the system-to-be, a set of objectives can be selected from the designer and modelled using the BINA tool. Then the tool analyses these relationships and characterises them. Subsequently, the tool analysis these relationships and characterises them. For instance, the CIRP *malware and forensic analysis* **detects, scrutinises and reveals** the adversarial objectives *deny, destroy, command and control* and *evasion*. The same CIRP also **detects** the malicious objective *modify*.

Examination of coverage of structural security constraints with the implementation of CIRPs: Based on NIST SP 800-160v2 [10] CIRPs implement structural security constraints. Structural security constraints guide and inform the design and implementation decisions throughout the surgical TRS life cycle. Many of the structural design principles are consistent with or leverage the CIRPs. If CIRPs are not sufficient, the designer will need to add more,

or if the model has redundant CIRPs the designer will need to remove them. This type of analysis is facilitated by the BINA tool that offers the capability to define structural security constraints and examine the coverage of the CIRPs that initially the designer has modelled. Fig. 8.27 shows that whereas most modelled CIRPs implement structural security constraints such as *leverage health and status data* is implemented with the use of the CIRPs *analytic monitoring* and *contextual awareness*. As the CIRP *contextual awareness* does not implement any other structural security constraints, unlike the CIRP that *analytic monitoring* that also implements the structural security constraints *layer defences and partition resources* and *contain and exclude behaviours*, the designer can choose and justify through this diagram the removal of the CIRP *contextual awareness*.

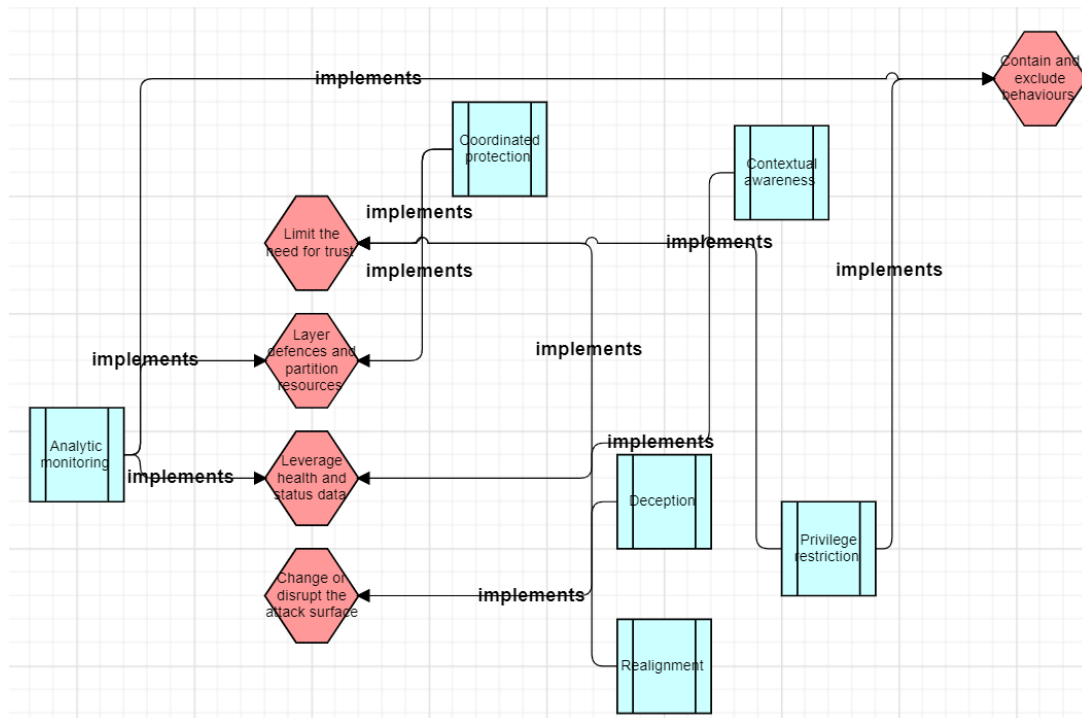


Figure 8.27: Structural security constraints implementation through CIRPs for the TRS.

Assessment of CIRPs specification with security controls: The designer can also analyse using the BINA tool the implementational aspect of the modelled CIRPs. CIRPs aggregate security controls. The designer can identify gaps in his/her analysis or redundant security controls using the BINA tool. For instance, in Fig. 8.28, the designer can see that s/he/they have for the CIRP *analytic monitoring* three security controls, namely *configure systems and components for high-risk areas*; *incident handling information correlation* and *decoys*. As the security control *configure systems and components for high-risk areas* do not aggregate to any other CIRP; the designer can consider it redundant and remove it from the model. The updated model will still meet the CIRPs required to maintain the surgical TRS's objectives.

Examination of the restrictions that strategic security constraints restrict objectives: Strategic security constraints guide and inform security analyses and resiliency analyses throughout the system life cycle and highlight different cyber resiliency techniques and approaches to apply them. *Strategic security constraints* restrict objectives. Security constraints indicate the type of incidents and risks the designer incorporate in his/her plan. One way to express priorities for cyber resiliency is through objectives. Each strategic security constraint supports the achievement of one or more cyber resiliency objectives. The BINA tool allows the designer to assess if the resiliency priorities are expressed through the restrictions that strategic security constraints impose on objectives. An example is shown in Fig. 8.29 where a designer can see

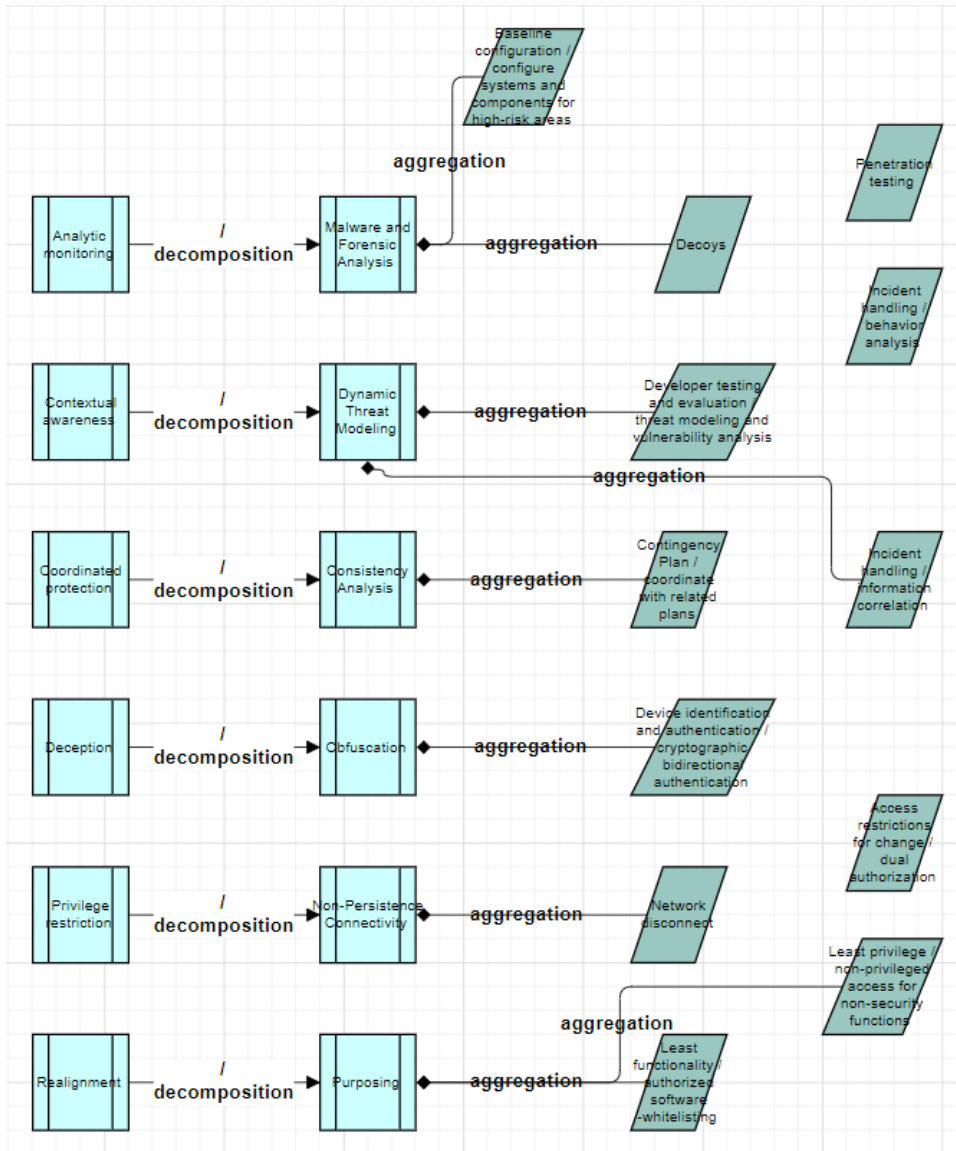


Figure 8.28: TRS security controls that aggregate to CIRPs.

through the BINA tool automation that most of the strategic security constraints restrict more than one objectives and that the strategic security constraint *assume compromised resources* restricts all five of the objectives. Due to limited surgical TRS design and development resources, the designer might choose to remove the other constraints as redundant for the surgical TRS resiliency model.

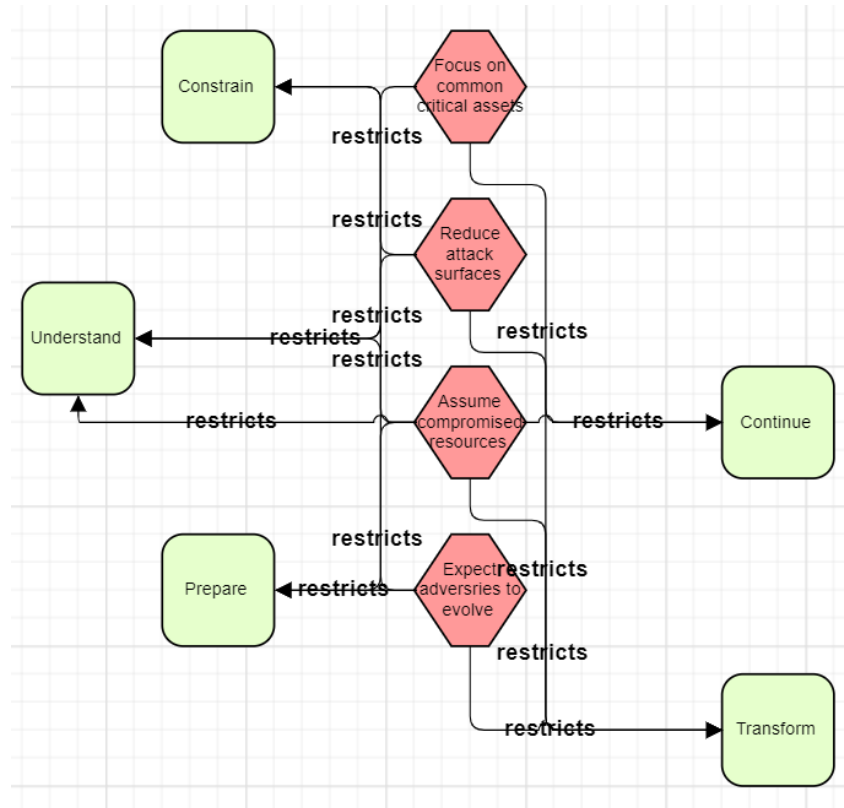


Figure 8.29: Strategic security constraints that restrict TRS objectives.

Analysis of compatibility between strategic and security objectives: Strategic objectives drive the selection of structural objectives. The decomposition relation can be used here to show how strategic objectives link with structural objectives' choices. A designer can use the tool to examine if the structural objectives shave modelled are justified by the strategic objectives or need to be amended. For example, in Fig. 8.30 it seems that all the strategic objectives can be decomposed to the modelled structural objectives and hence no amendments are required. Noticeable is that the strategic objective *assume compromised resources* can be decomposed to all five of the structural objectives, namely *contain and exclude behaviours; limit the need for trust; layer defences and partition resources; leverage health and status data and change or disrupt the attack surface*.

Coverage examination of threats and correspondent objectives: The modelled threats have objectives that need to be examined further. Threats have objectives. A system-to-be designer wants to ensure that the threats modelled correspond to adversarial objectives that need to be managed for the specific system-to-be. Fig. 8.31 shows two of the threats, namely *hijacking effect* and *ongoing intent modification* and their corresponding objectives. In this example, all objectives have a corresponding threat. That means that the designer does not need to introduce more threats in the model to analyse the attacker's profile of his choice. This automation gives him a clear indication of when to finish his analysis and justify that decision.

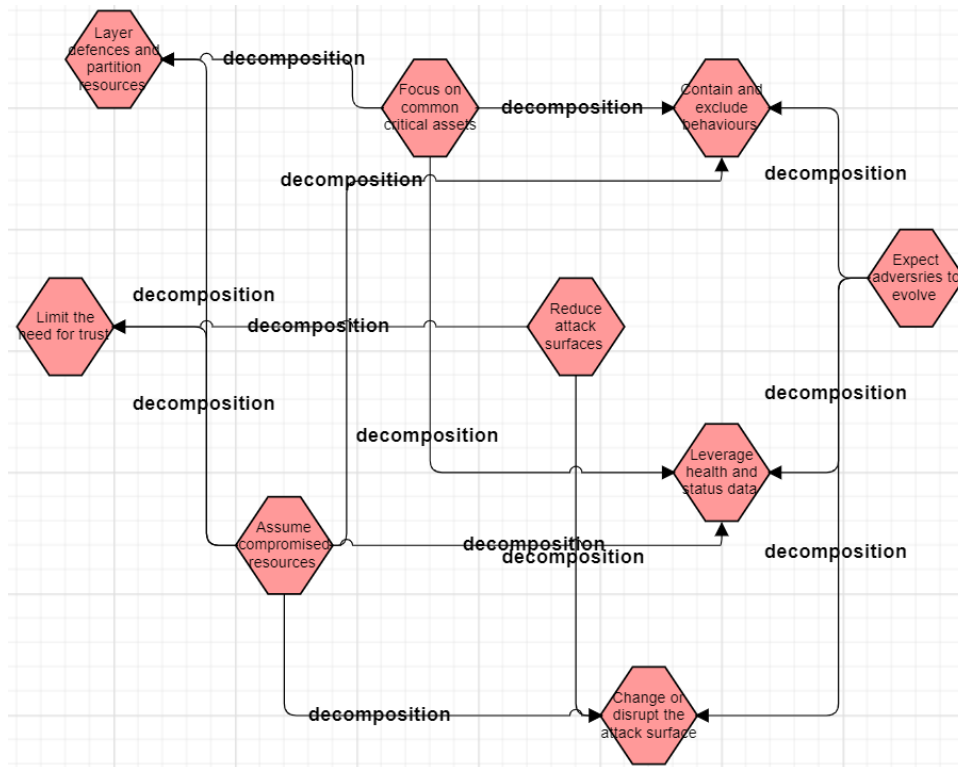


Figure 8.30: Decomposition of strategic constraints to structural constraints.

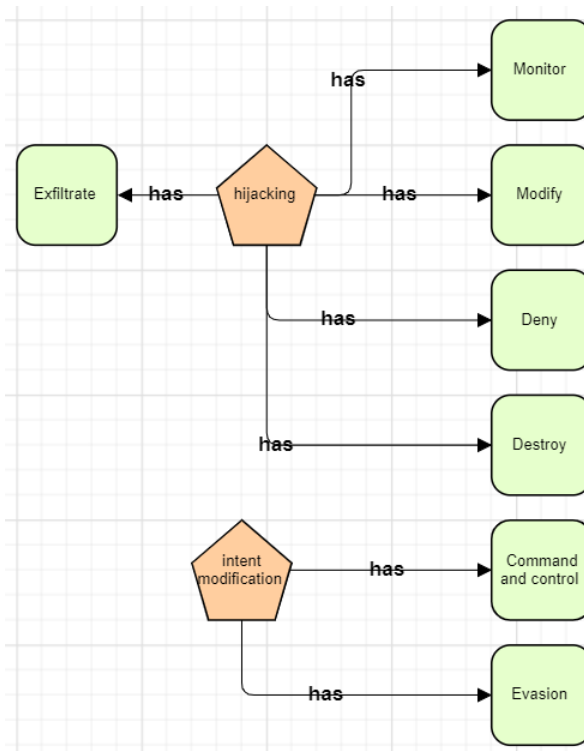


Figure 8.31: Threats and malicious objectives.

8.5 Evaluation of BINA methodology by case study research in the health care domain

This case study follows the same design objectives, context, collection, analysis and validity methods as those used in section 8.1 for the proof-of-concept. However, here we examine the experience of conducting a case study on applying BINA methodology in the UK's health care domain.

The Hospital at Home nursing team's primary duties include physical visits to patients' homes and the provision of healthcare services on site.

Clinical supervision is an integral part of quality assurance for the provision of healthcare services. Typically, a senior member of staff conducts clinical supervision through physical presence. Technology can support this process, allowing remote clinical supervision. In this way, clinical supervision costs are less and can happen even during pandemics, as COVID-19. The senior member of staff uses smart glasses to conduct clinical supervision remotely.

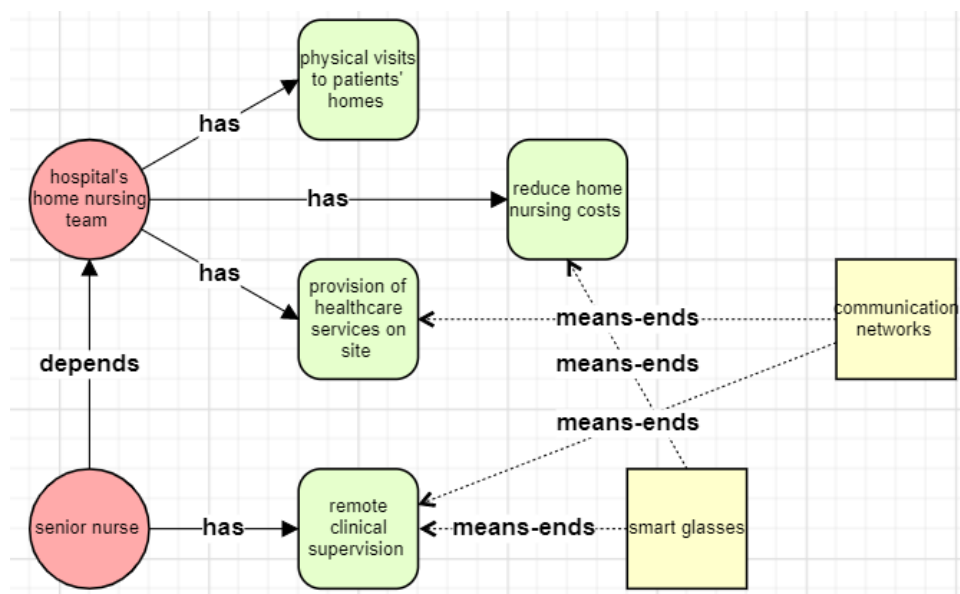


Figure 8.32: A typical interaction between a hospital's home nursing team and a smart glasses system.

Fig. 8.32 depicts a typical hospital's home nursing team where a senior nurse wants to conduct remote clinical supervisions. The senior nurse depends on the nursing team to visit a patient's home, use smart glasses and broadcast live video of image and sound. This simple model indicates that there can be endpoint and communication threats for the smart glasses and the communication networks they use to transfer real-time healthcare data that needs to be analysed further for resiliency.

8.5.1 Activity 1: Organisational modelling

We follow a typical scenario where the actors are a *community nurse*, a *patient*, a *senior nurse* and a *telemedicine system*. Here the telemedicine system is used to remote deliver healthcare services to patients' homes.

We formed the scenario based on discussions with domain experts, and we also studied

publicly available organisation documents regarding the structure of tele-medicine systems and healthcare policies. Once we had gathered as much information as we could from the domain, we constructed the organisational model. We started by modelling the objectives of the system under development. We identify which of them can be accomplished by the system itself and which ones are accomplished by other entities that the system depends. It was vital to examine this, as these dependencies are a potential source of resiliency planning issues. Fig. 8.33 represents the telemedicine system in an organisational model constructed using the BINA tool.

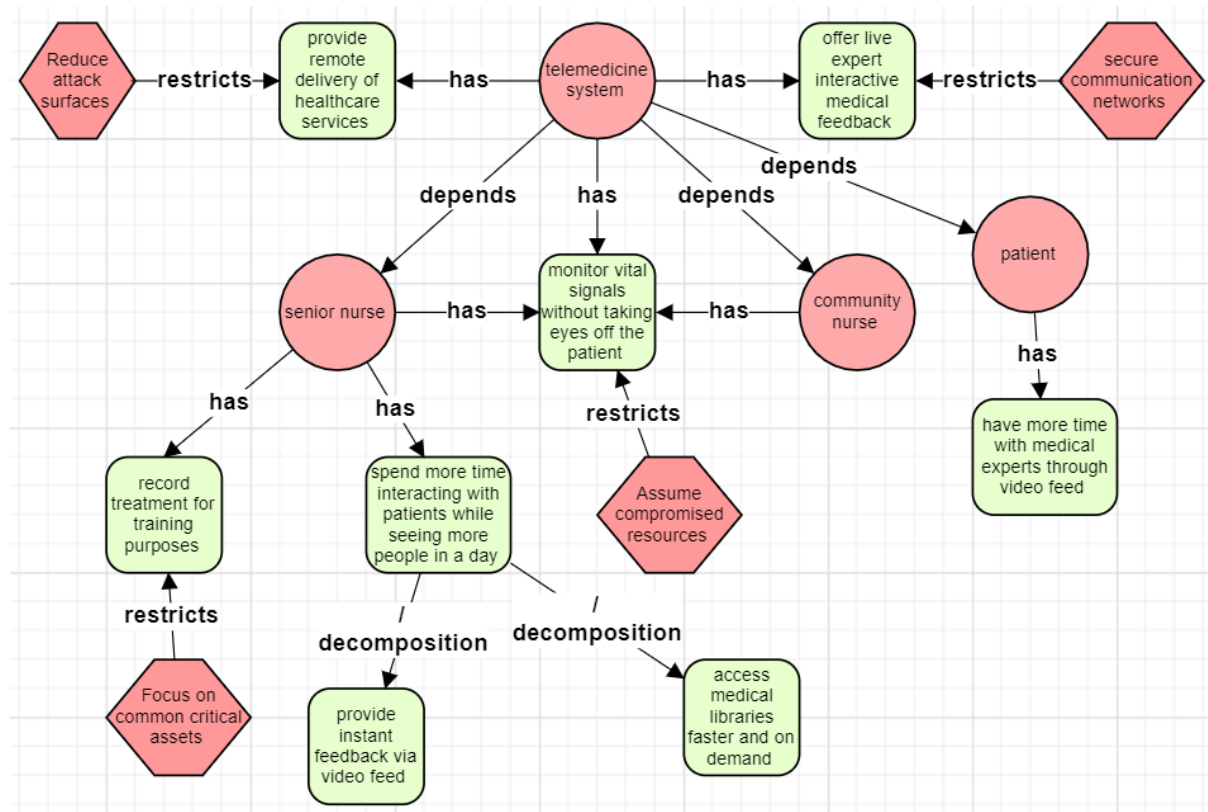


Figure 8.33: Partial telemedicine system organisational model.

The goals of the telemedicine system are to *provide remote delivery of healthcare services*; *offer live expert interactive medical feedback* and *monitor vital signals without taking eyes off the patient*. Different actors share some of these goals. For example, the goal *monitor vital signals without taking eyes off the patient* is shared among the actors *senior nurse*, *telemedicine system* and *community nurse*. Goals can decompose to more specific sub-goals. For example, the senior nurse's high-level goal is to *spend more time interacting with patients while seeing more people in a day*. This goal has sub-goals namely *provide instant feedback via video feed* and *access medical libraries faster and on demand* (cf. Fig 8.33). The organisational model is a hierarchy of goals of the telemedicine system and the actors with those objectives and security constraints. Constructing the organisational model is vital to identify the system's objectives on its own and those that cannot be achieved solely by the system itself.

The next step is to examine each objective and decide if the telemedicine system can achieve the objectives itself or it requires interacting with other actors of the system domain. There are goals that the system itself cannot fulfil unless it interacts with other entities of the system domain, namely *patient*, a *senior nurse* and *community nurse*. We consider the rest of the objectives as objectives that the system can fulfil.

We model the telemedicine system's objectives that the system cannot accomplish by itself as dependencies on other actors. Fig. 8.33 depicts the modelled dependencies using the BINA tool. The identified dependencies are the following:

- The telemedicine system depends on the *senior nurse* to *offer live expert interactive feedback*.
- The telemedicine system depends on the *community nurse* to *provide remote delivery of healthcare services*.
- The telemedicine system depends on the *community nurse* to *monitor vital signals without taking eyes off the patient*.
- The telemedicine system depends on the *patient* to *monitor vital signals*.

The modelled dependencies represent how the telemedicine system can fulfil its objective and be resilient for the stakeholders. However, the organisational model's dependencies represent the designer's assumptions. Hence they require further analysis.

The telemedicine system's modelled dependencies on other system domain entities constitute a potential threat to its resiliency. The system must be resilient, but the system must be secure and resilient as it operates, given the objectives and security constraints. For example, if the patient does not have a secure internet connection, then the telemedicine system will be exposed to threats, and the system is not resilient in terms of its cybersecurity. If the senior nurse uses a non-authorized terminal connected to the hospital's network that complies with the hospital's cybersecurity policies to access the patient's data, the system will be susceptible to attacks. Thus the system is not resilient in terms of users behaviour. If the senior nurse does not record a treatment, the system will not have an accurate treatment record for training purposes. Thus the system is not resilient to staffs' negligence. Implementing the system without investigating these dependencies and identifying ways to remove the uncertainties at this stage will result in a system with the risk of not being resilient.

8.5.2 Activity 2: Incident modelling

The telemedicine system we focus in this case is the use of smart glasses. Such augmented reality-based technology can bring a massive efficiency boost to healthcare processes. Still, their use causes controversies as cybersecurity researchers [230, 231] consider them to yield a high potential to undermine individuals' security and privacy, especially where not correctly cybersecurity resilient-friendly designed. The European Data Protection Supervisor recently issued a report exploring the implications of smart glasses.

We want to build confidence that the telemedicine system will be resilient. For that, we need to find Cyber Incident Response Plans (CIRPs) for the modelled dependencies. Each of the identified dependencies from the previous activity constitutes a potential vulnerability to the system because it is uncertain whether the actors will perform them as expected. To manage uncertainty, we need to search for possible incidents to resolve using CIRPs.

In section 4.4.2 we saw that an *incident* depicts a single or a series of violations or imminent threat/s of violation of security constraints. The constraints in this case study are *reduce attack surfaces*; *secure communication networks* and *monitor vital signals without taking eyes off the patient*. The incidents that violate one or more of these security constraints or present imminent fulfilments of their violation are *unauthorised access to patient's data* and *malicious control of smart glasses*.

Using BINA we take a build-in approach to resilient design and development of smart glasses. For that reason, we identify within this activity, possible Cyber Incident Response Plans (CIRPs) that address the incidents mentioned in the previous paragraph. The suitable CIRPs are many in this case, and some examples are *ban camera features except for services in charge of security and safety* and . We then model how we plan to implement these CIRPs by modelling specific security controls. Some of these controls are *contingency plan - identify critical assets; system monitoring - automated tools and mechanisms for real-time analysis* and *account enforcement - restrict access to specific information types*.

To analyse smart glasses' resiliency for home nursing remote services, we need to identify possible causes of such incidents. We are aware of what occurrences are unwanted given to a telemedicine system's goals. We will examine possible threats that can impact smart glasses, modelled in this activity as incidents and proposing CIRPs and security controls in the following activity. In order to examine in more detail their resiliency, we move to the third activity.

8.5.3 Activity 3: Holistic resiliency modelling

We identify two potential attack vectors for smart glasses. In the first case, the attacker targets either the smart glasses themselves or their components (e.g., battery). This type of compromise will require knowledge of the internal functionality of the smart glasses. In the second case, the attacker targets the communication networks. The community nurse that uses the smart glasses connects them to the patient's house WiFi and broadcast live video of image and sound. The nurse can also use the glasses to record and save video images. A senior nurse located in a hospital receives the video through a terminal using an app such as Zoom, Webex, Skype for Business. The hospital's cybersecurity services cover this part of the communication. However, the community nurse visits many patients during a day and connects the smart glasses to different WiFi's at each patient's house. This use of smart glasses exposes them to threats.

If an attacker aims to obstruct the use of the smart glasses or to harm the community nurse, then he/she/they can interfere with the thermal network of the smart glasses. These malicious objectives can be seen in Fig. 8.35 as the attacker's goals *make the use uncomfortable* and *impact the physical health safety of the user*. An attacker that targets the smart glasses can aim to make the glasses faulty. In other words, to render the machine learning models/methods of the smart glasses ineffective. Fig. 8.35 models this objective as *make classifier fail*. During the face detection process, the attacker finds a method/transformation of a face in an image/photo, so the face detection method does not detect the patient's face. The *attacker* can threaten the smart glasses resiliency by interfering with their hardware as their thermal network or use machine learning attacks. S/he/they can do so by exploiting vulnerabilities like access and interference with physical components and materials of smart glasses and *malicious use of Light Emitting Diodes (LEDs)*.

If an attacker aims to obtain data from the smart glasses, then s/he/they can target the communication between the smart glasses and the hospital's terminal. The attacker will have the goal *obtain the imputed numerical passwords on touch-enabled mobile devices* as modelled in Fig. 8.35. For that s/he/they can exploit that the vulnerability *patients do not perceive smart glasses can threaten their privacy and data protection*. If this is a patient's mindset, it can lead to the vulnerability *mobile device's screen in the view of smart glasses camera*. In this way, the attacker can threaten the telemedicine system's communication network with a *vision based side-channel attack*. The attacker can also exploit the *limited physical security* in a patient's house WiFi and acquire unauthorised access to data recorder at his/her/their house.

From a security perspective, smart glasses have to operate for the provision of healthcare services. The main objectives of the smart glasses as a telemedicine system in this scenario are *provide remote delivery of healthcare services; offer live expert interactive medical feedback and monitor vital signals without taking eyes off the patient* (cf. Fig. 8.35). Security constraints restrict these goals. For example, *assume compromised resources* restrict the objective *monitor vital signals without taking eyes off the patient*. This security constraint means that an attacker can compromise the system and its components for extended periods without being detected. Some compromises may never be detected. The system must remain capable of meeting performance and quality requirements, nonetheless. This constraint for cybersecurity means that hierarchical protection is not suitable for smart glasses. For resiliency, this means the need for localised capacity and loose coupling.

In this activity so far, we have been updating and reviewing the telemedicine system's existing model. Doing so is very important because when mounting an attack against smart glasses, an adversary may exploit a specific system property and disrupt an ongoing procedure by invalidating any of these security constraints.

For each of the analysed classes of threats, we seek to model an informed understanding of risks, events, incidents and vulnerabilities. For example, the threat *interference with thermal network* relates to the incidents *malicious control of smart glasses*. We can observe such incidents as events. For example, the incidents modelled in Fig 8.35 in practice will manifest as the events *issues of mass-market product security; highly identifiable information exchanged during live broadcast* and *modify face detection algorithm*. These events, if present associate with the incidents that potentially can impact the smart glasses system.

In the case of *interference with thermal network*, the attacker poses the risk of acquiring information that can use to *increase smart glasses temperature*. As a result, the event *issues of mass-market product security issues* occurs. The known vulnerabilities can lead to the *malicious control of smart glasses*. For the threat *adversarial machine learning attacks*, the relevant risks are *image-level distortions* and *face-level distortions*. These risks relate to the occurrence of the event *modify face detection algorithm*. The threat *vision based side-channel attack* poses the risk of *the patient may inadvertently be identified/recognised by the smart glasses*. This risk will be present if the event *highly identifiable information exchanged during live broadcast* holds.

This way of constructing the model allows the designer to identify resiliency objectives for the telemedical system under study. The security engineer extracts such goals not from the stakeholders directly but through the design of resiliency constructs. Firstly, security controls express the stakeholders' priorities. The security engineer identifies through stakeholders' meetings and interviews the threat scenarios that the smart glasses as a telemedicine system need to be resilient. Then the security engineer models particular ways to allow the system to operate even in the presence of incidents. The security engineer can now identify ways to make the *smart glasses* telemedicine system resilient. For that purpose, we analyse the CIRPs modelled and, using the BINA tool extract metrics that will enhance the design.

According to the BINA process, we have three automations that result from three functions. We will demonstrate them using the BINA tool. The user has given the following input to the CIRP properties:

- (1) The first function is for the property 'dependence level' (D) of the CIRP node.

$$D = \frac{\text{validCIRPs}}{\text{totalCIRPs}} \times \text{reliance level}$$

The BINA tool counts the valid CIRPs that have ticked the box for the property 'risk reduction'.

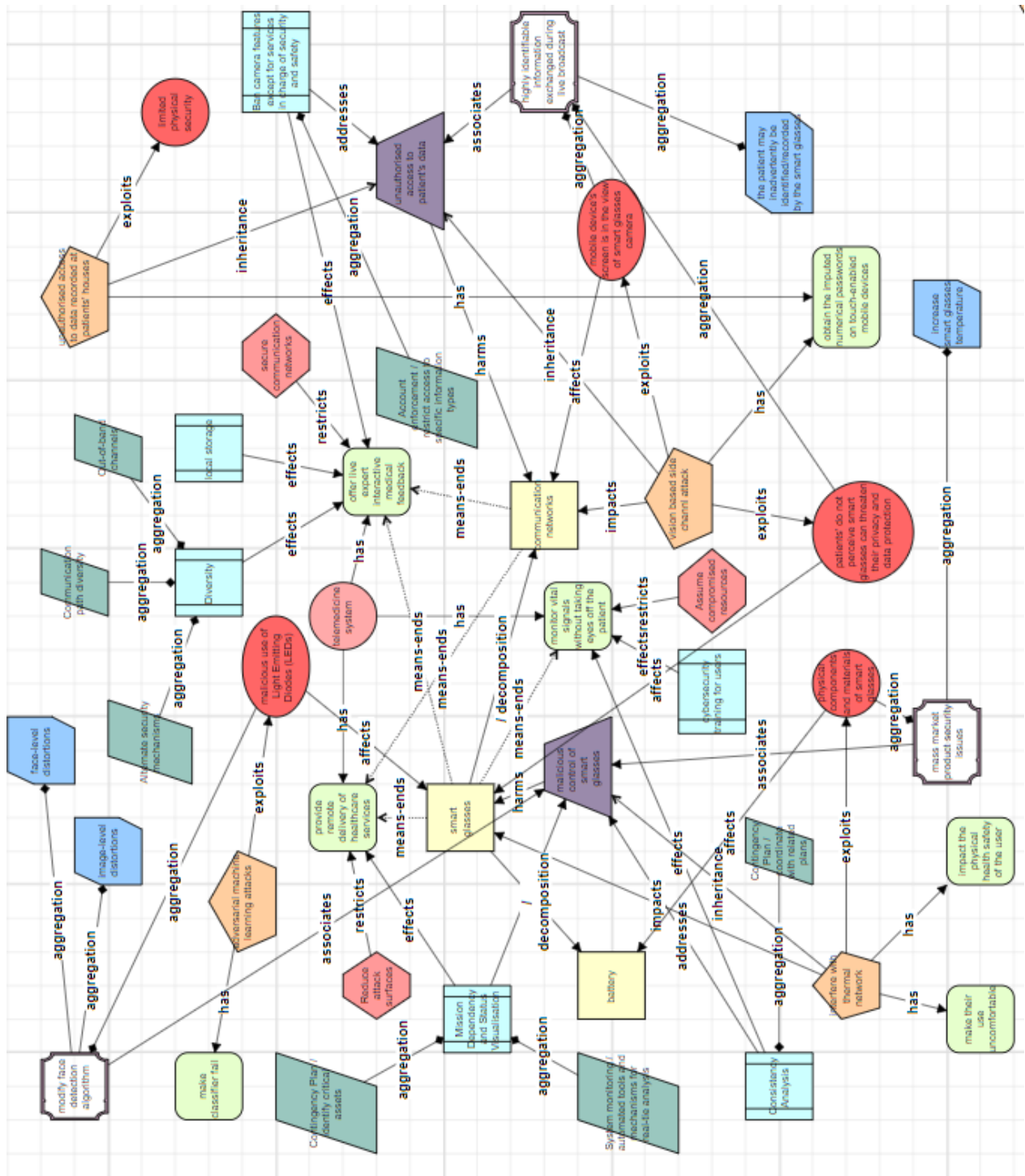


Figure 8.35: Partial holistic resilience model for smart glasses.

It also counts the total CIRPs with ticked boxes for the property 'risk reduction'. The property 'reliance level' is for each of the CIRPs, either ticked as one or unticked as zero. Consequently, the tool at the end of the design process of the user it auto-generates the value of the property 'reliance level' the CIRPs as the following examples show:

For the CIRP *Local storage*:

$$D = \frac{(\text{validCIRPs} = 4)}{(\text{totalCIRPs} = 6)} \times (\text{reliance level} = 1) = 0.66 \times 1 = 0.66$$

For the CIRP *Diversity*

$$D = \frac{(validCIRPs = 4)}{(totalCIRPs = 6)} \times (reliance\ level=0) = 0.66 \times 0 = 0$$

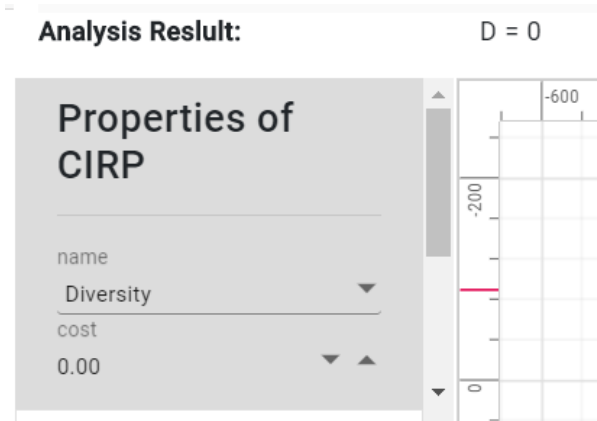


Figure 8.36: Dependency level (D) as generated from the BINA tool for the CIRP 'Diversity'.



Figure 8.37: Property section for CIRPs in BINA tool.

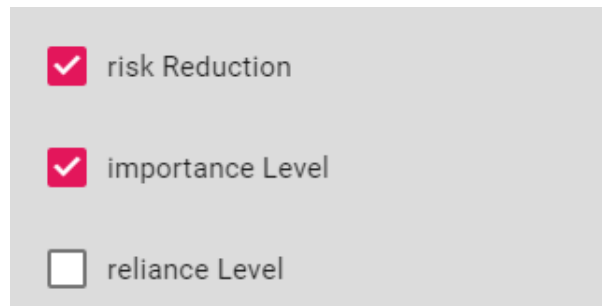


Figure 8.38: Properties of the CIRP 'Diversity' in BINA tool.



Figure 8.39: Property section for CIRPs in BINA tool.

(2) The second automation is for the property 'system resiliency' (SR).

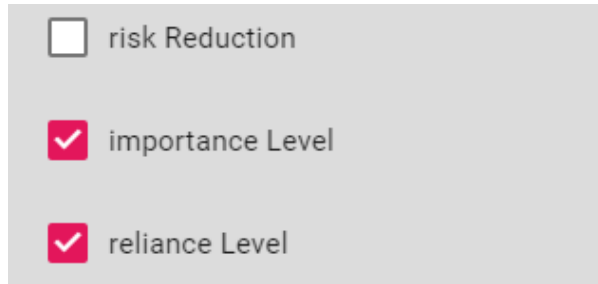


Figure 8.40: Properties of the CIRP 'local storage' in BINA tool.

$$SR = \left(\frac{\sum_{x=1}^n I_x \times R_x}{\sum_{x=1}^n I_x} \right) \times 100$$

The I stands for the importance level of CIRPs. The R stands for the reliance level of CIRPs. Following the values of our example, the SR is calculated as:

$$SR = \left(\frac{\sum_{x=1}^6 I_x \times R_x}{\sum_{x=1}^6 I_x} \right) \times 100$$

$$SR = \left(\frac{(1 \times 0) + (1 \times 1) + (1 \times 1) + (1 \times 0) + (1 \times 1) + (1 \times 0)}{(1 + 1 + 1 + 1 + 1 + 1)} \right) \times 100$$

$$SR = \left(\frac{3}{6} \right) \times 100$$

$$SR = 0.5 \times 100$$

$$SR = 50\%$$

The SR is automatically calculated from the BINA tool after the designer models the suitable CIRPs as it can be seen in Fig 8.41. Note that in the tool the result of the system resiliency (SR) appears as the Greek character sigma Σ .

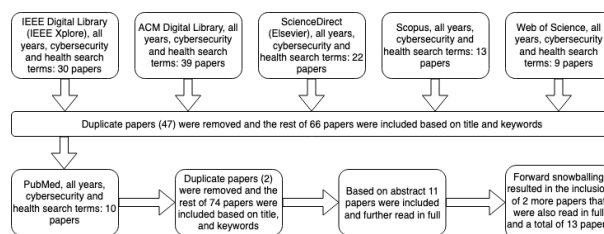


Figure 8.41: System Resiliency as generated from the BINA tool.

(3) The third automation is for the property 'risk level' of the node 'risk'

This property derives from the function:

$$\text{risk level} = f(\text{potentiality} \times \text{impact level})$$

The values of the properties 'potentiality' and 'risk level' came from the nodes 'incident' and 'event' respectively.

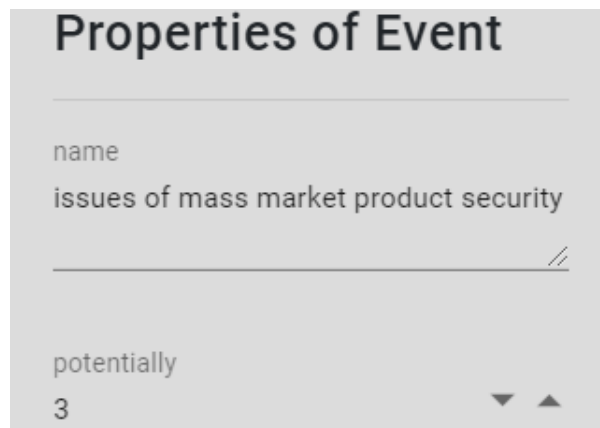


Figure 8.42: Properties of the construct 'Event'.

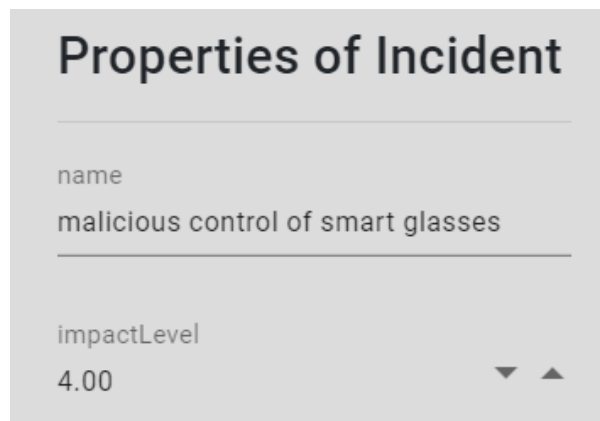


Figure 8.43: Properties of the construct 'Incident'.

In this example, that means that the 'risk level' property of 'risk' will automatically be calculated from the tool as follows:

For the risk *increase smart glasses temperature* we take the nodes 'incident', and 'event' that connect with this risk (cf. Fig. 8.35) and their properties (cf. Fig. 8.42 and Fig. 8.43) and use them for the 'risk level' function, which will become:

$$\text{risk level} = f(\text{potentiality} \times \text{impact level})$$

$$\text{risk level} = 3 \times 4$$

$$\text{risk level} = 12$$

This automation will complete the 'risk' property 'risk level' as shown in Fig 8.44.

The designer, based on the above, considers the existing system's resiliency, the dependence level and the risk level of the risks modelled. The designer assesses if s/he/they need to make adjustments to the existing incident model. Such considerations originate from a system's expected resiliency, the modelled dependencies that were not resolved and constituted a potential vulnerability to the smart glasses telemedicine system's resiliency, and the expected risk level of the modelled risks. Because the designer cannot be confident that the system



Figure 8.44: Properties of the construct 'Risk'.

will fulfil resiliency requirements given dependencies and risks once it is operational. Hence, the designer needs to identify new solutions to feel confident in the resiliency requirements' and dependencies' fulfilment. For the designer to come with new solutions, a more detailed analysis of the existing model needs to occur, which takes place in the next activity.

8.5.4 Activity 4: Resiliency analysis

Using the BINA tool, the designer can firstly validate the correctness of the model created based on the metamodel. This analysis happens automatically when the user presses the 'Check' in the BINA tool. After the designed model's correctness assessment takes place from the tool and the designer, further analysis can take place that can raise several critical implementational issues.

System resiliency before and after the resiliency analysis: Firstly, at any stage, the BINA tool automatically assessed the smart glasses system's resiliency. Before the resiliency analysis, the system's resiliency was at 50% (cf. Fig 8.41). When the analysis progressed and the designer addressed the relevant issues by adding resiliency requirements, the smart glasses' resiliency became 78.57143% (cf. Fig. 8.45).

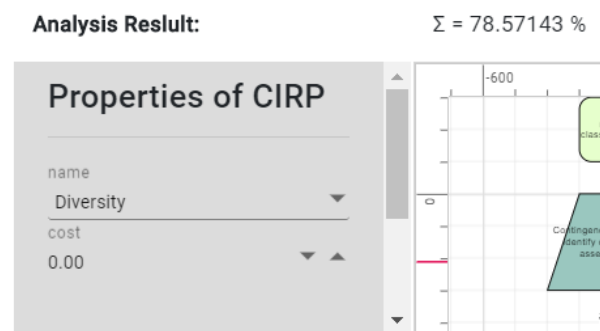


Figure 8.45: Smart glasses system resiliency after the resiliency analysis.

Potential interactions between CIRPs: The designer firstly chooses and models new objectives specific to resiliency planning. Based on the newly modelled resiliency objectives, the designer identifies and introduces four new CIRPs. The smart glasses system (modelled as a telemedicine system) needs to *prepare* for cyber-physical incidents. The CIRP *redundancy* implements this objective, and the objective *continue* the operation of critical healthcare processes,

conducted through the use of the smart glasses system. The CIRP *substantiated integrity* also implements this latter objective, and the objective *understand* the incident and the adversary. The CIRP *analytic monitoring* implements the objective *understand* and the objective *continue*. These two objectives have been already though covered from the CIRPs *substantiated integrity* and *redundancy* (cf. Fig. 8.46). The designer will need further to analyse the interactions among the newly modelled CIRPs. Finally, the designer introduces the CIRP *non-persistence* that implements the objective *re-architect* system architectures to handle adversity and address environmental changes more effectively.

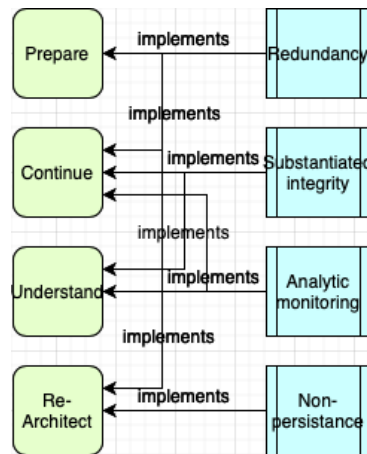


Figure 8.46: High-level CIRPs implementing smart glasses system objectives.

The introduced CIRPs can support (S), depend (D), use (U) and conflict or complicate (C) each others implementation. The relations among CIRPs are following the cyber resiliency techniques presented in NIST SP 800-160v2 [10]. Fig. 8.47 depicts an example of this type of analysis for a smart glasses system. For example, *non-persistence* **conflicts/complicates** the CIRP *analytic monitoring* whereas *substantiated integrity* **supports/uses** the CIRP *analytic monitoring*. Based on these relations, the designer can make informed decisions about which CIRPs are implementable to this particular system s/he/they analyse (cf. Fig 8.47).

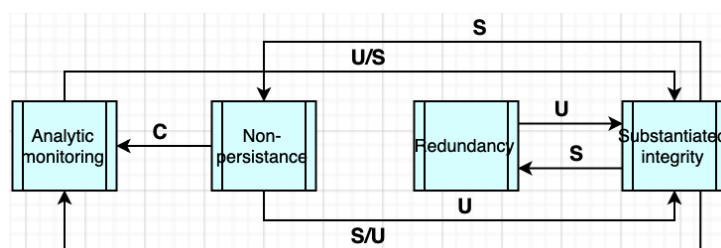


Figure 8.47: Potential interactions between smart glasses system CIRPs.

Moreover, if the designer has CIRPs from the NIST SP 800-160v2 [10] list, this type of analysis can extend. Fig. 8.48 shows the four new CIRPs and their relation to the already modelled (old) CIRP *diversity*. *Diversity* does not impact the CIRP *non-persistence* and vice versa. *Diversity* **conflicts/complicates** or **supports** the implementation of the CIRP *analytic monitoring*. This means that *diversity* if implemented could undermine the effectiveness of the CIRP *analytic monitoring*. Alternatively, in the case of **supports**, *diversity* can make the CIRP *analytic monitoring* more effective. This depends on the more specific implementation of CIRPs. Ana-

lytic monitoring uses diversity. Meaning that *analytic monitoring* can be implemented effectively in the absence of *diversity*; however, more options become available if *diversity* is also used. Similarly *diversity uses substantiated integrity* and *redundancy uses diversity*. Furthermore, *diversity supports redundancy* and *substantiated integrity supports diversity*.

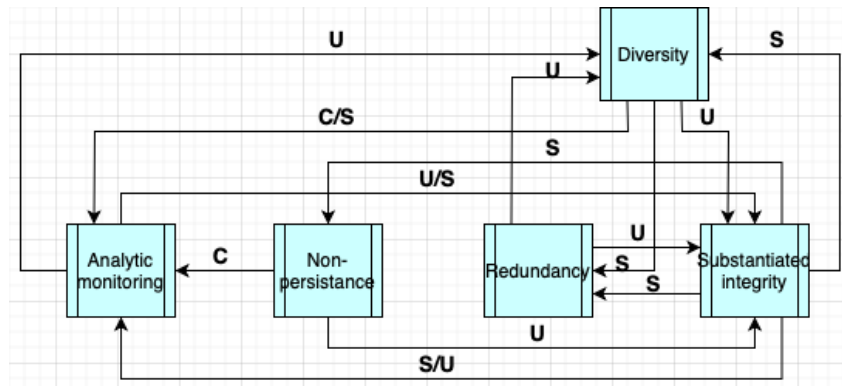


Figure 8.48: Potential interactions between new and old smart glasses system CIRPs.

Assessment of the implementation of objectives using the selected by the designer CIRPs: CIRPs can also be analysed in relation to the *security objectives* that they *implement*. Objectives motivate the definition of security requirements and the selection and tailoring of CIRP. For example, the objective *prepare* implies that a CIRP needs to support and maintain a set of appropriate courses of action that thwart adversity. The objective *continue* indicates that a CIRP is needed to extend the duration and reliability of a medical procedure in the presence of a threat. The objective *understand* expresses the need for a CIRP that offers situational awareness of the resources necessary for a medical procedure under siege. Finally, the objective *re-architect* signifies the need to modify architectures to handle adversity and address more effectively potential impacts on the system's environment.

Consequently, a designer can use objectives as a starting point for eliciting restatements of objectives and analysing how CIRPs meet these objectives or not. Using the objectives suggested in NIST SP 800-160v2 [10] and focusing on the smart glasses system, the designer, through the BINA tool, derives the relations shown in Fig. 8.49. The designer can see in that way that some CIRPs implement the same objectives, such as the CIRPs *protected buck up and restore* and *behaviour validation* implement the objective *prepare*. Based on this information and a limited security budget, the designer might choose to remove one of the CIRPs that meet the same objectives. For example, the designer can select between the CIRPs *behaviour validation* and *monitoring and damage assessment* as they both achieve the objectives *continue* and *understand*. Further, the designer can tailor these high-level cyber resiliency objectives to reflect the system's missions and processes. For example, in the smart glasses system, the *continue* objective can be tailored to enable the patient or healthcare provider to engage fail-safe mechanisms.

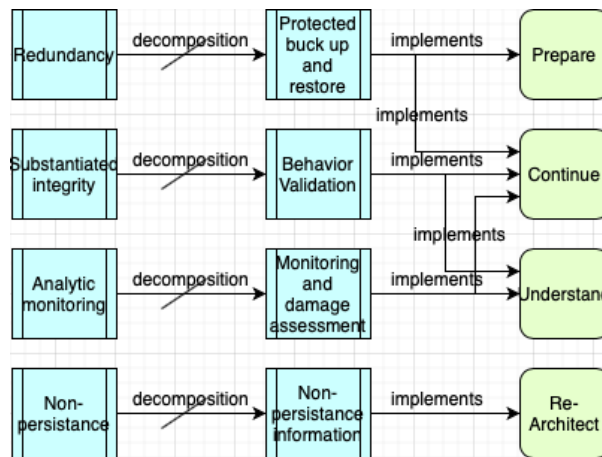


Figure 8.49: CIRPs implementing smart glasses system objectives.

Analysis of CIRPs effects on malicious objectives: The designer wants to effect malicious objectives that an adversary can have. S/he/they can do so by incorporating CIRPs as part of the model. Using the BINA tool, these *effect* relationships became more specific as shown in Fig. 8.50. Assuming that the adversary does not have prior knowledge of the system-to-be, a set of objectives can be selected from the designer and modelled using the BINA tool. Then the tool analyses these relationships and characterises them. For example, the CIRP *behaviour validation* **detects** the adversarial objectives *exploitation; privilege escalation; persistence* and *deny*. Other CIRPs effect the same objectives in different ways. For example, the CIRP *Non-persistence information* **preempts/exerts** the objective *privilege escalation*.

Note also that this analysis identifies the potential effects of the implementation approaches based on NIST SP 800-160v2 [10]. It does not and cannot assess how strongly an adversary will experience a CIRP's implementation. Also, this analysis identifies an effect on an adversary objective if it applies to at least one adversary action under that objective; it does not consider the number of possible actions under each objective. For a more detailed analysis, one could use scores that will need to be specific to the system's type and the organisation that the designer implements the CIRPs. Some effects are beyond what can be designed and implemented in a technical system from a resiliency perspective. For example, detection of adversary might involve non-cyber actions like intelligence gathering and analysis beyond the scope of cyber resiliency. This type of analysis does not cover these cases as the focus of this project is cyber resiliency.

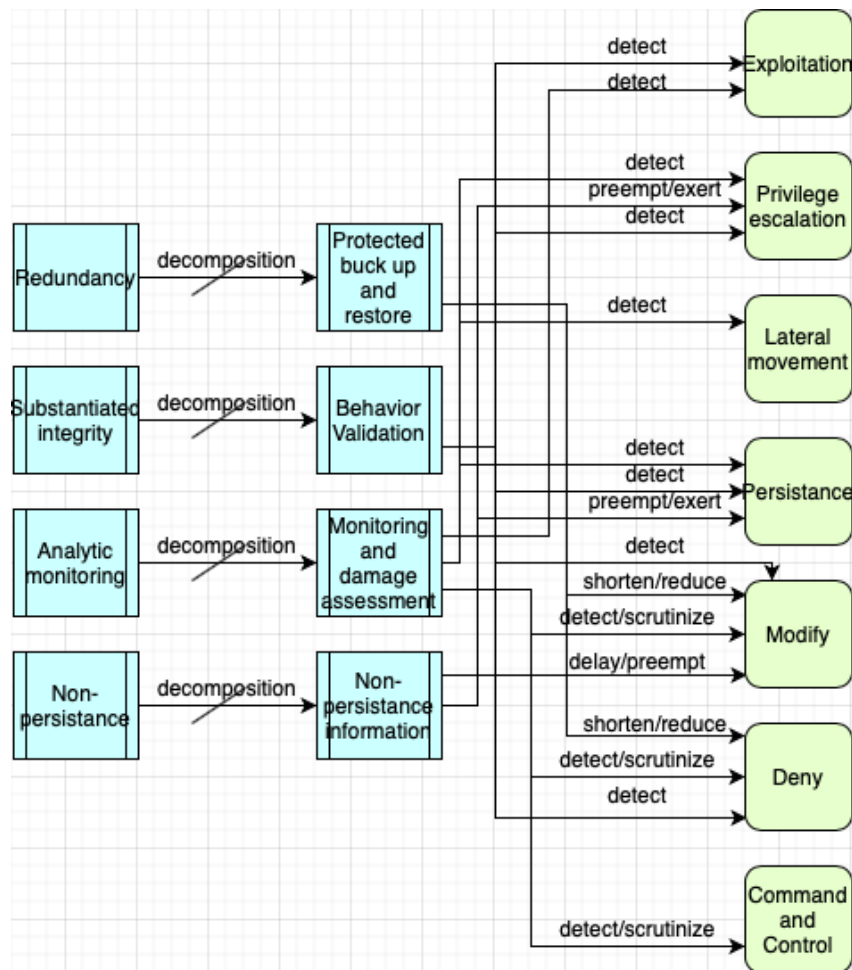


Figure 8.50: Analysis of the CIRPs effects on malicious objectives against the smart glasses system.

Examination of coverage of structural security constraints with the implementation of CIRPs: Based on NIST SP 800-160v2 [10] CIRPs implement structural security constraints. Structural security constraints guide and inform the design and implementation decisions throughout the smart glasses system life cycle. Many of the structural design principles are consistent with or leverage the CIRPs. If CIRPs are not sufficient, the designer will need to add more, or if the model has redundant CIRPs, the designer will need to remove them. The BINA tool facilitates this type of analysis, offering the capability to define structural security constraints and examine the coverage of the CIRPs that the designer has modelled initially. Fig. 8.51 shows that the modelled CIRPs implement structural security constraints. However, more than one CIRPs implement the same structural security constraint in some cases. For example, the CIRPs *substantiated integrity*; *analytic monitoring* and *non-persistence* **implement** the structural security constraint *contain and exclude behaviours*. Also, one CIRPs can implement more than one structural security constraints. For example, the CIRP *redundancy* **implements** the structural security constraints *plan and manage diversity*; *maintain redundancy* and *manage resources (risk) adaptively*. The designer can use this information to choose among CIRPs the most suitable ones for the smart glasses system as modelled. Hence, in this case, the designer might choose to implement only two of them, namely the *redundancy* and the *substantiated integrity*.

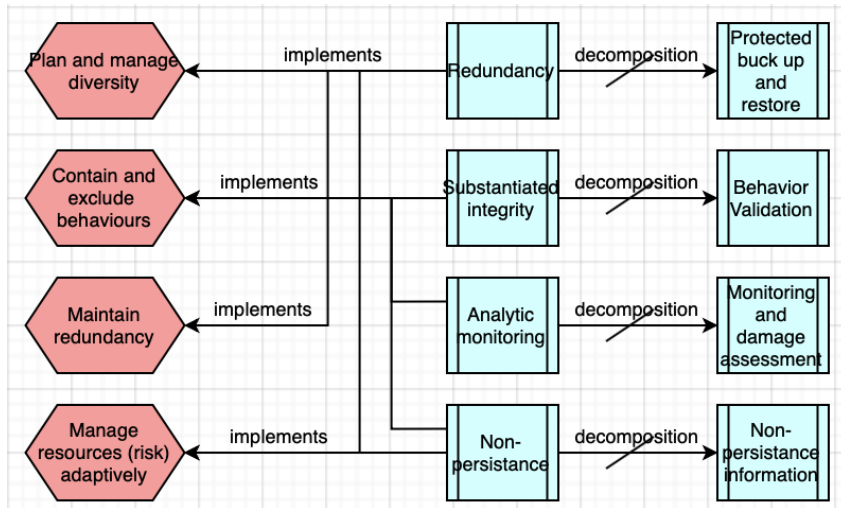


Figure 8.51: Structural security constraints implementation through CIRPs for the smart glasses system.

Assessment of CIRPs specification with security controls: The designer can also analyse using the BINA tool the implementational aspect of the modelled CIRPs. CIRPs aggregate security controls. The designer can identify gaps in their analysis or redundant security controls using the BINA tool. For instance, in Fig. 8.52, the designer can see that they have for the CIRP *non-persistence information* two security controls, namely *boundary protection | prevent exfiltration* and *non-modifiable executable programs | no writable storage*. As the security control *non-modifiable executable programs | no writable storage* do not aggregate to any other CIRP; the designer can consider it redundant and remove it from the model. The updated model will steel meet the CIRPs required to maintain the smart glasses system’s objectives.

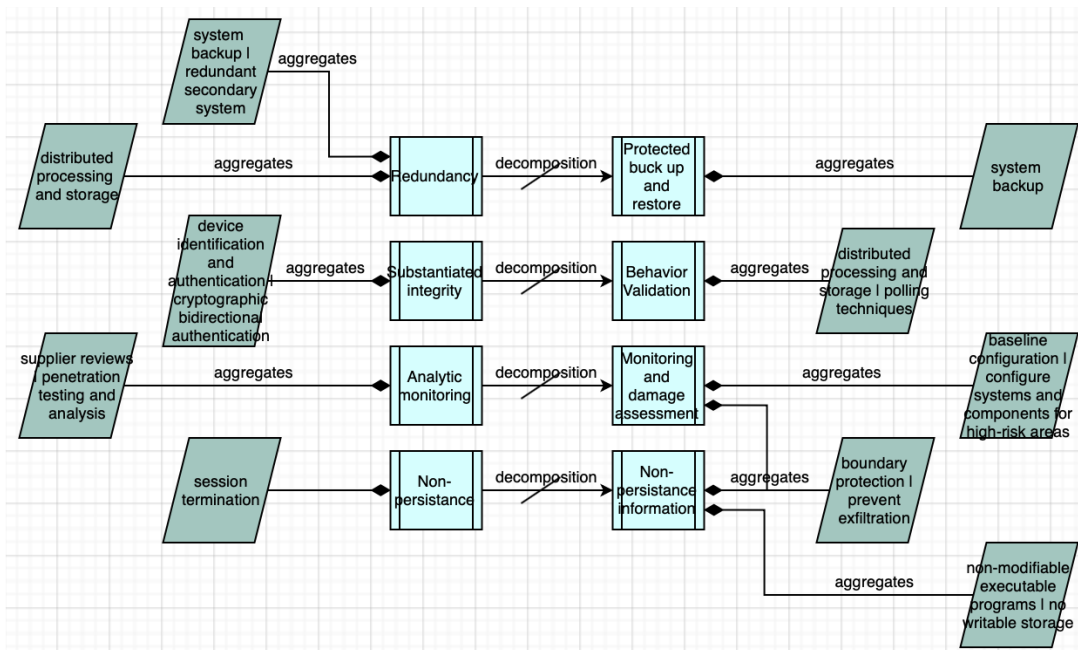


Figure 8.52: Smart glasses system security controls that aggregate to CIRPs.

Examination of the restrictions that strategic security constraints restrict objectives: Strategic security constraints guide and inform security and resiliency analyses throughout the system life cycle and highlight different cyber resiliency techniques and approaches to apply them. *Strategic security constraints* restrict *objectives*. Security constraints indicate the type of incidents and risks the designer incorporate in their plan. One way to express priorities for cyber resiliency is through objectives. Each strategic security constraint supports the achievement of one or more cyber resiliency objectives. The BINA tool allows the designer to assess if the restrictions that strategic security constraints impose on objectives express the resiliency priorities modelled. For example, in Fig. 8.53, a designer can see through the BINA tool automation that all the strategic security constraints restrict more than one objectives. For example, the strategic security constraint *assume compromised resources* restricts all four of the objectives. Due to limitations in smart glasses design and resource availability, the designer might remove the other constraints as redundant for the smart glasses resiliency model.

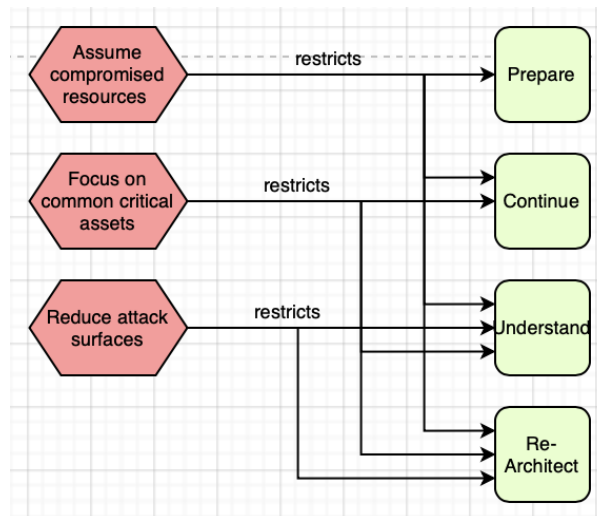


Figure 8.53: Strategic security constraints that restrict smart glasses system's objectives.

Analysis of compatibility between strategic and security objectives: Strategic objectives drive the selection of structural objectives. The designer can use the decomposition relation to show how strategic objectives link with structural objectives through the BINA tool. A designer can use the tool to examine if they can justify the structural objectives they have modelled by the strategic objectives or if they need to amend them. For example, in Fig. 8.54, not all the strategic objectives decompose to the modelled structural objectives. Consequently, the designer can choose to remove the strategic objective *reduce attack surfaces*. Noticeable is that the strategic objective *focus on common critical assets* decomposes to all five of the structural objectives, namely *plan and manage diversity; contain and exclude behaviours, maintain redundancy and manage resources (risk) adaptively*.

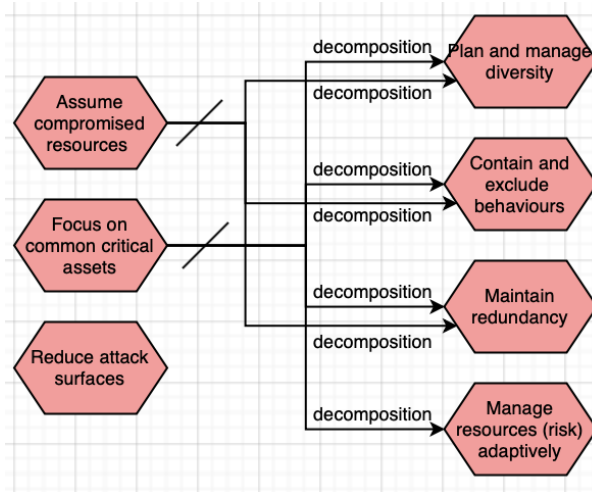


Figure 8.54: Decomposition of strategic constraints to structural constraints for the smart glasses system.

Coverage examination of threats and correspondent objectives:

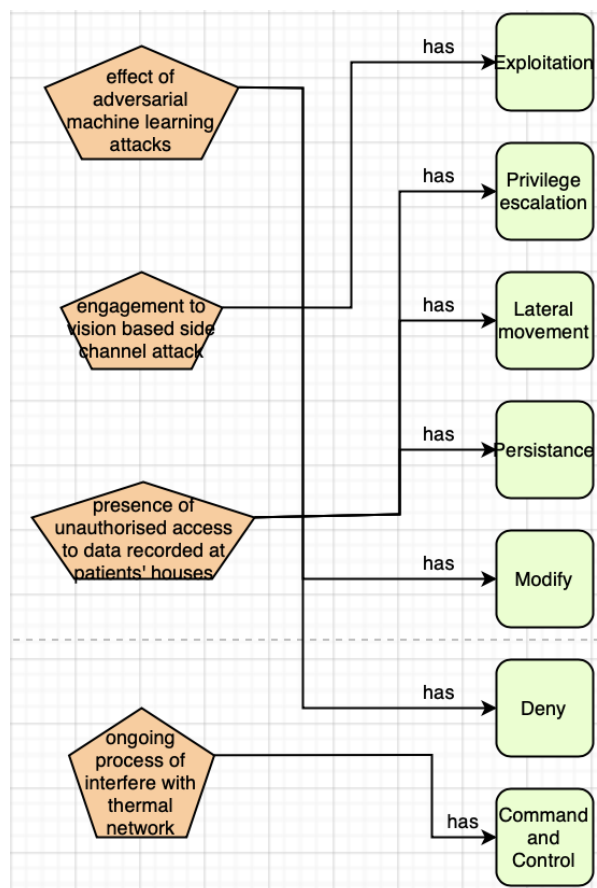


Figure 8.55: Threats and malicious objectives against the smart glasses system.

The modelled threats have objectives that the designer might choose to examine further. Threats have objectives. A designer wants to ensure that the threats modelled correspond

to adversarial objectives that need they have chosen to manage for the specific system-to-be. Fig. 8.55 shows four of the threats, namely *effect of adversarial machine learning attacks*; *engagement to vision-based side-channel attacks*; *the presence of unauthorised access to data recorded at patients' houses* and *ongoing process of interference with thermal network* and their corresponding objectives. In this example, all objectives have a corresponding threat. That means that the designer does not need to introduce more threats in the model to analyse the attacker's profile of their choice. This automation gives them a clear indication of when to finish their analysis and justify that decision.

8.6 Discussion and Closing Remarks

In this chapter, we used two case studies to test the applicability and observe the benefits of the BINA methodology on a single healthcare system. We used case studies representative of medical systems (BCI) that operate within healthcare environments and medical systems (TRS) that are operated remotely and even in hostile environments. Our objective was to increase the practitioner's ability to understand and capture cyber resiliency relationships during information systems development. We demonstrated that theoretically by applying the BINA framework to two representative case studies.

We used the BINA tool to analyse and understand its use to explore cyber resiliency factors influencing the cyber resiliency of a telemedicine system that uses smart glasses to offer remote diagnostic services. We used a real case study to apply the BINA methodology and see how it can be used for a system under development. We captured a range of perspectives using this case study, which gave us a greater understanding of the subject and reduced the potential for any bias as we represented what was relevant to the case rather than suitable for the methodology.

Chapter 9

Evaluation of BINA methodology by interviews and a survey research

An essential category of the empirical study is that of the survey. The participants are individuals that use specific methods and tools on projects. In this case, they are asked to provide information about the method and tool [200]. Then the information collected from the survey is analysed using standard statistical techniques. We adopted the survey method as a way to evaluate our BINA methodology further and confirm, strengthen, and further generalise our research claims about the efficacy and usefulness of our methodology.

All the survey phases were conducted online. Expert individuals, including practitioners and industry researchers, performed a trial of our proposed methodology using a simulated case study, and then they answered the online questionnaires after an evaluation has been completed. Throughout this thesis, we will use the term "user" for those expert individuals as they were the users of the methodology. The evaluation study was both a quantitative and qualitative survey. On the one hand, it was quantitative because it was an inquiry of the number of researchers that they agreed with the statements presented to them.

Moreover, it was qualitative because there was a feature-based evaluation carried out by users who had studied and had the experience of the methodology. Users assessed the extent to which the methodology and the tool provide the required features in an as usable and effective manner based on personal opinion. Fig. 9.1 depicts the survey approach.

The survey aims to produce evidence to assess our claims and propositions as generated from the data of the previous evaluation through the case study. In particular, to collect enough data from a sufficient number of users, all adhering to the same methodology, in order to obtain a statistically significant result on the attribute of concern compared to some other treatment, i.e. the methodologies that users were using at their institution.

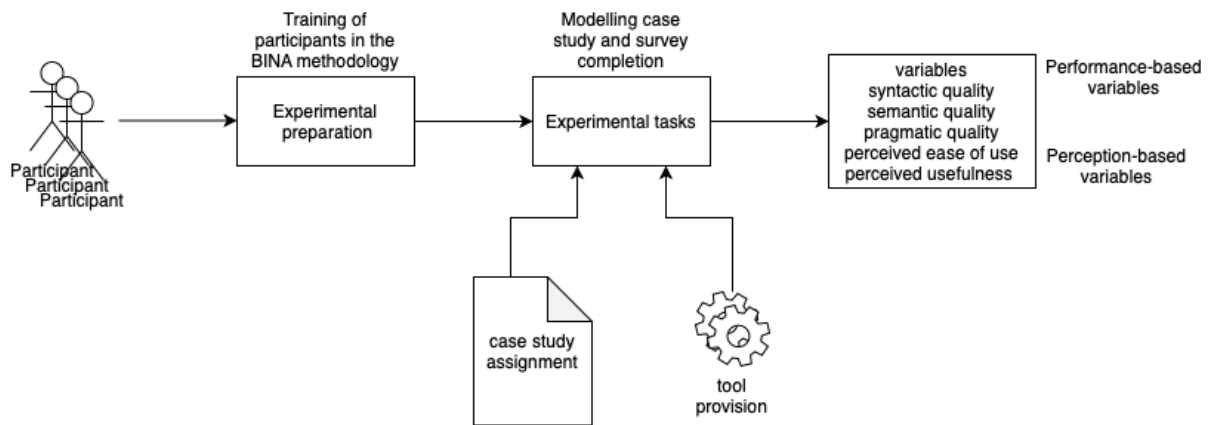


Figure 9.1: survey approach.

9.1 Survey design

9.1.1 Survey objectives

The survey objectives are to answer the research questions of the evaluation chapter 8. Therefore, we set the following research objectives to address the research questions of the evaluation study, that they use perception-based measures and performance-based measures.

- Measure to what extent the methodology enables the user to model and reason about resiliency relationships during information systems development (perceived efficacy).
- Measure to what extent the methodology enables the user to model and analyse resiliency requirements during information systems development (perceived efficacy).
- Measure to what extent the methodology enables the user to assess system resiliency at a requirements level (perceived efficacy).
- Measure the ease of use of the methodology (perceived efficiency).
- Measure the actual effectiveness of the methodology by evaluating how well the participants perform the evaluation exercise. The evaluation will be in terms of the validity and completeness of the developed models.

9.1.2 Subjects

To evaluate our methodology, we organised online sessions. The participants had experience or understanding in software development, cybersecurity and/or virtual learning environments. The participants were asked to apply our methodology on a COVID-19 vaccine supply chain threat scenario. The specific participants were selected based on judgemental and convenience sampling, because of their research speciality, which can bring more accurate results, and because of the ease of recruiting them, their accessibility to us, and the availability of limited resources. The users who participated in the sessions had already experience with software development methodologies, and especially the ones from the academic institutions were familiar with virtual learning environments.

In total, five users voluntarily took part in the online session. Two were from a technology company in Greece, one from a healthcare provider in the UK, one from a US medical devices producer company, and one from Swiss company that offers medical devices documentation management. The users were industry researchers. All five users had more than fifteen years of experience in software engineering and/or information security. Also, three users were experienced in security engineering, while two had experience in healthcare cybersecurity and resiliency. Four users were familiar with UML, while two users were also familiar with Secure Tropos modelling language.

9.1.3 Ethics approval

We followed the European Code of Conduct for Research Integrity [232]. Subjects were informed fully about the purpose, methods, and intended possible uses of the research and their participation in the research. Also, the subjects voluntarily participated in the research study and provided their consent. Also, the confidentiality of any sensitive information supplied by subjects and their anonymity was respected and preserved.

9.1.4 Tools

The participants used their laptops to download and run the BINA tool. We provided them with a link that included the most recent version of the BINA tool for the Microsoft Windows operating system.

9.1.5 Training

Since BINA is a new methodology, and the users were not familiar with it, we presented them with a forty-five-minute introduction of the BINA methodology was carried out in order to provide training to the users. The presentation did not include any general information regarding resiliency in software engineering but focused on the methodology. It explained the methodology's goal, its concepts, the process, and the calculations regarding the resolution levels of a dependency and the system trustworthiness. At the end of the presentation users' questions were answered. After that, we described the scenario on which the users applied the BINA methodology.

The scenario was based on the IBM's report about a malicious campaign that started in September 2020 [233]. The attack was described as phishing emails that were sent out across countries, which targeted organisations linked to the Cold Chain Equipment Optimisation Platform (CCEOP) of Gavi, the international vaccine alliance. It involves organisations (e.g., the World Health Organization, Unicef, the World Bank and the Bill & Melinda Gates Foundation) that help distribute vaccines worldwide to some of the poorest regions. This vaccine distribution chain sometimes requires a "cold chain".

A "cold chain" for the PfizerBioNTech vaccine must be kept at a temperature of about -70C during the transition. The vaccines are sent in special ice packs and can be stored in a freezer farm for up to six months. The unopened dry ice packs with the vaccine have ten days to reach the vaccination centre. Once delivered, the vaccine can be stored to up to five days in a fridge between 2°C and 8°C [234].

The attackers impersonated a business executive from a legitimate Chinese company involved in CCEOP's supply cold chain to make it more likely the targets would engage with

the email. They then sent phishing emails to organisations that provided transportation, which contained malicious code and asked for people's login credentials. That could have allowed them to understand the infrastructure that governments intended to use to distribute vaccines.

9.1.6 Tasks

We gave the scenario to the participants and asked them to carry out a resiliency analysis of the system of the scenario performing the following tasks:

- Model cybersecurity relationships and identify the underlying resiliency assumptions about them;
- Identify and model resiliency requirements;
- Assess the system's resiliency at a requirements level.

The users had to construct the respective BINA models, and the duration for the completion of the task was one hour. Moreover, specific aspects of the "cold chain" for the PfizerBioNTech vaccine were given to the users as the focus is on resiliency analysis. We wanted to identify if the users of the BINA tool, could carry out the following activities:

- Model the "cold chain" for the PfizerBioNTech vaccine decomposing it into system components;
- Model possible incidents and resiliency plans;
- Model specific threat scenarios that can cause the predetermined incidents;
- Analyse the system's resiliency
- Adjust their resiliency plan to be implementable and satisfactory for their goals.

9.1.7 Data collection methods

In this study, the unit of analysis was the individual user. We used a questionnaire to collect data, as shown in Fig. 9.2. After completing the tasks, we asked the users to complete the questionnaire. The questionnaire collected both quantitative (close questions) and qualitative data (open-ended questions). The questionnaire contained twelve (12) questions, categorised as related to:

- User's profile;
- Modelling language;
- Process;
- BINA tool;
- Open recommendations.

We used an online questionnaire to carry out the survey employing the Microsoft Forms service. Consequently, we collected and stored online data automatically.

We also collected data through observation of the users while they were carrying out the requested tasks. We did that through Microsoft Teams and Skype meetings. During the observation process, we focused on how much time the users spend on each task, the questions they asked, and the comments they made verbally. We recorded the gathered data from the observations as field notes, that began during the actual observation. We wrote what is necessary and fill in the details later after the end of the online meeting.

9.1.8 Data analysis methods

To analyse the survey data, we tabulated them and then identified patterns in the tables. Then we evaluated the different aspects of the BINA methodology based on the survey data and using two types of measures:

- **Performance-based measures:** they focus on how well the users perform the task. To evaluate the user’s task performance, we used three measures, i.e. syntactic quality, semantic quality and pragmatic quality. Syntactic quality is the degree of accuracy and completeness with which the users applied the methodology. Semantic quality is the degree of correctness with which the users applied the methodology. Pragmatic quality is the degree of the usefulness and fitful purpose with which the users applied the methodology.
- **Perception-based measures:** they focus on the users’ perceptions of usefulness and easiness of the methodology. Perceived usefulness is the degree to which the user thinks that the methodology effectively achieves its objectives. Perceived ease of use is the degree to which the user considers that the methodology is free of effort.

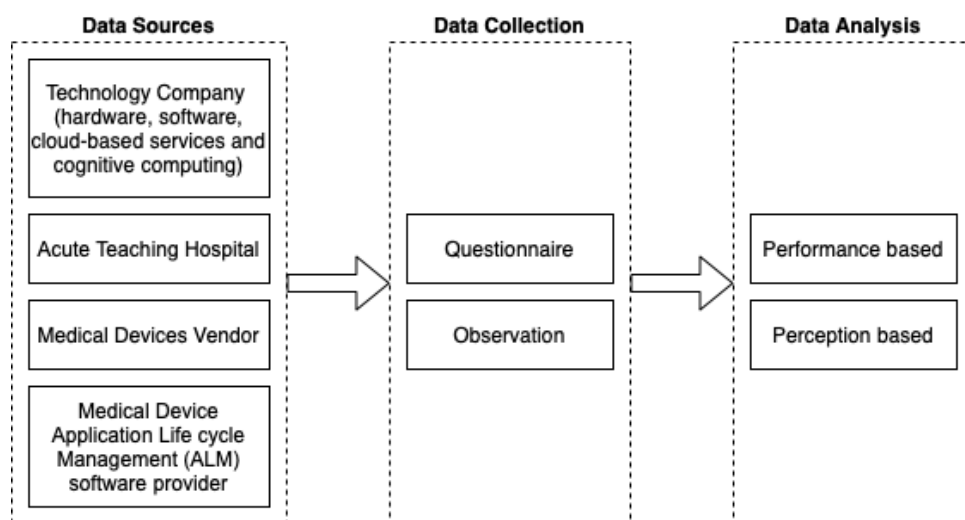


Figure 9.2: Survey data collection and analysis methods.

9.1.9 Study validity

For construct validity, we improved the questionnaires' quality after several iterations of improvement. Each iteration followed on the feedback from the University of Brighton's questionnaire experts' feedback to ensure no significant understanding of discrepancies by the users. Also, we carried out a pilot test at the University of Brighton, and there was a process of reflection and redevelopment of definition to make sure that the users understood the terms used. Further, there was an investigation in the literature and comparison with other metrics used in similar surveys. We evaluated the BINA methodology and correctly measured quantitative metrics, such as the efficacy and the effort required to undertake resiliency analysis activities in a healthcare system. The participants answered most of the questions, except those perceived as unsuitable for a simple scenario at an early analysis stage.

To increase the study's internal validity, we did not get involved directly in applying the methodology on the scenario given. Our involvement was limited to answering any questions of the users regarding the methodology and observing their behaviour. Also, there was method triangulation as we collected data with two different ways, through questionnaires and observation of the users while applying the methodology.

We held the workshops online to increase the external validity of the study. The users were from various countries, and among them, they were academics, industry researchers, research students, and post-graduate students. These users represent the expected user population.

9.2 Data collection

We made available to the users the presentation slides of the online introduction to the BINA methodology and tool. We also gave an already started project for the "cold chain" for the PfizerBioNTech vaccine scenario with an instance of a CIRP to make the users get started.

After the users attended the BINA presentation, started performing the evaluation tasks. We observed them and captured first-hand data collection behaviour and answered any possible additional questions that the users might have. The intent was to capture the users' way of conducting resiliency analysis. We wanted to establish a communication with the users since users reveal their thought process most naturally when communicating their way of working [203]. This online communication offers the best opportunity for us, due to COVID-19 to observe the application of BINA. All users constructed the BINA models with at least a part of the system functionalities stated in the scenario.

Following the scenario's resiliency analysis, the users were given web links to the online questionnaire to fill in and complete the online evaluation session. In general, we observed that the users developed the proposed BINA models satisfactorily regarding data validation, which means that the BINA methodology was applied correctly and following the process. Therefore, we can claim that the obtained data was valid to conduct the proposed evaluation.

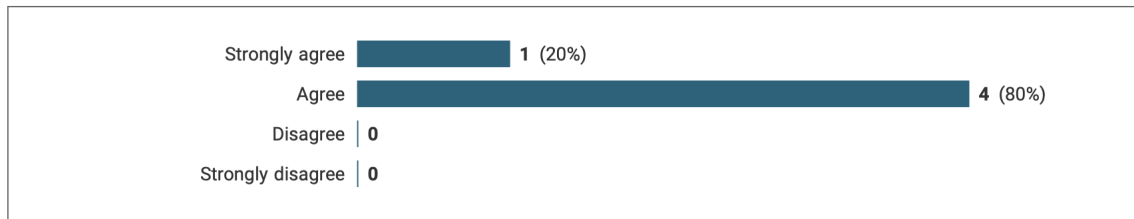
9.3 Data analysis

We evaluated the results combining quantitative and qualitative analysis techniques. For the quantitative data, we used descriptive statistics techniques. For the qualitative data, we coded them and then we identified patterns and formulated generalisations. These analyses achieved

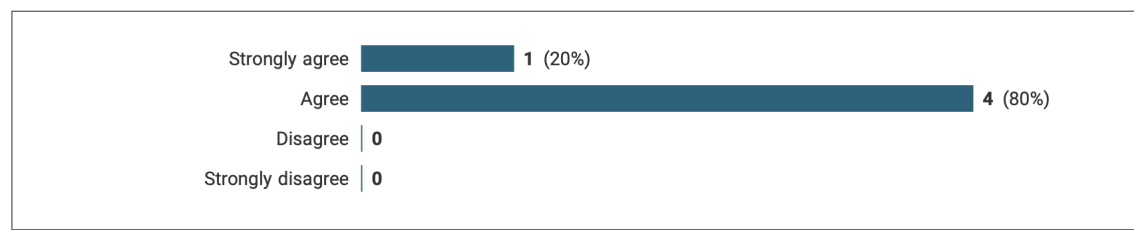
the objectives that we set at the start of the survey evaluation.

Among the survey participants, 80% agreed that the modelling language is powerful enough to support resiliency analysis and modelling. 80% of the survey participants strongly disagreed that the modelling language includes redundant concepts, and 20% disagreed that the modelling language had redundant concepts. 80% agreed, and 20% strongly agreed that the modelling language concepts were well-defined. Additionally, 60% of the survey participants agreed, and 40% disagreed that the modelling language's graphical notation was intuitive (Fig. 9.3).

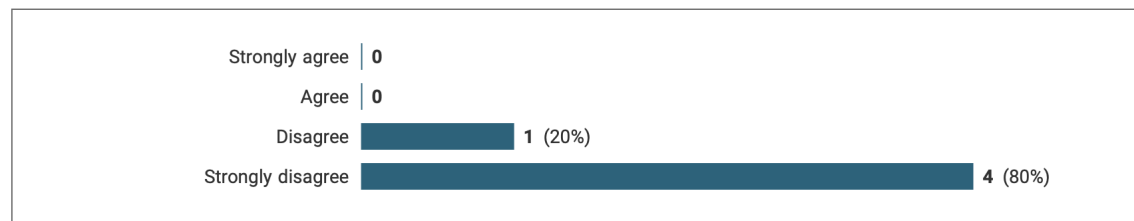
1 The BINA modelling language is powerful enough in order to support resiliency analysis and modelling.



2 The BINA language concepts are well defined.



3 The BINA modelling language includes redundant concepts.



4 The graphical notation employed by the BINA language is intuitive.

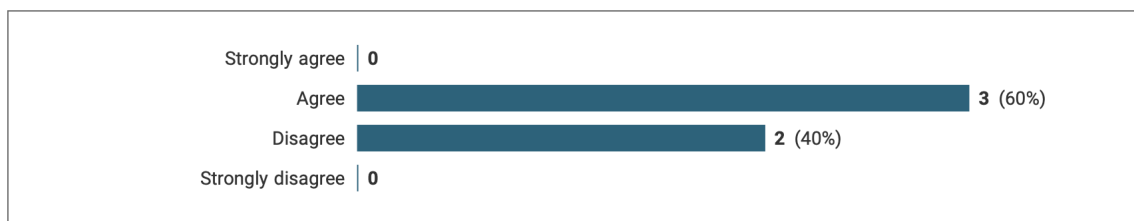
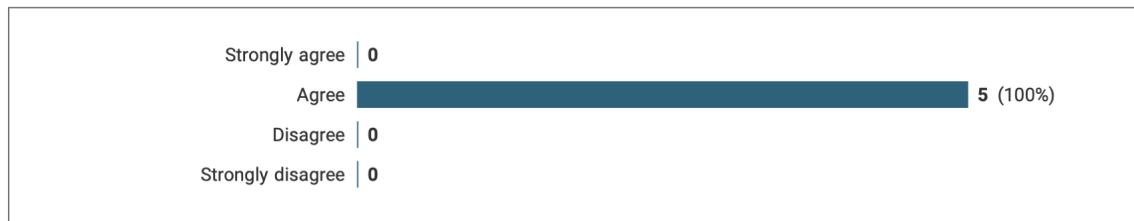


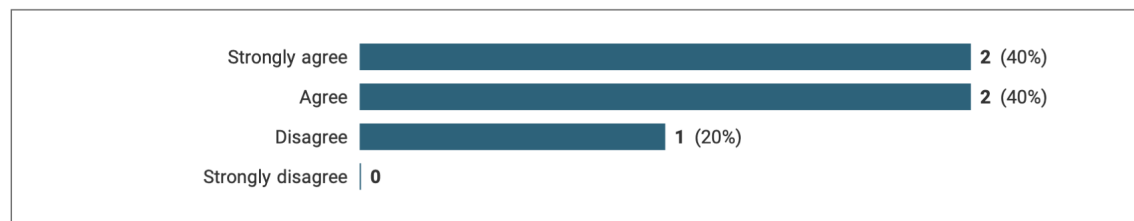
Figure 9.3: Survey results concerning the BINA modelling language.

Concerning the BINA modelling tool, all survey participants agreed that the tool required further improvement. On the other hand, 40% and 60% of the survey participants agreed and strongly agreed that the tool's resilience-related functions are satisfying, respectively. Further, 40% agreed, and 40% strongly agreed that the BINA tool was easy to use, and only 20% disagreed that the use of the tool is easy (cf. Fig. 9.4).

5 The BINA tool requires further improvement.



6 The BINA tool is easy to use.



7 The resiliency related functions of the BINA tool are satisfying.

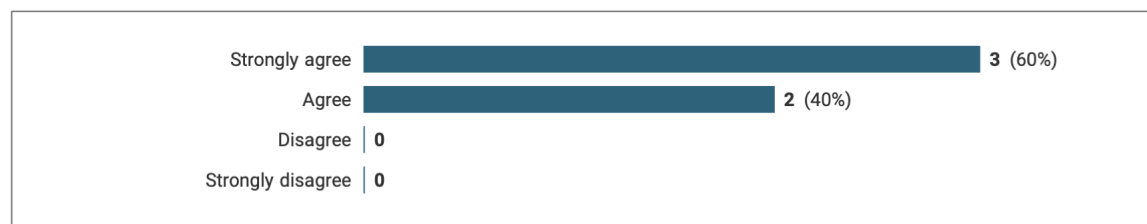
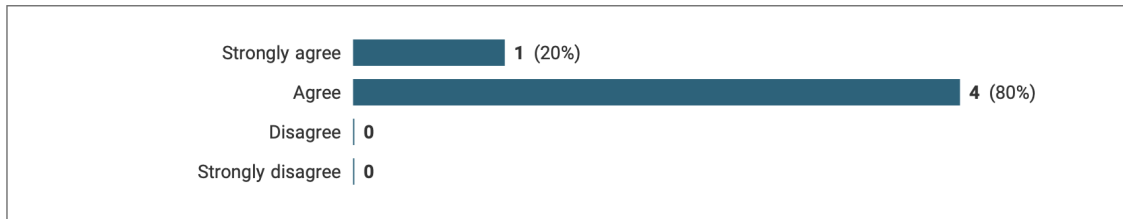


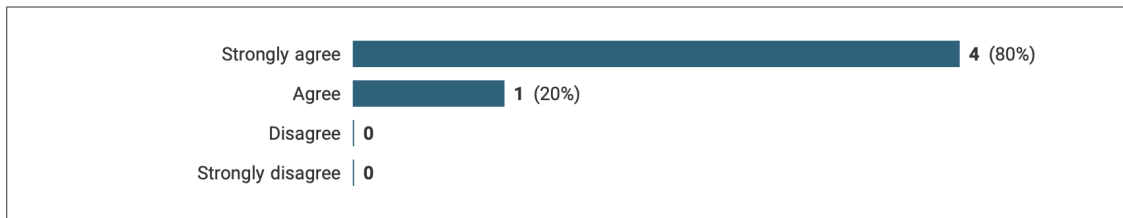
Figure 9.4: Survey results concerning the BINA tool.

Regarding the methodology as a whole, 80% and 20% of the survey participants agreed and strongly agreed that BINA methodology allows them to capture resiliency assumptions explicitly. Also, 100% of the survey participants strongly agreed that the methodology successfully captures resiliency requirements. This capability is a very significant result, as this is one of the most critical aspects of the methodology. Besides, 20% and 80% agreed and strongly agreed that the methodology successfully assesses the system resiliency at a requirements level. The method's usability, 60% and 40% of the survey participants responded that they strongly agreed and agreed that the methodology's activities were easy to follow (cf. Fig. 9.5).

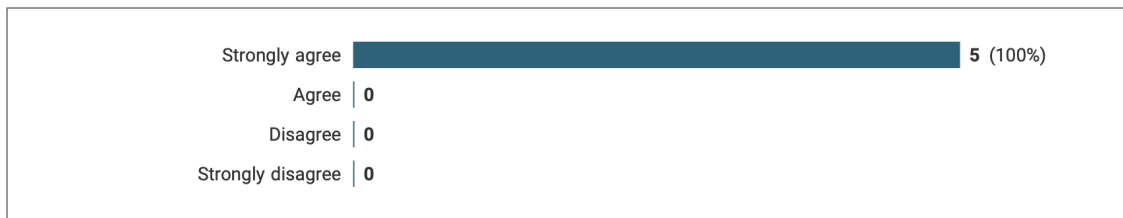
8 The use of the BINA methodology captures resiliency assumptions.



9 The BINA methodology successfully assesses the system resiliency.



10 The BINA methodology successfully captures resiliency requirements.



11 It is easy to follow the activities of the BINA methodology.

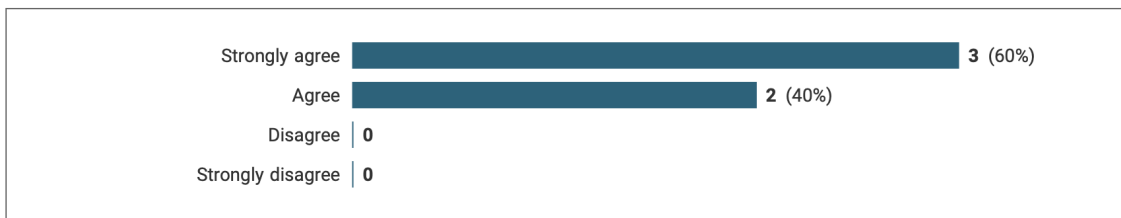


Figure 9.5: Survey results concerning the BINA methodology.

We took the coded qualitative data from the users' responses and identified patterns. Based on these patterns, we had the following outcomes:

- **The resiliency-related automation is useful.** In particular, automation is useful to identify the level of dependency and the system's reliance level. Moreover, this automation enables the calculation of the system resiliency at a requirements level.

- **A more intuitive type of notation would be preferable.** The goal modelling languages are not very popular among users. Thus, a BINA modelling language with a more intuitive even symbolic graphical notation could have been easier to learn and remember.
- **Users might find it challenging to use the methodology if they do not have prior goal modelling experience.** As goal modelling is the methodology's base; the users need to be familiar with goal models. Consequently, users not familiar with goal modelling will require individual training to learn to use the methodology.
- **The BINA tool has opportunities for improvement.** The improvement could be integrating the tool with other tools or integrating other relevant methodologies or becoming real-time and using machine learning. Moreover, BINA models tend to become large and complex, and the user's lack of modelling space is an issue.

During the lab session, we observed the execution of the survey tasks by the users, and we collected data in the form of notes. We took the coded data and made several observations, which contributed to the evaluation of our methodology. In this context, the main observations were the following:

- **BINA process:** The users identified the BINA methodology activities as operational and adequate to model and analyse resiliency requirements. Users found the activities systematic and reasonably applicable. They also expressed that the overall process reduces the resiliency reasoning bias and offers them guidance for argumentation of their final decisions.
- **BINA artefacts:** BINA provides a graphical representation of artefacts produced by its activities. Models provide a visual representation of resiliency analysis. Hence, users can communicate the resiliency requirements decision-making with other users, as observed during the online sessions.
- **BINA models:** The BINA models' size may become significant. This issue is from goal modelling, and as goal models are the base for the design of BINA models, they inherit this characteristic. A system under development may have many interactions with other entities of the system environment. By representing all the system dependencies in a model, the model becomes large. BINA adds overhead to that since it requires the modelling of CIRPs and reliance level on other actors. Further, it requires the modelling of resiliency requirements. As a result, the models tend to become big and complicated to read and analyse.
- **BINA validation techniques:** We proposed that once the user identifies the incidents and CIRPs, s/he/they need to seek evidence, such as organisational records and experience, to examine their implementational capacity, apart from the automation offered from the tool. Still, this may not be adequate for the user to proceed to such examination of validity. To this end, the user might need other validation techniques. For example, a user might need techniques that would guide him/her/they on where to seek evidence and what kind of evidence to seek. Such techniques will allow a system validation of resiliency and could complement the methodology.

9.4 Discussion and Closing Remarks

In this section, we conducted an empirical evaluation of our proposed methodology. It included two evaluation methods, the "cold chain" for the PfizerBioNTech vaccine case study

and a qualitative and quantitative survey. For the survey, we organised three online sessions inviting security engineers and researchers to apply our methodology. The case study and the survey enable us to evaluate our methodology. We reported the feedback the participants gave us and the observations we made during the case study and the online sessions. We also derived an understanding of the limitations of our methodology and the areas that need further research. Overall, the BINA methodology based on the survey is valid. Our observations during the case study were consistent with each other and with the user's feedback. We found that our proposed methodology was both easy to use and useful in modelling and reasoning about resiliency relationships, modelling and analysing resiliency requirements and assessing the system resiliency at a requirements level.

Chapter 10

Conclusions and Future Work

Nowadays, resiliency in cybersecurity is not simply a technical problem. The management of resiliency has become a vital issue within security-oriented organisations. Security engineers recognise that the impact of a resiliency solution to the overall organisational cybersecurity is critical. Resiliency risk management methods are methodological tools dealing with this concern. However, this research has observed that, despite structured processes, the (intermediate and final) products of those methods are generally informal. It has also observed that those methods mainly focus on evaluating posterior existing Information System (IS) rather than support the IS development. Moreover, since each method uses its terminology, it is challenging to combine them.

In this thesis, we have proposed a model-based approach for Build-In Resiliency Analysis (BINA) of a system's cybersecurity, applicable since the early phases of IS design and development, but also applicable once the IS is designed. Our work focuses on the modelling support to such an approach by proposing a framework consisting of a domain model, a process and a tool to support BINA. Our domain model helps improve the interoperability between the existing cybersecurity approaches when combining them and the different artefacts produced (contracts, metrics, processes). The domain model is also used to compare the cyber resiliency support of existing security-oriented modelling languages. To meet these objectives, we have proposed three complementary contributions summarised in the next section. Then, we describe the limitations of the contributions and propose directions for future work.

10.1 Review of research questions

According to two phases, we formulated a set of research questions related to the methodology development and evaluation. This section offers an overview of the research questions and the initial findings (cf. Tab. 10.1).

10.2 Research contributions

The framework presented in this work contributes to healthcare systems' cyber resiliency. More specifically, the contributions were made in resiliency modelling, security modelling, software-aided cyber resiliency analysis, and decision support. The significant contributions of the framework can be summarised as follows:

Table 10.1: Summary of research questions and proposed treatments

Research Phase	Research Question	Proposed Treatment
Knowledge and Design phase	What concepts should be present in a modelling language supporting Build-In ResilieNcy Analysis (BINA) for cyber-secure ISs?	We aligned the relevant concepts from the literature (cf. Chapter 2) and designed an initial BINA domain model (cf. Chapter 4), based on project-specific requirements (cf. Chapter 3).
Knowledge and Design phase	What metrics are relevant to perform Build-In ResilieNcy Analysis (BINA) and reason for cyber resiliency?	We aligned the relevant metrics from the literature (cf. Chapter 2) and integrated them into an updated version of the BINA domain model (cf. Chapter 5) based on project-specific requirements (cf. Chapter 3).
Knowledge and Design phase	What is the Build-In ResilieNcy Analysis (BINA) support provided by security-oriented modelling languages and how it can be improved?	We compared the proposed BINA domain model with security-oriented modelling languages (cf. Chapter 6) and enhanced the BINA methodology by designing a suitable process and a tool (cf. Chapter 7).
Evaluation phase	How well the proposed methodology supports modelling and reasoning about cyber resiliency requirements modelling and analysis?	We performed case studies and survey evaluation (cf. Chapter 8).

- A list of the fundamental characteristics and requirements of a cyber-resilient healthcare system. (relates to RQ1)
- A cyber resiliency domain model that derived from the semantic alignment and conceptual interoperability among cyber security and cyber resiliency resources. (relates to RQ1)
- A modelling language for developing models of healthcare systems to facilitate cyber resiliency analysis and decision support. The modelling language consists of syntax, semantics and graphical notation. (relates to RQ1)
- A metamodel for creating cyber-resilient system models to be used in the early phases of a system’s design and development engineering cycle. The models that can be instantiated can capture the intent of a healthcare system. As a result, the constructs of the design phase metamodel are used to express the high-level components of a cyber-resilient healthcare system (relates to RQ1)
- A set of metrics derived from cyber security and resiliency sources that enrich the domain model and allow quantification of cyber resiliency entities. (relates to RQ2)
- A method for assessing cyber security modelling languages about the coverage they offer for cyber resiliency entities. (relates to RQ3)
- An extension of the Secure Tropos metamodel to support cyber resiliency entities. (relates to RQ3)
- An extension of the Secure Tropos notation for resilient cyber systems. The notation is instantiated on a model, depending on the information that needs to be conveyed for a healthcare system under analysis. (relates to RQ3)
- A process supporting the application of the BINA framework that clarifies how to transition from an organisational model to an incident model and then to a holistic resiliency model. (relates to RQ3)

- An analysis algorithm to validate a model by the rules of the metamodel of the language. The algorithm can be applied dynamically on imported models to check their validity. Furthermore, it can be used automatically during the development of a model by prohibiting incorrect behaviour. (relates to RQ3)
- Algorithms to propose cyber resiliency insights on the dependence level among nodes, the system's resiliency as designed and analysis of the relations among cyber resiliency constructs. The cyber resiliency insights are used to facilitate the decision-making process by highlighting the model's attributes that can increase the system's resiliency. (relates to RQ3)
- A software tool that fully supports the use of the framework and automates its processes and algorithms. The tool support additional features such as customisation of the representation of models. (relates to RQ3)
- A proof-of-concept of the BINA framework through the use of two healthcare case studies and implementation of the BINA framework to a real case study. (relates to RQ4)
- An evaluation of the BINA framework through interviews and an online survey. (relates to RQ4)

10.3 Research limitations

The work reported in this thesis has several limitations. The limitations we have noticed are:

- In Chapter 5, we defined a set of metrics related to cyber resiliency. We further analysed the related literature and compared the elicited metrics. However, it could help compare these metrics with other security measurement frameworks, like [235, 236, 39]. This comparison could highlight the strengths and weaknesses of cyber resiliency approaches regarding other security approaches and their differences at the metric level.
- Regarding the comparison of modelling languages, we took into account only conceptual support. However, a comparison at the metric level is also necessary to fully assess a language regarding the domain model. For example, we have not analysed our estimation needs to assess existing languages degree of support.
- The validation for BINA has limitations. We illustrated the cyber-resiliency aware Secure Tropos extension through a real case study. Its use in a natural environment would validate its usefulness and efficiency to support the different systems and potentially not only healthcare systems. It would also highlight its limitations. Another limitation of the validation is that the case we used assesses BINA on an existing and evolving healthcare system. We did not have the opportunity to experiment with the Living Lab during the actual system development to introduce their resiliency requirements.
- The thesis's application part was about evaluating the domain model, metrics, process and tool support in a real context. The conclusion drawn on this evaluation is limited because we did not perform a comparative analysis to assess the methodology's efficiency. An experiment related to (a) the efficiency of the use of the domain model, compared to the use of a method or standard in natural language, for learning purposes (b) the efficiency of the use of the domain model, compared to the use of a method or standard in natural language, as guidelines for risk assessment, would both increase the validation level of the contributions.

10.4 Future work

- We could focus on early requirements till the requirements validation and documentation. One of our main assumptions is that it is necessary to deal with resiliency since the early stages of requirements engineering. We thus focus our work on early modelling approaches. By extending our approach to the full requirements engineering circle, we need to take into account other approaches such as UMLsec [180], SecureUML [178] or Mal-activity diagrams [237]. We could also extend the work of Secure Tropos to contain improvements for the requirements stage and the design stage.
- Explore further if medical systems' evolution requires a specification at a conceptual level and specialisation of a resiliency methodology associated with healthcare models for patients resiliency and survivability.
- We offer a tool that helps a designer deal with model complexity issues, the iterations in modelling, and traceability between models. However, as a tool-based automated recording and analysis of incidents could make the tool more efficient in dealing with real-time issues through machine learning and artificial intelligence. In this case, the language and overall methodology can extend to the development and improvement of systems-to-be.
- As the field of cyber resiliency is expanding, future approaches could focus not only on the NIST SP 800-160v2 [10] standard, especially at a tool analysis level. However, future studies extend to cover updated and new resiliency frameworks and security resiliency and compliance frameworks.
- Develop validation techniques for resiliency plans. This research requires more investigation into human psychology and resource availability. Future work can propose methods that will further support developers in validating systems' resilience. For instance, it can research the required type and quantity of evidence to validate a resiliency plan.
- Further research could focus on formalising the proposed methodology. The formalisation will complement the methodology by extending the BINA modelling language into a formal specification language. In this way, the language will be able to conduct a formal analysis of a system's resiliency capability, and it will be able to verify the resiliency model by employing formal verification techniques.
- Further work can focus on improving the BINA tool. Resiliency requirement concepts should go inside the system goal diagram because they are system functionality. The tool can allow the user to insert attributes, constructs and links that correspond to their needs. The graphical notation would also need to change to reflect the new constructs visually and intuitively.
- One possible direction of research in cyber resiliency includes mimicking the resilience of biological systems. For example, distributed autonomous agents may specialise in measuring the degradation of functionality in individual components rather than measuring global impact. Likewise, those distributed agents would respond and recover only the components they are responsible for, playing the role of cyber immunisers, similarly as IBM envisioned in [238]. The agents might also send measurements to a central brain capable of estimating the overall functionality and mission impact.

10.5 Publications in relation to this thesis

- Athinaiou, Myrsini Mouratidis, Haris Fotis, Dr Theofanis Pavlidis, Michalis. (2020). A Conceptual Redesign of a Modelling Language for Cyber Resiliency of Healthcare Systems. 10.1007/978-3-030-42048-2_10.
- Athinaiou, Myrsini Mouratidis, Haris Fotis, Dr Theofanis Pavlidis, Michalis Panaousis, Emmanouil. (2018). Towards the Definition of a Security Incident Response Modelling Language: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings. 10.1007/978-3-319-98385-1_14.
- Athinaiou, Myrsini. (2017). Cyber security risk management for health-based critical infrastructures. 402-407. 10.1109/RCIS.2017.7956566.

Bibliography

- [1] R. Beaumont, "Types of Health Information Systems (IS)," tech. rep., The Royal College of Surgeons of Edinburgh and Edinburgh University, Edinburgh, Sept. 2011.
- [2] L. Ayala, "Cyber-Physical Attack Recovery Procedures," in *Cyber-Physical Attack Recovery Procedures*, pp. 1–14, Berkeley, CA: Apress, 2016.
- [3] A. Stavert-Dobson, *Health Information Systems*. Health Informatics, Cham: Springer International Publishing, 2016.
- [4] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," Tech. Rep. NIST SP 800-61r2, National Institute of Standards and Technology, Aug. 2012.
- [5] N. P. S. Agency, "A risk matrix for risk managers," tech. rep., NHS, Jan. 2008.
- [6] M. Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte, and K. Scarfone, "Guide for cybersecurity event recovery," Tech. Rep. NIST SP 800-184, National Institute of Standards and Technology, Gaithersburg, MD, Dec. 2016.
- [7] D. Bodeau, R. Graubart, W. Heinbockel, and E. Laderman, "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques," Tech. Rep. MTR140499R1, MITRE, Bedford, MA, May 2015.
- [8] D. J. Bodeau, R. D. Graubart, J. Picciotto, and R. McQuaid, "Cyber Resiliency Engineering Framework," Technical Report MTR110237, MITRE, Bedford, MA, Jan. 2012.
- [9] M. Pavlidis, S. Islam, and H. Mouratidis, "A CASE Tool to Support Automated Modelling and Analysis of Security Requirements, Based on Secure Tropos," in *IS Olympics: Information Systems in a Diverse World* (W. van der Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, C. Szyperski, and S. Nurcan, eds.), vol. 107, pp. 95–109, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
- [10] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber resilient systems:: a systems security engineering approach."
- [11] L. Ayala, *Cyber-security glossary of building hacks and cyber-attacks*. CreateSpace Independent Publishing Platform, Sept. 2015.
- [12] WHO, "Health Systems Strengthening - Glossary," tech. rep., World Health Organization, Jan. 2011.
- [13] R. R. Nelson and S. G. Winter, *An evolutionary theory of economic change*. Cambridge, Mass.: The Belknap Press of Harvard Univ. Press, digitally reprinted ed., 2004. OCLC: 255191816.

- [14] E. Union, "REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC," *Official Journal of the European Union*, Apr. 2017.
- [15] E. Union, "REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU," Apr. 2017.
- [16] E. Union, "REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)," Apr. 2019.
- [17] T. E. P. a. T. C. of The European Union, "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Document 32016L1148*, July 2016.
- [18] C. Office, "Summary of the 2015 - 16 Sector Resilience Plans," tech. rep., Crown copyright, London, Apr. 2016.
- [19] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *1st international conference on High Confidence Networked Systems*, pp. 47–54, ACM Press, 2012.
- [20] P. Cheng, H. Zhang, and J. Chen, *Cyber security for industrial control systems: from the viewpoint of close-loop*. 2016. OCLC: 945552739.
- [21] Insup Lee, O. Sokolsky, Sanjian Chen, J. Hatcliff, Eunkyong Jee, BaekGyu Kim, A. King, M. Mullen-Fortino, Soojin Park, A. Roederer, and K. K. Venkatasubramanian, "Challenges and Research Directions in Medical Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 100, pp. 75–90, Jan. 2012.
- [22] L. Ayala, "Medical Facility Cyber-Physical Attacks," in *Cybersecurity for Hospitals and Healthcare Facilities*, pp. 39–45, Berkeley, CA: Apress, 2016.
- [23] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," *Journal of Medical Internet Research*, vol. 20, p. e10059, May 2018.
- [24] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Proceedings of the conference on The future of Software engineering - ICSE '00*, pp. 35–46, ACM Press.
- [25] E. Yu, "Towards modelling and reasoning support for early-phase requirements engineering," *Proceedings of ISRE '97: 3rd IEEE International Symposium on Requirements Engineering*, pp. 226–235, 1997.
- [26] M. Jackson, "The meaning of requirements," vol. 3, pp. 5–21.
- [27] M. Glinz, "On non-functional requirements," in *15th IEEE International Requirements Engineering Conference (RE 2007)*, pp. 21–26, IEEE.
- [28] S. Robertson and J. Robertson, *Mastering the requirements process*. ACM Press books, ACM Press. OCLC: 833551226.
- [29] K. E. Wiegers and J. Beatty, *Software requirements*. Microsoft Press, s division of Microsoft Corporation, third edition ed. OCLC: ocn850176256.

- [30] "IEEE recommended practice for software requirements specifications: approved 25 June 1998." OCLC: 254961688.
- [31] I. S. . Q. systems, "ISO 9001:2015 quality management systems — requirements."
- [32] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements Engineering*, vol. 10, pp. 34–44, Jan. 2005.
- [33] H. Mouratidis and P. Giorgini, "Secure tropos: a security-oriented extension of the tropos methodology," *International Journal of Software Engineering and Knowledge Engineering*, vol. 17, pp. 285–309, Apr. 2007.
- [34] J. C. Henderson and N. Venkatraman, "Strategic alignment: Leveraging information technology for transforming organizations," *IBM Syst. J.*, vol. 32, pp. 4–16, 1993.
- [35] "Exploring services science." OCLC: 964897376.
- [36] R. Costa Climent and D. M. Haftor, "Value creation through the evolution of business model themes," vol. 122, pp. 353–361.
- [37] B. Meng, D. Larraz, K. Siu, A. Moitra, J. Interrante, W. Smith, S. Paul, D. Prince, H. Herencia-Zapana, M. F. Arif, M. Yahyazadeh, V. Tekken Valapil, M. Durling, C. Tinelli, and O. Chowdhury, "VERDICT: A language and framework for engineering cyber resilient and safe system," vol. 9, no. 1, p. 18.
- [38] A. Ferreira and R. Cruz-Correia, "COVID-19 and cybersecurity: Finally, an opportunity to disrupt?," vol. 2, no. 2, p. e21069.
- [39] D. Beyer and G. Ourada, "An overview of the cyber resiliency level® (CRL®) framework for weapon, mission, and training systems," in *AIAA Scitech 2021 Forum*, American Institute of Aeronautics and Astronautics.
- [40] B. Bauer and J. Odell, "UML 2.0 and agents: how to build agent-based systems with the new UML standard," vol. 18, no. 2, pp. 141–157.
- [41] P. A. Laplante, *Requirements engineering for software and systems, second edition*. OCLC: 893419202.
- [42] C. 4009, "CNSSI 4009 committee on national security systems (CNSS) glossary."
- [43] N. S. 800-66, "NIST special publication 800-66 revision 1 an introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule."
- [44] N. S. 800-34, "NIST special publication (SP) 800-34, revision 1, contingency planning guide for federal information systems."
- [45] N. S. 800-30, "NIST special publication 800-30 revision 1."
- [46] L. Ayala, *Cybersecurity for Hospitals and Healthcare Facilities*. Berkeley, CA: Apress, 2016.
- [47] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: a proposal and a discussion," *Requirements Engineering*, vol. 11, pp. 102–107, Mar. 2006.
- [48] N. Cross, "Chapter 5 - Design Cognition: Results from Protocol and other Empirical Studies of Design Activity," in *Design Knowing and Learning: Cognition in Design Education*, pp. 79–103, Elsevier, 2001.

- [49] R. Wieringa, *Design Science Methodology for Information Systems and Software Engineering*. Springer-Verlag.
- [50] A. van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models," in *Proceedings. 26th International Conference on Software Engineering*, (Edinburgh, UK), pp. 148–157, IEEE Comput. Soc, 2004.
- [51] T. K. Mackey and B. A. Liang, "Pharmaceutical digital marketing and governance: illicit actors and challenges to global patient safety and public health," *Globalization and Health*, vol. 9, no. 1, p. 45, 2013.
- [52] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, pp. 1–10, Feb. 2017.
- [53] V. J. Watzlaf, L. Zhou, D. R. DeAlmeida, and L. M. Hartman, "A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices Used By Healthcare Providers," *International Journal of Telerehabilitation*, vol. 9, pp. 39–58, Nov. 2017.
- [54] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health Care and Cybersecurity: Bibliometric Analysis of the Literature," *Journal of Medical Internet Research*, vol. 21, p. e12644, Feb. 2019.
- [55] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, July 2018.
- [56] S. T. Argaw, N.-E. Bempong, B. Eshaya-Chauvin, and A. Flahault, "The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review," *BMC Medical Informatics and Decision Making*, vol. 19, p. 10, Dec. 2019.
- [57] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, pp. 113–122, July 2017.
- [58] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of Biomedical Informatics*, vol. 55, pp. 272–289, June 2015.
- [59] I. Ben Ida, A. Jemai, and A. Loukil, "A survey on security of IoT in the context of eHealth and clouds," in *2016 11th International Design & Test Symposium (IDT)*, (Hammamet, Tunisia), pp. 25–30, IEEE, Dec. 2016.
- [60] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Information and Software Technology*, vol. 51, pp. 7–15, Jan. 2009.
- [61] M. S. Jalali, B. Russell, S. Razak, and W. J. Gordon, "EARS to cyber incidents in health care," *Journal of the American Medical Informatics Association*, vol. 26, pp. 81–90, Jan. 2019.
- [62] NSA, *Untangling the web: a guide to Internet research*. 2013. OCLC: 845013431.
- [63] T. L. Wiant, "Information security policy's impact on reporting security incidents," *Computers & Security*, vol. 24, pp. 448–459, Sept. 2005.
- [64] T. Cooper, J. Collmann, and H. Neidermeier, "Organizational Repertoires and Rites in Health Information Security," *Cambridge Quarterly of Healthcare Ethics*, vol. 17, pp. 441–452, Oct. 2008.

- [65] P. A. H. Williams, "Is Cyber Resilience in Medical Practice Security Achievable?," in *Proceedings of the 1st International Cyber Resilience Conference*, (Edith Cowan University, Perth Western Australia), pp. 105 – 111, Aug. 2010.
- [66] C. DeVoe and S. S. M. Rahman, "Incident Response Plan for a Small to Medium Sized Hospital," *International Journal of Network Security & Its Applications*, vol. 5, pp. 1–20, Mar. 2013.
- [67] P. N. Genes, MD, M. Chary, PhD, and K. W. Chason, DO, "Case study. An academic medical center's response to widespread computer failure," *American Journal of Disaster Medicine*, vol. 8, pp. 145–150, Apr. 2013.
- [68] Q. Chen and J. Lambright, "Towards Realizing a Self-Protecting Healthcare Information System," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, (Atlanta, GA, USA), pp. 687–690, IEEE, June 2016.
- [69] D. Sittig and H. Singh, "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks," *Applied Clinical Informatics*, vol. 07, pp. 624–632, Apr. 2016.
- [70] A. Boddy, W. Hurst, M. Mackay, and A. E. Rhalibi, "A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning - IML '17*, (Liverpool, United Kingdom), pp. 1–7, ACM Press, 2017.
- [71] Y. He and C. Johnson, "Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization," *Informatics for Health and Social Care*, vol. 42, pp. 393–408, Oct. 2017.
- [72] S. Ghafur, E. Grass, N. A. Jennings, and A. Darzi, "The challenges of cybersecurity in health care: the UK National Health Service as a case study," *The Lancet Digital Health*, vol. 1, pp. e10–e12, May 2019.
- [73] D. McGlade and S. Scott-Hayward, "ML-based cyber incident detection for Electronic Medical Record (EMR) systems," *Smart Health*, vol. 12, pp. 3–23, Apr. 2019.
- [74] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare Data Breaches: Implications for Digital Forensic Readiness," *Journal of Medical Systems*, vol. 43, p. 7, Jan. 2019.
- [75] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem," vol. 7, no. 3, pp. 352–366.
- [76] B. Sheehan, F. Murphy, A. N. Kia, and R. Kiely, "A quantitative bow-tie cyber risk classification and assessment framework," pp. 1–20.
- [77] T. Llansó and M. McNeil, "Towards an organizationally-relevant quantification of cyber resilience," in *Hawaii International Conference on System Sciences 2021*. OCLC: 1232149270.
- [78] B. Ransford, S. S. Clark, D. F. Kune, K. Fu, and W. P. Burlison, "Design Challenges for Secure Implantable Medical Devices," in *Security and Privacy for Implantable Medical Devices* (W. Burlison and S. Carrara, eds.), pp. 157–173, New York, NY: Springer New York, 2014.
- [79] L. Ayala, "Active Medical Device Cyber-Attacks," in *Cybersecurity for Hospitals and Healthcare Facilities*, pp. 19–37, Berkeley, CA: Apress, 2016.

- [80] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, pp. 30–39, Jan. 2008.
- [81] M. J. Ryan, "1.2.2 The Role of Stakeholders in Requirements Elicitation," *INCOSE International Symposium*, vol. 24, pp. 16–26, July 2014.
- [82] Q. Shafi, "Cyber Physical Systems Security: A Brief Survey," in *2012 12th International Conference on Computational Science and Its Applications*, (Salvador, Bahia, Brazil), pp. 146–150, IEEE, June 2012.
- [83] P. Dong, Y. Han, X. Guo, and F. Xie, "A Systematic Review of Studies on Cyber Physical System Security," *International Journal of Security and Its Applications*, vol. 9, pp. 155–164, Jan. 2015.
- [84] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, vol. 4, pp. 1802–1831, Dec. 2017.
- [85] P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems: A systematic mapping study," *Information and Software Technology*, vol. 83, pp. 116–135, Mar. 2017.
- [86] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems," *KSII Transactions on Internet and Information Systems*, vol. 8, Dec. 2014.
- [87] S. A. Haque, S. M. Aziz, and M. Rahman, "Review of Cyber-Physical System in Healthcare," *International Journal of Distributed Sensor Networks*, vol. 10, p. 217415, Apr. 2014.
- [88] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. S. Tavares, "Medical cyber-physical systems: A survey," *Journal of Medical Systems*, vol. 42, p. 74, Apr. 2018.
- [89] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic, "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," *IEEE Internet of Things Journal*, vol. 5, pp. 3810–3822, Oct. 2018.
- [90] K. K. Venkatasubramanian, S. Nabar, S. Gupta, and R. Poovendran, "Cyber physical security solutions for pervasive health monitoring systems," in *User-driven healthcare: concepts, methodologies, tools, and applications*, Essential reference, pp. 447–465, Hershey, PA: IGI Global, 2013.
- [91] J. L. Fernández-Alemán, I. C. Señor, P. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, vol. 46, pp. 541–562, June 2013.
- [92] P. Ma, Z. Wang, X. Zou, J. Zhang, Q. Liu, X. Lyu, and W. Wang, "Medical Imaging Device Security: An Exploratory Study," *arXiv:1904.00224 [cs]*, Mar. 2019. arXiv: 1904.00224.
- [93] Z. u. Rehman, S. Altaf, and S. Iqbal, "Survey of Authentication Schemes for Health Monitoring: A Subset of Cyber Physical System," in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, (Islamabad, Pakistan), pp. 653–660, IEEE, Jan. 2019.
- [94] F. da Silveira, I. R. Neto, F. M. Machado, M. P. da Silva, and F. G. Amaral, "Analysis of Industry 4.0 Technologies Applied to the Health Sector: Systematic Literature Review," in *Occupational and Environmental Safety and Health* (P. M. Arezes, J. S. Baptista, M. P. Barroso, P. Carneiro, P. Cordeiro, N. Costa, R. B. Melo, A. S. Miguel, and G. Perestrelo, eds.), vol. 202, pp. 701–709, Cham: Springer International Publishing, 2019.

- [95] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari, and P. D. Curtis, "CERT® Resilience Management Model, Version 1.2," Tech. Rep. DM-0003234, Carnegie Mellon University Software Engineering Institute, Feb. 2016.
- [96] A. B. Urken, A. "Buck" Nimz, and T. M. Schuck, "Designing evolvable systems in a framework of robust, resilient and sustainable engineering analysis," *Advanced Engineering Informatics*, vol. 26, pp. 553–562, Aug. 2012.
- [97] D. D. Woods, "Four concepts for resilience and the implications for the future of resilience engineering," *Reliability Engineering & System Safety*, vol. 141, pp. 5–9, Sept. 2015.
- [98] W. E. Forum, "Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines (p.14)," tech. rep., World Economic Forum, Geneva, Switzerland, 2012.
- [99] F. Björck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber Resilience – Fundamentals for a Definition," in *New Contributions in Information Systems and Technologies* (A. Rocha, A. M. Correia, S. Costanzo, and L. P. Reis, eds.), vol. 353, pp. 311–316, Cham: Springer International Publishing, 2015.
- [100] D. of Homeland Security Risk Steering Committee, "DHS Risk Lexicon," tech. rep., Department of Homeland Security Risk Steering Committee, Sept. 2010.
- [101] M. E. Csete and J. C. Doyle, "Reverse Engineering of Biological Complexity," *Science*, vol. 295, pp. 1664–1669, Mar. 2002.
- [102] E. Hollnagel, *The ETTO Principle: Efficiency-Thoroughness Trade-Off: Why Things That Go Right Sometimes Go Wrong*. CRC Press, 1 ed., Nov. 2017.
- [103] J. H. Kahan, A. C. Allen, and J. K. George, "An Operational Framework for Resilience," *Journal of Homeland Security and Emergency Management*, vol. 6, Jan. 2009.
- [104] K. R. Reddi and Y. B. Moon, "A framework for managing engineering change propagation," *International Journal of Innovation and Learning*, vol. 6, no. 5, p. 461, 2009.
- [105] A. Waller and R. Craddock, "Managing Runtime Re-engineering of a System-of-Systems for Cyber Security," in *2011 6th International Conference on System of Systems Engineering (SoSE 2011)*, pp. 13–18, Albuquerque, New Mexico, USA: IEEE, June 2011. OCLC: 839118051.
- [106] S. Ranjan, M. Kumar Maurya, K. M. Apurva, R. Yadav, R. Gupta, M. Mishra, and S. Rai, "Building an Information Security Infrastructure - A Comprehensive Framework towards a Robust, Resilient and Dependable Infrastructure," *International Journal of Computer Science Issues*, vol. 9, pp. 414–419, May 2012.
- [107] D. Bodeau and R. Graubart, "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls," Project No.: 19128454-CA MTR130531, MITRE Corporation, Bedford, MA, Sept. 2013.
- [108] G. Dsouza, S. Hariri, Y. Al-Nashif, and G. Rodriguez, "Resilient Dynamic Data Driven Application Systems (rDDDDAS)," *Procedia Computer Science*, vol. 18, pp. 1929–1938, 2013.
- [109] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environment Systems and Decisions*, vol. 33, pp. 471–476, Dec. 2013.

- [110] D. J. Bodeau, R. D. Graubart, and E. R. Laderman, "Cyber Resiliency Engineering Overview of the Architectural Assessment Process," *Procedia Computer Science*, vol. 28, pp. 838–847, 2014.
- [111] E. D. Vugrin, M. J. Baca, M. D. Mitchell, and K. L. Stamber, "Evaluating the effect of resource constraints on resilience of bulk power system with an electric power restoration model," *International Journal of System of Systems Engineering*, vol. 5, no. 1, pp. 68–91, 2014.
- [112] U. Bhatia, D. Kumar, E. Kodra, and A. R. Ganguly, "Network Science Based Quantification of Resilience Demonstrated on the Indian Railways Network," *PLOS ONE*, vol. 10, p. e0141890, Nov. 2015.
- [113] P. Clay, "A modern threat response framework," *Network Security*, vol. 2015, pp. 5–10, Apr. 2015.
- [114] D. DiMase, Z. A. Collier, K. Heffner, and I. Linkov, "Systems engineering framework for cyber physical security and resilience," *Environment Systems and Decisions*, vol. 35, pp. 291–300, June 2015.
- [115] R. Filippini and A. Silva, "IRML: An Infrastructure Resilience-Oriented Modeling Language," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, pp. 157–169, Jan. 2015.
- [116] E. T. Yano, W. de Abreu, P. M. Gustavsson, and R.-M. Åhlfeldt, "A framework to support the development of Cyber Resiliency with Situational Awareness Capability," (Annapolis, Maryland, USA), p. 11, International Command and Control Institute, June 2015.
- [117] J. Zalewski, S. Drager, W. McKeever, A. J. Kornecki, and B. Czejdo, "Modeling Resiliency and Its Essential Components for Cyberphysical Systems," pp. 107–114, Oct. 2015.
- [118] CISCO, "Cyber Resilience: Safeguarding the Digital Organization," white Paper, Cisco Public, 2016.
- [119] B. Keys, A. Chhajer, Z. Liu, D. Horner, and S. Shapiro, "A framework for assessing cyber resilience," tech. rep., World Economic Forum, Apr. 2016.
- [120] V. Mehta, P. D. Rowe, G. Lewis, A. Magalhaes, and M. Kochenderfer, "Decision-Theoretic Approach to Designing Cyber Resilient Systems," in *Proceedings, 2016 IEEE 15th International Symposium on Network Computing and Applications: 30 October-2 November 2016, Cambridge, MA, USA*, pp. 302–309, 2016. OCLC: 985481226.
- [121] H. Tran, E. Campos-Nanez, P. Fomin, and J. Wasek, "Cyber resilience recovery model to combat zero-day malware attacks," *Computers & Security*, vol. 61, pp. 19–31, Aug. 2016.
- [122] W. A. Conklin, D. Shoemaker, and A. Kohnke, "Cyber resilience: rethinking cybersecurity strategy to build a cyber resilient architecture," in *Proceedings of the 5th International Conference on Management Leadership and Governance*, pp. 105–111, Mar. 2017.
- [123] J. Rajamäki and R. Pirinen, "Design science research towards resilient cyber-physical eHealth systems," *Finnish Journal of eHealth and eWelfare*, vol. 9, pp. 203–216, May 2017.
- [124] N. Rashid, J. Wan, G. Quiros, A. Canedo, and M. A. A. Faruque, "Modeling and Simulation of Cyberattacks for Resilient Cyber-Physical Systems," in *2017 13th IEEE Conference on Automation Science and Engineering (CASE): 20-23 Aug. 2017.*, IEEE Conference on Automation Science and Engineering, (Xi'an, China), pp. 988–993, IEEE Robotics and Automation Society, Aug. 2017. OCLC: 1028643048.

- [125] D. Whelihan, M. Vai, N. Evancich, K. Kwak, J. Li, M. Britton, B. Frantz, D. Hadcock, M. Lynch, D. Schafer, J. DeMatteis, and D. Russo, "Designing agility and resilience into embedded systems," in *IEEE Military Communications Conference (MILCOM)*, pp. 249–254, Baltimore, MD, USA: IEEE Military Communications Conference, Oct. 2017. OCLC: 1025339357.
- [126] H. Kamrul, S. Sachin, H. Amin, B. S. Malek, and C. Jay, "Self-Healing Cyber Resilient Framework for Software Defined Networking-enabled Energy Delivery System," in *2018 IEEE Conference on Control Technology and Applications (CCTA): 21-24 August 2018.*, pp. 1692–1697, Copenhagen, Denmark: IEEE, Aug. 2018. OCLC: 1076574445.
- [127] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, and J. Sztipanovits, "SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 106, pp. 93–112, Jan. 2018.
- [128] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, "Building organizational resilience in the face of multiple disruptions," *International Journal of Production Economics*, vol. 197, pp. 63–83, Mar. 2018.
- [129] X. Merino Aguilera, C. Otero, M. Ridley, and D. Elliott, "Managed Containers: A Framework for Resilient Containerized Mission Critical Systems," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, (San Francisco, CA, USA), pp. 946–949, IEEE, July 2018.
- [130] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," *Computers in Industry*, vol. 104, pp. 47–58, Jan. 2019.
- [131] I. Kotenko, I. Saenko, and O. Lauta, "Modeling the Impact of Cyber Attacks," in *Cyber Resilience of Systems and Networks* (A. Kott and I. Linkov, eds.), pp. 135–169, Cham: Springer International Publishing, 2019.
- [132] N. U. I. Hossain, F. Nur, S. Hosseini, R. Jaradat, M. Marufuzzaman, and S. M. Puryear, "A Bayesian network based approach for modeling and assessing resilience: A case study of a full service deep water port," *Reliability Engineering & System Safety*, vol. 189, pp. 378–396, Sept. 2019.
- [133] F. Januario, A. Cardoso, and P. Gil, "A Distributed Multi-Agent Framework for Resilience Enhancement in Cyber-Physical Systems," *IEEE Access*, vol. 7, pp. 31342–31357, 2019.
- [134] M. Li, Z. Liu, X. Li, and Y. Liu, "Dynamic risk assessment in healthcare based on Bayesian approach," *Reliability Engineering & System Safety*, vol. 189, pp. 327–334, Sept. 2019.
- [135] M. D. Wood, E. M. Wells, G. Rice, and I. Linkov, "Quantifying and mapping resilience within large organizations," *Omega*, vol. 87, pp. 117–126, Sept. 2019.
- [136] R. van der Kleij and R. Leukfeldt, "Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security," in *Advances in Human Factors in Cybersecurity* (T. Ahram and W. Karwowski, eds.), vol. 960, pp. 16–27, Cham: Springer International Publishing, 2020.
- [137] A. van Lamsweerde, "Goal-oriented requirements engineering: a guided tour," in *Proceedings Fifth IEEE International Symposium on Requirements Engineering*, (Toronto, Ont., Canada), pp. 249–262, IEEE Comput. Soc, 2000.

- [138] Dubois, P. Heymans, N. Mayer, and R. Matulevičius, “A Systematic Approach to Define the Domain of Information System Security Risk Management,” in *Intentional Perspectives on Information Systems Engineering* (S. Nurcan, C. Salinesi, C. Souveyet, and J. Ralyté, eds.), pp. 289–306, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.
- [139] J. Rumbaugh, I. Jacobson, and G. Booch, *The unified modeling language reference manual*. The Addison-Wesley object technology series, Reading, Mass: Addison-Wesley, 1999.
- [140] ISO/TC 199 Safety of machinery, “ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects,” tech. rep., International Organization for Standardization (ISO), Dec. 2018.
- [141] R. Ross, R. Graubart, D. Bodeau, and R. McQuaid, “Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems,” tech. rep., NIST, Mar. 2018.
- [142] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” Tech. Rep. NIST SP 800-82r2, National Institute of Standards and Technology, June 2015.
- [143] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, “ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements,” Tech. Rep. 2, International Organization for Standardization (ISO), Oct. 2013.
- [144] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, “ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity,” tech. rep., International Organization for Standardization (ISO), July 2012.
- [145] G. O’Brien, S. Edwards, K. Littlefield, N. McNab, S. Wang, and K. Zheng, “Securing Wireless Infusion Pumps In Healthcare Delivery Organizations,” Draft NIST SPECIAL PUBLICATION 1800-8, National Institute of Standards and Technology, U.S. Department of Commerce and National Cybersecurity Center of Excellence, May 2017.
- [146] Technical Committee ISO/TC 215 Health informatics, “ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002,” Tech. Rep. 2, International Organization for Standardization (ISO), July 2016.
- [147] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” Tech. Rep. NIST SP 800-66r1, National Institute of Standards and Technology, Gaithersburg, MD, Oct. 2008.
- [148] N. Genon, “Modelling security during early requirements: contributions to and usage of a domain model for information system security risk management,” Master’s thesis, University of Namur, Belgium, 2007.
- [149] J. Rumbaugh, I. Jacobson, and G. Booch, *The Unified Modeling Language reference manual: covers UML 2.0*. The Addison-Wesley object technology series, Boston: Addison-Wesley, 2. ed ed., 2005. OCLC: 837656983.
- [150] R. Matulevičius, P. Heymans, and A. L. Opdahl, “Comparing GRL and KAOS using the UEML Approach,” in *Enterprise Interoperability II* (R. J. Gonçalves, J. P. Müller, K. Mertins, and M. Zelm, eds.), pp. 77–88, London: Springer London, 2007.

- [151] P.-Y. Schobbens, P. Heymans, J.-C. Trigaux, and Y. Bontemps, "Generic semantics of feature diagrams," *Computer Networks*, vol. 51, pp. 456–479, Feb. 2007.
- [152] D. Harel and B. Rumpe, "Meaningful modeling: what's the semantics of "semantics"?", *Computer*, vol. 37, pp. 64–72, Oct. 2004.
- [153] E. Rahm and P. A. Bernstein, "A survey of approaches to automatic schema matching," *The VLDB Journal*, vol. 10, pp. 334–350, Dec. 2001.
- [154] I. Reinhartz-Berger, P. Soffer, and A. Sturm, "A Domain Engineering Approach to Specifying and Applying Reference Models," in *Workshop on Enterprise Modeling Information Systems Architecture (EMISA '05)*, vol. 1, pp. 50–63, 2005.
- [155] K. C. Kang, S. G. Cohen, J. A. Hess, W. E. Novak, and A. S. Peterson, "Feature-Oriented Domain Analysis (FODA) Feasibility Study," Tech. Rep. ADA235785, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, Nov. 1990.
- [156] W. Frakes, R. Prieto-Diaz, and C. Fox, "DARE: Domain analysis and reuse environment," *Annals of Software Engineering*, vol. 5, no. 1, pp. 125–141, 1998.
- [157] B. Hjørland, "Domain analysis in information science: Eleven approaches – traditional as well as innovative," *Journal of Documentation*, vol. 58, pp. 422–462, Aug. 2002.
- [158] M. Dunn Cavelti, "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities," vol. 20, no. 3, pp. 701–715.
- [159] B. Rodrigues, M. Franco, G. Parangi, and B. Stiller, "SEconomy: A framework for the economic assessment of cybersecurity," in *Economics of Grids, Clouds, Systems, and Services* (K. Djemame, J. Altmann, J. Bañares, O. Agmon Ben-Yehuda, and M. Naldi, eds.), vol. 11819, pp. 154–166, Springer International Publishing. Series Title: Lecture Notes in Computer Science.
- [160] S. Yung, "Cybersecurity Fortification Initiative," Tech. Rep. B1/15C, B9/29C, Hong Kong Monetary Authority, Hong Kong, Dec. 2016.
- [161] R. van Solingen, V. Basili, G. Caldiera, and H. D. Rombach, "Goal Question Metric (GQM) Approach," in *Encyclopedia of Software Engineering* (J. J. Marciniak, ed.), p. 142, Hoboken, NJ, USA: John Wiley & Sons, Inc., Jan. 2002.
- [162] G. Wingate, ed., *Computer systems validation: quality assurance, risk management, and regulatory compliance for pharmaceutical and healthcare companies*. Boca Raton, FL: Interpharm/CRC, 2004.
- [163] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis," in *In the 40th Annual Hawaii International Conference on System Sciences*, 2007.
- [164] V. Viduto, C. Maple, W. Huang, and D. López-Peréz, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem," *Decision Support Systems*, vol. 53, pp. 599–610, June 2012.
- [165] D. D. LLC., "Hacktivism A defender's playbook," threat Intelligence and Analytics, Deloitte Touche Tohmatsu Limited, Aug. 2016.
- [166] A. E. Stuck, J. M. Walthert, T. Nikolaus, C. J. Büla, C. Hohmann, and J. C. Beck, "Risk factors for functional status decline in community-living elderly people: a systematic literature review," *Social Science & Medicine*, vol. 48, pp. 445–469, Feb. 1999.

- [167] I. Trump, "What is the price of healthcare cyber-attacks?," *SC Media UK*, Mar. 2016.
- [168] M. a. H. products Regulatory Agency, "Alerts and recalls for drugs and medical devices," drug Safety Update, Medicines and Healthcare products Regulatory Agency, June 2017.
- [169] V. R. Basili, G. Caldiera, and H. D. Rombach, "The Goal Question Metric Approach," in *Encyclopedia of Software Engineering*, Wiley, 1994.
- [170] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI) a practical quantitative model:," in *Proceedings of the 3rd International Workshop on Security in Information Systems*, pp. 239–252, SciTePress - Science and and Technology Publications.
- [171] S. Fowler and P. P. Chen, "CsPI: A new way to evaluate cybersecurity investments: A position paper," in *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 283–284, IEEE.
- [172] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, and J. Woodill, "Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods," MITRE TECHNICAL REPORT MTR180314, MITRE, Bedford, MA, Sept. 2018.
- [173] O. Altuhhova, R. Matulevičius, and N. Ahmed, "Towards definition of secure business processes," in *Advanced Information Systems Engineering Workshops* (M. Bajec and J. Eder, eds.), vol. 112, pp. 1–15, Springer Berlin Heidelberg. Series Title: Lecture Notes in Business Information Processing.
- [174] M. Ekstedt, T. Sommestad, H. Holm, and L. NordstrM, "CySeMoL: A tool for cyber security analysis of enterprises," in *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*, pp. 1109–1109, Institution of Engineering and Technology.
- [175] R. Matulevicius, P. Heymans, and A. L. Opdahl, "Ontological Analysis of KAOS Using Separation of Reference," in *Proceedings of the Workshop of Exploring Modeling Methods for Systems Analysis and Design (EMMSAD'06)*, (Namus University), pp. 395–406, 2006.
- [176] F. Zickert, "Evaluation of the Goal-Oriented Requirements Engineering Method KAOS," in *AMCIS 2010 Proceedings*, (Lima, Peru), Aug. 2010.
- [177] J. Whittle, D. Wijesekera, and M. Hartong, "Executable misuse cases for modeling security concerns," in *Proceedings of the 13th international conference on Software engineering - ICSE '08*, p. 121, ACM Press.
- [178] T. Lodderstedt, D. Basin, and J. Doser, "SecureUML: A UML-based modeling language for model-driven security," in *UML 2002 — The Unified Modeling Language* (J.-M. Jézéquel, H. Hussmann, and S. Cook, eds.), vol. 2460, pp. 426–441, Springer Berlin Heidelberg. Series Title: Lecture Notes in Computer Science.
- [179] M. Seidl, M. Scholz, C. Huemer, and G. Kappel, *The State Machine Diagram*, pp. 85–106. Springer International Publishing. Series Title: Undergraduate Topics in Computer Science.
- [180] J. Jürjens, "UMLsec: Extending UML for secure systems development," in *UML 2002 — The Unified Modeling Language* (J.-M. Jézéquel, H. Hussmann, and S. Cook, eds.), vol. 2460, pp. 412–425, Springer Berlin Heidelberg. Series Title: Lecture Notes in Computer Science.

- [181] R. F. Babiceanu and R. Seker, "Cybersecurity and resilience modelling for software-defined networks-based manufacturing applications," in *Service Orientation in Holonic and Multi-Agent Manufacturing* (T. Borangiu, D. Trentesaux, A. Thomas, P. Leitão, and J. B. Oliveira, eds.), vol. 694, pp. 167–176, Springer International Publishing. Series Title: Studies in Computational Intelligence.
- [182] V. Chapurlat, N. Daclin, A. Bony-Dandrieux, J. Tixier, D. Kamissoko, F. Benaben, and B. Nastov, "Towards a model-based method for resilient critical infrastructure engineering how to model critical infrastructures and evaluate its resilience? : How to model critical infrastructures and evaluate its resilience?," in *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, pp. 561–567, IEEE.
- [183] I. Häring, S. Ebenhöch, and A. Stolz, "Quantifying resilience for resilience engineering of socio technical systems," vol. 1, no. 1, pp. 21–58.
- [184] R. Darimont, E. Delor, P. Massonet, and A. van Lamsweerde, "GRAIL/KAOS: An Environment for Goal-Driven RequirementsEngineering," in *Proceedings of the 1997 International Conference on Software Engineering: May 17 - 23, 1997, Boston, Massachusetts, USA* (I. C. on Software Engineering, I. C. Society, and A. for Computing Machinery, eds.), pp. 612 – 613, Los Alamitos, Calif.: IEEE Computer Society Press, 1997. Meeting Name: International Conference on Software Engineering (ICSE) OCLC: 833109465.
- [185] I. Alexander, "Misuse cases: use cases with hostile intent," *IEEE Software*, vol. 20, pp. 58–66, Jan. 2003.
- [186] J. Whittle, D. Wijesekera, and M. Hartong, "Executable Misuse Cases for Modeling Security Concerns," in *2008 30th International Conference on Software Engineering: ICSE ; Leipzig, Germany, 10 - 18 May 2008* (A. for Computing Machinery and I. C. Society, eds.), pp. 121–130, Piscataway, NJ: IEEE, 2008. Meeting Name: International Conference on Software Engineering.
- [187] G. Sindre, "A Look at Misuse Cases for Safety Concerns," in *Situational Method Engineering: Fundamentals and Experiences* (J. Ralyté, S. Brinkkemper, and B. Henderson-Sellers, eds.), vol. 244, pp. 252–266, Boston, MA: Springer US, 2007. Series Title: IFIP — The International Federation for Information Processing.
- [188] R. Matulevicius, H. Mouratidis, N. Mayer, E. Dubois, and P. Heymans, "Syntactic and semantic extensions to secure tropos to support security risk management," *Journal of Universal Computer Science*, vol. 18, no. 6, pp. 816–844, 2012.
- [189] M. Pavlidis, H. Mouratidis, E. Panaousis, and N. Argyropoulos, "Selecting Security Mechanisms in Secure Tropos," in *Trust, Privacy and Security in Digital Business* (J. Lopez, S. Fischer-Hübner, and C. Lambrinouidakis, eds.), vol. 10442, pp. 99–114, Cham: Springer International Publishing, 2017.
- [190] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt, "P² CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, pp. 626–639, Nov. 2015.
- [191] T. Sommestad, M. Ekstedt, and H. Holm, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures," *IEEE Systems Journal*, vol. 7, pp. 363–373, Sept. 2013.
- [192] Y. Asnar and P. Giorgini, "Modelling Risk and Identifying Countermeasure in Organizations," 2006.

- [193] D. L. Moody, P. Heymans, and R. Matulevicius, "Improving the Effectiveness of Visual Representations in Requirements Engineering: An Evaluation of i* Visual Syntax," in *2009 17th IEEE International Requirements Engineering Conference*, (Atlanta, Georgia, USA), pp. 171–180, IEEE, Aug. 2009.
- [194] A. L. Opdahl and B. Henderson-Sellers, "A Unified Modelling Language without referential redundancy," *Data & Knowledge Engineering*, vol. 55, pp. 277–300, Dec. 2005.
- [195] D. Moody, "What Makes a Good Diagram? Improving the Cognitive Effectiveness of Diagrams in IS Development," in *Advances in Information Systems Development* (W. Wojtkowski, W. G. Wojtkowski, J. Zupancic, G. Magyar, and G. Knapp, eds.), pp. 481–492, Boston, MA: Springer US, 2007.
- [196] O. Foundation, "Electron."
- [197] Microsoft, "Blazor."
- [198] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empirical Software Engineering*, vol. 14, pp. 131–164, Apr. 2009.
- [199] S. Baškarada, "Qualitative case studies guidelines," vol. 19, no. 40, pp. 1–25.
- [200] B. Kitchenham, "DESMET: A method for evaluating software engineering methods and tools."
- [201] S. Easterbrook, J. Singer, M.-A. Storey, and D. Damian, "Chapter 11 selecting empirical methods for software engineering research," in *Guide to Advanced Empirical Software Engineering*, pp. 285–311.
- [202] M. Zelkowitz and D. Wallace, "Experimental models for validating technology," vol. 31, no. 5, pp. 23–31.
- [203] G. G. Gable, "Integrating case study and survey research methods: an example in information systems," *European Journal of Information Systems*, vol. 3, no. 2, pp. 112–126, 1994.
- [204] B. A. Kitchenham, S. L. Pfleeger, L. M. Pickard, P. W. Jones, D. C. Hoaglin, K. El-Emam, and J. Rosenberg, "Preliminary guidelines for empirical research in software engineering."
- [205] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*. Springer Berlin Heidelberg.
- [206] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, "On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces," (Bellevue, WA), pp. 143–158, Aug. 2012.
- [207] R. Murphy, "Human–robot interaction in rescue robotics," vol. 34, no. 2, pp. 138–153.
- [208] P. S. Schenker, "NASA research and development for space telerobotics," vol. 24, no. 5, pp. 523–534.
- [209] M. Lum, D. Trimble, J. Rosen, K. Fodero, H. King, G. Sankaranarayanan, J. Doshier, R. Leuschke, B. Martin-Anderson, M. Sinanan, and B. Hannaford, "Multidisciplinary approach for developing a new minimally invasive surgical robotic system," in *The First IEEE/RAS-EMBS International Conference on Biomedical Robotics and Biomechatronics, 2006. BioRob 2006.*, pp. 841–846, IEEE.

- [210] J. R. Wolpaw, N. Birbaumer, D. J. McFarland, G. Pfurtscheller, and T. M. Vaughan, "Brain-computer interfaces for communication and control," vol. 113, pp. 767–791.
- [211] G. Raphael, A. Behneman, V. Tan, N. Pojman, and C. Berka, "Interactive neuro-educational technologies (i-NET): Development of a novel platform for neurogaming," in *Foundations of Augmented Cognition. Directing the Future of Adaptive Systems* (D. D. Schmorrow and C. M. Fidopiastis, eds.), vol. 6780, pp. 452–461, Springer Berlin Heidelberg. Series Title: Lecture Notes in Computer Science.
- [212] A. Kaklauskas, E. Zavadskas, A. Banaitis, I. Meidute-Kavaliauskiene, A. Liberman, S. Dzitic, I. Ubarte, A. Binkyte, J. Cerkauskas, A. Kuzminske, and A. Naumcik, "A neuro-advertising property video recommendation system," vol. 131, pp. 78–93.
- [213] A. M. Jacobs, "Sentiment analysis for words and fiction characters from the perspective of computational (neuro-)poetics," vol. 6, p. 53.
- [214] M. Inzlicht, I. McGregor, J. B. Hirsh, and K. Nash, "Neural markers of religious conviction," vol. 20, no. 3, pp. 385–392.
- [215] J. P. Rosenfeld, J. R. Biroshak, and J. J. Furedy, "P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms," vol. 60, no. 3, pp. 251–259.
- [216] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: security and privacy for neural devices," vol. 27, no. 1, p. E7.
- [217] T. Bonaci, R. Calo, and H. J. Chizeck, "App stores for the brain: Privacy & security in Brain-Computer Interfaces," pp. 1–7, IEEE, May 2014.
- [218] M. J. Lum, D. C. Friedman, G. Sankaranarayanan, H. King, A. Wright, M. Sinanan, T. Lendvay, J. Rosen, and B. Hannaford, "Objective assessment of telesurgical robot systems: Telerobotic FLS," pp. 132:263–5.
- [219] M. Lum, J. Rosen, T. Lendvay, M. Sinanan, and B. Hannaford, "Effect of time delay on telesurgical performance," in *2009 IEEE International Conference on Robotics and Automation*, pp. 4246–4252, IEEE.
- [220] N. Falliere, L. O Murchu, and E. Chien, "W32.stuxnet dossier."
- [221] G. S. Lee and B. Thuraingham, "Cyberphysical systems security applied to telesurgical robotics," *Computer Standards & Interfaces*, vol. 34, pp. 225–229, Jan. 2012.
- [222] M. E. Tozal, Y. Wang, E. Al-Shaer, K. Sarac, B. Thuraingham, and B.-T. Chu, "Adaptive information coding for secure and reliable wireless telesurgery communications," vol. 18, no. 5, pp. 697–711.
- [223] K. Coble, W. Wang, B. Chu, and Z. Li, "Secure software attestation for military telesurgical robot systems," in *MILCOM 2010 Milcom 2010 Military Communications Conference*, pp. 1817 – 1822, IEEE.
- [224] S. Iqbal, S. Farooq, K. Shahzad, A. W. Malik, M. M. Hamayun, and O. Hasan, "SecureSurgiNET: A framework for ensuring security in telesurgery," vol. 15, no. 9, p. 155014771987381.
- [225] M. Lum, D. C. W. Friedman, H. King, T. Broderick, M. Sinanan, J. Rosen, and B. Hannaford, "Field operation of a surgical robot via airborne wireless radio link," in *Proceedings of the IEEE International Conference on Field and Service Robotics*, p. 7, IEEE.

- [226] J. M. Thompson, M. P. Ottensmeyer, and T. B. Sheridan, "Human factors in telesurgery: Effects of time delay and asynchrony in video and control feedback with local manipulative assistance," vol. 5, no. 2, pp. 129–137.
- [227] Y. E. Simon, H. Jin B., G. Mengmeng, and K. Dong Seong, "Composite metrics for network security analysis," vol. 1, pp. 137–160.
- [228] M. Almulhim, N. Islam, and N. Zaman, "A lightweight and secure authentication scheme for IoT based e-health applications," vol. 19, no. 1, pp. 107–120.
- [229] H. King, K. Tadano, R. Donlin, D. Friedman, M. Lum, V. Asch, C. Wang, K. Kawashima, and B. Hannaford, "Preliminary protocol for interoperable telesurgery," in *2009 International Conference on Advanced Robotics*, pp. 1–6, IEEE.
- [230] S. Safavi and Z. Shukur, "Improving google glass security and privacy by changing the physical and software structure," vol. 11, no. 5, pp. 109 – 117.
- [231] P. Chan, T. Halevi, and N. Memon, "Glass OTP: Secure and convenient user authentication on google glass," in *Financial Cryptography and Data Security* (M. Brenner, N. Christin, B. Johnson, and K. Rohloff, eds.), vol. 8976, pp. 298–308, Springer Berlin Heidelberg. Series Title: Lecture Notes in Computer Science.
- [232] "The european code of conduct for research integrity."
- [233] C. Zaboeva and M. Frydrych, "IBM uncovers global phishing campaign targeting the COVID-19 vaccine cold chain."
- [234] Z. Kleinman, "How will we keep the covid vaccine at a cold enough temperature?,"
- [235] S. Houmb, G. Georg, R. France, J. Bieman, and J. Jurjens, "Cost-benefit trade-off analysis using BBN for aspect-oriented risk-driven development," in *10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'05)*, pp. 195–204, IEEE.
- [236] "An integrated security verification and security solution design trade-off analysis approach," in *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (H. Nemati, ed.), p. 25, IGI Global.
- [237] G. Sindre, "Mal-activity diagrams for capturing attacks on business processes," in *Requirements Engineering: Foundation for Software Quality* (P. Sawyer, B. Paech, and P. Heymans, eds.), vol. 4542, pp. 355–366, Springer Berlin Heidelberg. Series Title: Lecture Notes in Computer Science.
- [238] E. Farzadnia, H. Shirazi, and A. Nowroozi, "A novel sophisticated hybrid method for intrusion detection using the artificial immune system," vol. 58, p. 102721.

Appendix A

Literature extracted definitions for healthcare cyber resiliency constructs

A.0.1 Cyber resiliency standards

NIST SP 800-184 [6, p. 4] perceives enterprise resiliency as: **Enterprise Resiliency** *ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions...throughout the enterprise security lifecycle* [6, p. 4].

The NIST SP 800-61r2 [4, p. 60] suggests a definition for the term Incident Response that is considered synonymous to Incident Handling. **Incident Response** *The mitigation of violations of security policies and recommended practices* [4, p. 60]. Whereas an Incident also called Computer Security Incident stands for: **Incident** *A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices* [4, p. 60]. In contrast with an Incident the term Event means: **Event** *Any observable occurrence in a network or system* [4, p. 60].

A.0.2 Cybersecurity standards

ISO/TR 22100-4:2018 [140], does not define resilience separately from cybersecurity, but as part of its context: **Cybersecurity** *protection of an IT-system from the attack or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides* [140]. The examination of this interpretation of cybersecurity is indicating a risk management approach as it connects cause and effect. Furthermore, this definition requires clarification of the meaning of the concepts of attack and damage. It does define attack: **Attack** *attempt to gain unauthorized access to system services, resources, or information* [140]. An Attack is differently defined compared to an IT-Security Incident and a Threat, which are defined respectively as: **IT-Security Incident** *occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IT-system attack* [140]. **Threat** *any IT-security incident with the potential to adversely impact machinery operations vulnerability weakness in the security of an IT-system that can be exploited or triggered by a threat* [140]. However, it does not provide a definition for the term damage.

NIST SP 800-82r2 [141] distinguishes the terms attack, threat and incident. An attack stands for: **Attack** *An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.* [141, p. B-1]. However, a threat does not necessarily involve a violation of at least one security property. Instead, it

relates to an occurrence that can have a negative impact. **Threat** *Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.* [141, p. B-17]. A threat initiates from a threat event and has a threat source. **Threat Event** *An event or situation that has the potential for causing undesirable consequences or impact.* [141, p. B-17]. **Threat Source** *The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent.* [141, p. B-17]. The same standard defines an incident as: **Incident** *An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies* [141, p. B-8].

For attacks, threats and incidents to occur, there needs to be at list one exploitable vulnerability, which stands for: **Vulnerability** *Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.* [141, p. B-18]. For the protection of vulnerabilities, security and technical controls are introduced to a system. **Security Controls** *The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.* [141, p. B-14]. **Technical Controls** *The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.* [141, p. B-16]. The introduction of security controls takes place following a security plan. **Security Plan** *Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.* [141, p. B-15]. When a system operates, as usual, it is at a steady-state. **Steady State** *A characteristic of a condition, such as value, rate, periodicity, or amplitude, exhibiting only negligible change over an arbitrarily long period of time.* [141, p. B-16].

NIST SP 800-160v1 [142] defines security as: **Security** *Freedom from those conditions that can cause loss of assets with unacceptable consequences.* [142, p. 171]. In general a consequence is: **Consequence** *Effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system.* [142, p. 167]. An unacceptable consequence relates to an adverse consequence that is perceived as: **Adverse Consequence** *An undesirable consequence associated with a loss.* [142, p. 164].

An event is defined differently from an incident. **Event** *Occurrence or change of a particular set of circumstances.* [142, p. 168]. **Incident** *Anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system.* [142, p. 168]. Events and incidents except from having a consequence they also have a probability of occurrence, named likelihood. **Likelihood** *Chance of something happening.* [142, p. 168]. An event can be a threat based on the consequences it can have. **Threat** *An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.* [142, p. 175]. If threats result from the presence of at least one vulnerability. **Vulnerability** *Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.* [142, p. 176]. All these types of occurrence (event, incident, threat) happen within an environment. **Environment (system)** *Context determining the setting and circumstances of all influences upon a system.* [142, p. 168].

Security, as mentioned above, aims to protect assets. **Asset** *An item of value to achievement of organizational mission/business objectives.* [142, p. 165]. Different assets have a variable criticality that relates to their importance in relation to the achievement of a mission/business

objective/goal. **Criticality** *An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals.* [142, p. 167].

To do so, security forms constraints in relation to missions, objectives and/or goals. **Constraints** *Factors that impose restrictions and limitations on the system or actual limitations associated with the use of the system.* [142, p. 167]. These constraints have the form of requirements. **Requirement** *Statement that translates or expresses a need and its associated constraints and conditions. A condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification, or other formally imposed documents.* [142, p. 170]. It is in particular a security requirement, within the cybersecurity context. **Security Requirement** *A requirement that specifies the functional, assurance, and strength characteristics for a mechanism, system, or system element.* [142, p. 172]. Security requirements can be met at a design level with security controls and at an implementational level with security mechanisms. **Security Control** *A mechanism designed to address needs as specified by a set of security requirements.* [142, p. 171]. **Security Mechanism** *A method, tool, or procedure that is the realization of security requirements.* [142, p. 172].

ISO/IEC 27001:2013 [143] centres around information technology. It defines an information system as: **Information System** *Set of applications, services, information technology assets, or other information-handling components.* [143]. Such systems have objectives that try to achieve. **Objective** *Result to be achieved.* [143]. The persuasion of objectives takes place within a certain context which has external and internal aspects. **External Context** *External environment in which the organization seeks to achieve its objectives.* [143]. **Internal Context** *Internal environment in which the organization seeks to achieve its objectives.* [143].

The expectations from a system take the form of requirements. **Requirement** *Need or expectation that is stated, generally implied or obligatory.* [143]. Based on the system's behaviour requirements are either satisfied or not. **conformity** *fulfilment of a requirement* [143]. **nonconformity** *Non-fulfilment of a requirement.* [143].

Within the context of information security these requirements take the form of security properties. This is reflected in the information security's definition: **Information Security** *Preservation of confidentiality, integrity and availability of information.* [143]. However, security is enhanced with the definition of security continuation. **Information Security Continuity** *Processes and procedures for ensuring continued information security operations.* [143]. Security continuation is important in the presence of incidents that security needs to manage. **Information Security Incident Management** *Set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.* [143].

ISO/IEC 27001:2013 [143] distinguishes treats from attacks, events, security events, incidents and security incidents defining them as follows: **Attack** *Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.* [143]. **Event** *Occurrence or change of a particular set of circumstances. Note 1 to entry: An event can be one or more occurrences, and can have several causes. Note 2 to entry: An event can consist of something not happening. Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".* [143]. **Information Security Event** *Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.* [143]. **Information Security Incident** *Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.* [143]. **Threat** *Potential cause of an unwanted incident, which can result in harm to a system or organization.* [143]. Threats exploit vulnerabilities that are interpreted as: **Vulnerability** *Weakness of an asset or control that can be exploited by one or more threats.* [143].

The constructs of consequence and likelihood characterise these types of occurrences. **Con-**

sequence *Outcome of an event affecting objectives.*

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and, in the context of information security, is usually negative.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects. [143]. **Likelihood** *Chance of something happening. [143].*

ISO/IEC 27032:2012 [144] is concerned with the cyberspace. **Cyberspace** *Complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. [144].* Cyberspace is associated with cybersecurity and also cybersafety. Cybersecurity once more relates to security properties whereas cybersafety covers all the other types of properties. This can be seen clearer through their definitions: **Cybersecurity** *Preservation of confidentiality, integrity and availability of information in the cyberspace. [144].* **Cybersafety** *Condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable. [144].*

Within the cyberspace, there are different types of assets, namely information, physical and virtual. A particular type of assets that are relevant to cybersecurity and cybersafety are named controls. The term asset and its sub-concepts are defined below: **Asset** *Anything that has value to an individual, an organization or a government. [144].* **Information Asset** *Knowledge or data that has value to the individual or organization. [144].* **Physical Asset** *Asset that has a tangible or material existence. [144].* **Virtual Asset** *Representation of an asset in the cyberspace. [144].* When an asset is introduced to safeguard other assets from unwanted events it is called control. **Control** *Countermeasure means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature. [144].*

Nevertheless, assets and controls have vulnerabilities that can cause unwanted occurrences. **Vulnerability** *Weakness of an asset or control that can be exploited by a threat. [144].* A vulnerability is necessary for threats to occur. **Threat** *Potential cause of an unwanted incident, which may result in harm to a system, individual or organization. [144].* When such a cause is intentional it is referred as attack. **Attack** *Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. [144].* Every attack has a probability to occur and achieve its purpose. These two attack properties are captured with the use of the term attack potential. **Attack Potential** *Perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation. [144].* Attack initiators use various techniques to pursue their purposes and these different avenues that lead to a malicious occurrence are named as attack vectors. **Attack Vector** *Path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome. [144].*

A.0.3 Health-related standards

ISO 27799:2016 [146] emphasises on healthcare that is defined as: **Healthcare** *Type of services provided by professionals or paraprofessionals with an impact on health status. [146].* For healthcare provision, different types of systems are used. ISO 27799:2016 focuses on information systems used within the healthcare environment and names them health information systems. **Health Information System** *Repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users. [146].* The healthcare environment within which these systems operate is a healthcare organisation

that stands for: **Healthcare Organisation** *Organization that provides healthcare services.* [146].

The provision of healthcare services is the ultimate objective of healthcare organisations and systems. Healthcare objectives achievement involves specific for the healthcare context types of actors. Namely the healthcare professional, the subject of care and the patient, that have the following definitions: **Healthcare Professional** *Person who is authorised by a recognised body to be qualified to perform certain health duties.* [146]. **Subject of Care** *One or more persons scheduled to receive, receiving, or having received a health service.* [146]. **Patient** *Subject of care consisting of one person.* [146].

NIST SP 800-66r1 [147] has a Health Insurance Portability and Accountability Act (HIPAA) orientation approaching it from an implementational point of view. It emphasises information systems, regarded as: **Information System** *An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.* [147, p. A-5]. Correspondingly the same standard limits security to the context of information systems: **Security** *Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:*

(A) *integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;*

(B) *confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and*

(C) *availability, which means ensuring timely and reliable access to and use of information.* [147, p. A-6].

For security attainment, NIST SP 800-66r1 distinguishes three types of safeguards: administrative, physical and technical. Below are their definitions: **Administrative Safeguards** *Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.* [147, p. A-1]. **Physical Safeguards** *Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.* [147, p. A-5]. **Technical Safeguards** *The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.* [147, p. A-6].

A.0.4 Cyber resiliency frameworks

MTR140499R1 [7] updates and guides the application of a CRE framework that focuses at a system level, where a system is: **System** *A set of interacting or interdependent parts forming an integrated whole; any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions... The term "system" typically includes people and organizational processes as well as technology; among those who use the term more restrictively, to include only technology, the term "socio-technical system" is used to refer to the combination of technology, people, and processes.* [7, p. 13]. A system consists of components. **Component** *A part of a system that can be replaced or managed separately from other parts of the system. Examples of components include hardware devices, embedded devices (e.g., sensors, controllers, medical devices such as pacemakers, vehicle automation such as collision avoidance), desktop or laptop computers, servers, routers, firewalls, virtual machine monitors (VMMs) or hypervisors, operating systems (OSs), applications, and databases. When "system" is construed as a socio-technical system, examples also include people and separately managed processes.* [7, p. 12].

Two more terms need to be defined, to understand better the definition of a system. These terms are the resource and the process. **Resource** *A component of, or a service or capability provided by, a system, which can be used by multiple mission/business functions. General examples include bandwidth, processing, and storage. Other examples are more system- or mission/business process-specific, and can include information resources (e.g., data of a specified quality) as well as computing or networking services subject to service-level agreements (SLAs).* [7, p. 12-13]. **Process** *A structured set of activities within an organization. Note that this usage does not refer to a computing process, i.e., to a running instance of a program. A process can be supported by tools.* [7, p. 12]. To clarify the term process, we need the meaning of the construct tool, that is: **Tool** *A technology or type of technology that can be used to perform some function (e.g., implement an approach or technique). While specific products could be identified as examples of tools, such identification can quickly be outdated; therefore, the following table identifies classes of products.* [7, p. 13].

Every system is part of an organisation to support the achievement of a mission/business function: **Mission/Business Function** *An activity, process, or set of related activities or processes intended to achieve a mission or business objective.* [7, p. 12]. However, as systems offer business functions, they also form a vulnerable surface that attackers can target. **Attack Surface** *The set of resources and vulnerabilities that are exposed to potential attack.* [7, p. 12]. The presence of an attack surface can lead to the occurrence of adverse cyber events for an organisation. **Adverse Cyber Event** *An event involving cyber resources that has adverse consequences for cyber resources. Adverse cyber events include, but are not limited to, cyber attacks.* [7, p. 12].

An organisation in response to adverse cyber events, employees a range of Tactics, Techniques, and Procedures (TTPs): **Tactics, Techniques, and Procedures (TTPs)** *The use of capabilities and resources in relation to each other (tactics); non-prescriptive ways or methods used to perform missions, functions, or tasks (techniques); and standard, detailed steps that prescribe how to perform specific tasks (procedures).* [7, p. 13]. Such activities form an organisational defensive Cyber Course of Action (CCoA) that consists of: **Defensive Cyber Course of Action (CCoA)** *A set of activities or TTPs employed by automation, cyber defenders (...) and, as needed, other cyber staff (...) and mission staff in response to adverse cyber events.* [7, p. 12].

In MTR110237 [8] resiliency is defined within the cyberspace that stands for: **Cyberspace** *The collection of Information and Communications Technology (ICT) infrastructures, applications, and devices on which the organization, enterprise, or mission depends, typically including the Internet, telecommunications networks, computer systems, personal devices, and (when networked with other ICT) embedded sensors, processors, and controllers.* [8, p. 7]. The cyberspace consists of cyber resources that are: **Cyber Resources** *Separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, infrastructures, shared services, and devices.* [8, p. 7]. Cyber resources are subject to cyber attacks that do not necessarily originate from the cyberspace. A cyber attack is: **Cyber Attack** *An attack on cyber resources. The attack is typically, but not necessarily, carried out by cyber means. The attack may be intended to adversely affect the cyber resources, or to adversely affect the missions, business functions, organizations, or populations that depend on those resources.* [8, p. 7].

The meaning of resiliency within the cyberspace captures the term cyber resiliency. **Cyber Resiliency** *The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function.* [8, p. 8]. These two fundamental terms and their definitions make clear that the scope of cyber resilience can vary. The variations fall under one of the two categories, the top-down or the bottom-up. If cyber resiliency follows a top-down approach it is considered at national or local level and involves governmental participation [63][64][66][74]. If cyber resiliency follows a bottom-up approach, then it is analysed at an organisational level and involves internal and external stakeholders [65].

In order for a nation, organisation or business function to have cyber resiliency ability, cyber resiliency engineering takes place. **Cyber Resiliency Engineering** *The sub-discipline of mission assurance engineering which considers (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for applying those practices.* [8, p. 8]. This definition provides the two main activities that take place in Cyber Resiliency Engineering (CRE), the design of alternative cyber resiliency plans and the assessment of their substitution and applicability.

Citation	Level	Artefact	Eval./Val. method	Ability	Continuation	Intended Outcomes	Adverse cyber event	Challenges
[125]	by-design	agile and resilient embedded systems (ARES) methodology and metric set	benchmark and flight tests	embedded cyberphysical systems	mitigation of threats that security cannot alleviate	mission assurance	any cause of loss of mission essential functions	further refinement, validation, application and automation
[126]	run-time	self-healing cyber resilient framework	simulation	network	self-healing	automated management	cyber attacks	extent to specific network types
[127]	by-design	SecUre and REsilient Cyber-Physical Systems (SURE) platform	three case studies	cyberphysical system	monitoring, control	resilience evaluation	cyber attacks	empirical research
[128]	life cycle	business continuity and disaster recovery planning (IBCDRP) model	case study	organisation (critical functions, resources)	continuity, resumption, restoration	evaluation of strategic and tactical decisions	natural and man-made hazards (simultaneous and sequential)	management of interdependent events
[129]	run-time	framework for resilient mission critical systems	tests	stateful applications	moving target defence, availability	mission survivability	anomalies	distinguish and analyse anomalies at run-time
[130]	by-design	manufacturing testbed, cybersecurity-resilience ontology and framework	N/A	system	return to nominal performance after an acceptable period, restoration	maintain the system in its required state of security	security breach	interoperability of cyber manufacturing environment
[131]	run-time	method for modelling the impact of cyber attacks	examples and experiments	network	threat assessment, justification of requirements	assess cyber resilience	cyber attacks	concurrent and unknown attacks modelling
[132]	run-time	modelling and assessment approach	case study	Bayesian network	absorption, adaptation, restoration	risk assessment	diverge range of risks (natural, cyber, human)	improve accuracy
[133]	run-time	architecture for resilience enhancement	case study	physical, network, and application	reliability and operational normalcy	disturbances, including attacks	vulnerabilities and potential physical and cyber attacks	implementation difficulty
[134]	run-time	dynamic medical risk assessment model	case study	Bayesian network	safety measures assignment and adaptation	risk assessment	failures, repairs, and human errors	model healthcare complexity
[135]	life cycle	methodology for quantifying and mapping resilience	interviews, literature review, case study	physical, information, cognitive, social	plan, absorb, adapt	assess organisational resilience (missions, capabilities)	uncertain future events	limited ability to incorporate novel, resilience strategies
[136]	preparation	framework of cyber resilient behaviour	survey and pilot study	human behaviour	anticipate, monitor, and learn	organisational needs related to human aspect of cyber resilience	cyber attacks	link behaviour change interventions to resilient behaviour of employees

Appendix B

Alignment table of cyber resiliency concepts

event = any observable occurrence in a system or network
event = any observable occurrence in a system or network

-

threat event = An event or situation that has the potential for causing undesirable consequences or impact. disturbance = An undesired change in a variable being applied to a system that tends to adversely affect the value of a controlled variable.

event = Occurrence or change of a particular set of circumstances.

event = occurrence or change of a particular set of circumstances Note 1 to entry: An event can be one or more occurrences, and can have several causes. Note 2 to entry: An event can consist of something not happening. Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident". information security event = identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that can be security relevant

-

-

adverse cyber event = An event involving cyber resources that has adverse consequences for cyber resources. Adverse cyber events include, but are not limited to, cyber attacks.

Adverse conditions and stresses = include not only the faults, errors, surges in demand, and failures of supporting infrastructures (e.g., power loss due to natural disaster) considered in contingency planning, but also adversary activities that have not risen to the level of an attack (e.g., reconnaissance).

incident = a violation of acceptable policies, or security policies and best practices

incident = A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

IT-security incident = occurrence that actually or potentially jeopardises the confidentiality, integrity, or availability of an IT-system

incident = An occurrence that actually or potentially jeopardises the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

Table B.1: Aggregation of treatments by publication year (continuation)

Type	Concept	Cyber resiliency standards				Cybersecurity standards			
		NIST SP 800-184	NIST SP 800-61r2	ISO/TR 22100-4:2018	NIST SP 800-82r2	NIST SP 800-160v1	ISO/IEC 27001:2013	ISO/IEC 27032:2012	
	event	event	event	-	threat event	event	event	-	
	incident	incident cyber event	incident cyber event computer security incident	disturbance IT-security incident	incident	information security event incident	information security incident	-	
	recover	recover	-	-	-	-	-	-	
	CIRP	CIRP	CIRP	-	-	-	-	-	
	resilience	resilience	-	-	-	-	information security continuity	-	
	asset	asset	-	-	-	asset	-	cybersafety asset information asset physical asset virtual asset	
	CIRT	-	CSIRT CIRC	-	-	-	-	-	
	incident response	-	incident response incident handling	-	-	-	-	-	
	indicator	-	indicator	-	-	-	-	-	
	precursor	-	precursor	-	-	-	-	-	
	threat	-	threat	threat	threat	threat	threat	threat	
	vulnerability	-	vulnerability	vulnerability	vulnerability	vulnerability	vulnerability	vulnerability	
	attack	-	-	attack	attack	-	attack	attack	
	measure	-	-	risk reduction measure protective measure	-	mechanism security mechanism	measure risk treatment	-	
	security control	-	-	-	security control technical control operational control	security control	-	control	
	threat source	-	-	-	threat source	-	-	-	
	domain	-	-	-	domain security domain system context	environment (system) internal context	external context	-	
	risk	-	-	-	risk	risk	risk	-	
	impact	-	-	-	-	adverse consequence consequence	residual risk consequence	-	
	constraints	-	-	-	-	constraints	-	-	
	cyber-physical system	-	-	-	-	cyber-physical system	-	-	
	evidence	-	-	-	-	evidence	-	-	
	likelihood	-	-	-	-	likelihood	likelihood	attack potential	
	requirement	-	-	-	-	requirement security requirement system security requirement	requirement	-	
	objective	-	-	-	-	-	objective	-	
	subject of care	-	-	-	-	-	-	-	

incident = Anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system.

information security incident = single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

cyber event = a specific cybersecurity incident or set of related cybersecurity incidents that result in the successful compromise of one or more information systems

cyber event = a specific cybersecurity incident or set of related cybersecurity incidents that result in the successful compromise of one or more information systems

recover = the development and implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event.

-

CIRP = establish procedures to address cyber attacks against an organisation's information system(s).

CIRP = establish procedures to address cyber attacks against an organisation's information system(s).

resilience = ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.

-

-

-

-

information security continuity = processes and procedures for ensuring continued information security operations

cybersafety = condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable Note 1 to entry: This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protection of people or of assets. Note 2 to entry: Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions.

-

-

-

cyber resiliency = The ability of a nation, organisation, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function.

asset = enable the governance, management, and use of IT to accomplish the enterprise mission... people, process, and technology assets, and the assets of external partners that are connected to or associated with enterprise resources. (unavailable or reduced capability)

-

-

-

asset = An item of value to achievement of organisational mission/business objectives. Note 1:

Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organisational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organisation. Note 2: An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation).

asset = anything that has value to an individual, an organisation or a government. information asset = information asset physical asset = asset that has a tangible or material existence Note 1 to entry: Physical assets usually refer to cash, equipment, inventory and properties owned by the individual or organisation. Software is considered an intangible asset, or a non-physical asset. virtual asset = representation of an asset in the Cyberspace Note 1 to entry: In this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise.

-
-

resource = A component of, or a service or capability provided by, a system, which can be used by multiple mission / business functions. General examples include bandwidth, processing, and storage. Other examples are more system- or mission/business process-specific, and can include information resources (e.g., data of a specified quality) as well as computing or networking services subject to service-level agreements (SLAs).

cyber resource = Separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, infrastructures, shared services, and devices.

-

incident response = The mitigation of violations of security policies and recommended practices. -

-
-
-
-
-
-

CCoA = A set of activities or tactics, techniques, and procedures (TTPs) employed by automation, cyber defenders (e.g., CND staff; staff in a Security Operations Center or a Cyber Security Operations Center) and, as needed, other cyber staff (e.g., staff in a Cyber Operations Center, system administrators, network operators) and mission staff in response to adverse cyber events.

-

-

indicator = A sign that an incident may have occurred or may be currently occurring.

-

precursor = A sign that an attacker may be preparing to cause an incident.

-

threat = The potential source of an adverse event.

threat = any IT-security incident with the potential to adversely impact machinery operations

threat = Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

threat = An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Note: The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions.

threat = potential cause of an unwanted incident, which can result in harm to a system or organisation.

threat = potential cause of an unwanted incident, which may result in harm to a system, individual or organisation.

-

vulnerability = A weakness in a system, application, or network that is subject to exploitation or misuse.

vulnerability = weakness in the security of an IT-system that can be exploited or triggered by a threat.

vulnerability = Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

vulnerability = Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

vulnerability = weakness of an asset or control that can be exploited by one or more threats.

vulnerability = weakness of an asset or control that can be exploited by a threat

-

-

attack = attempt to gain unauthorised access to system services, resources, or information

attack = An attempt to gain unauthorised access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

-

attack = attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset

attack = attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset

-

-

-

cyber attack = An attack on cyber resources. The attack is typically, but not necessarily, carried out by cyber means. The attack may be intended to adversely affect the cyber resources, or to adversely affect the missions, business functions, organisations, or populations that depend on those resources.

-

-
risk reduction measure/protective measure = action or means to eliminate hazards or reduce risks

-
mechanism = A process or system that is used to produce a particular result. The fundamental processes involved in or responsible for an action, reaction, or other natural phenomenon. A natural or established process by which something takes place or is brought about. Refer to security mechanism. Note: A mechanism can be technology- or nontechnology-based (e.g., apparatus, device, instrument, procedure, process, system, operation, method, technique, means, or medium). security mechanism = A method, tool, or procedure that is the realisation of security requirements. Note 1: A security mechanism exists in machine, technology, human, and physical forms. Note 2: A security mechanism reflects security and trust principles. Note 3: A security mechanism may enforce security policy and therefore must have capabilities consistent with the intent of the security policy.

measure = variable to which a value is assigned as the result of measurement. risk treatment = process (3.54) to modify risk (3.61) Note 1 to entry: Risk treatment can involve: — avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — taking or increasing risk in order to pursue an opportunity; — removing the risk source; — changing the likelihood (3.40); — changing the consequences (3.12); — sharing the risk with another party or parties (including contracts and risk financing); — retaining the risk by informed choice. Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. Note 3 to entry: Risk treatment can create new risks or modify existing risks.

-
-
-
= The use of capabilities and resources in relation to each other (tactics); non-prescriptive ways or methods used to perform missions, functions, or tasks (techniques); and standard, detailed steps that prescribe how to perform specific tasks (procedures).

-
-
-
security control = The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. technical control = The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. operational control = The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

security control = A mechanism designed to address needs as specified by a set of security requirements.

-
control = countermeasure means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be administrative, technical, management, or legal in nature

technical safeguards = The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. physical safeguards = Physical

measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorised intrusion.

-

tool = A technology or type of technology that can be used to perform some function (e.g., implement an approach or technique). While specific products could be identified as examples of tools, such identification can quickly be outdated; therefore, the following table identifies classes of products.

-

-

-

threat source = The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent.

-

-

-

domain = An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture environment (system) = Context determining the setting and circumstances of all influences upon a system.

security domain = A domain within which behaviours, interactions, and outcomes occur and that is defined by a governing security policy. Note: A security domain is defined by rules for users, processes, systems, and services that apply to activity within the domain and activity with similar entities in other domains. system context = The specific system elements, boundaries, interconnections, interactions, and environment of operation that define a system.

external context = external environment in which the organization seeks to achieve its objectives (3.49) Note 1 to entry: External context can include the following: — the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; — key drivers and trends having impact on the objectives of the organization (3.50); — relationships with, and perceptions and values of, external stakeholders (3.37). internal context = internal environment in which the organization (3.50) seeks to achieve its objectives Note 1 to entry: Internal context can include: — governance, organizational structure, roles and accountabilities; — policies (3.53), objectives (3.49), and the strategies that are in place to achieve them; — the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes (3.54), systems and technologies); — information systems (3.35), information flows and decision-making processes (both formal and informal); — relationships with, and perceptions and values of, internal stakeholders (3.37); — the organization's culture; — standards, guidelines and models adopted by the organization; — form and extent of contractual relationships.

-

covered entities = Covered entity means: (1) A health plan. (2) A healthcare clearinghouse. (3) A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this sub-chapter. (4) Medicare Prescription Drug Card Sponsors. healthcare = type of services provided by professionals or paraprofessionals with an impact on health status.

-
-
-
-
-
risk = The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

risk = Effect of uncertainty on objectives. Note: Risk can be positive or negative, where positive risk may also be referred to as an opportunity.

risk = effect of uncertainty on objectives (3.49) Note 1 to entry: An effect is a deviation from the expected — positive or negative. Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Note 3 to entry: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009, 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence. Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization. residual risk = risk (3.61) remaining after risk treatment (3.72) Note 1 to entry: Residual risk can contain unidentified risk. Note 2 to entry: Residual risk can also be referred to as “retained risk”.

-
-
-
-
adverse consequence = An undesirable consequence associated with a loss. consequence = Effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system.

consequence = outcome of an event affecting objectives Note 1 to entry: An event can lead to a range of consequences. Note 2 to entry: A consequence can be certain or uncertain and, in the context of information security, is usually negative. Note 3 to entry: Consequences can be expressed qualitatively or quantitatively. Note 4 to entry: Initial consequences can escalate through knock-on effects. [SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — Note 2 to entry has been changed after “and”.]

-
-
-
-
constraints = Factors that impose restrictions and limitations on the system or actual limitations associated with the use of the system.

-
-
-
criticality = An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals.

-
-
-
-
cyber-physical system = A system that includes engineered, interacting networks of physical and computational components. -

-
information system = An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

health information system = repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users.

system = A set of interacting or interdependent parts forming an integrated whole [4]; any organised assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions [5]. This definition is recursive; it includes a system-of-systems, i.e., “a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities” [6]. The term “system” typically includes people and organisational processes as well as technology; among those who use the term more restrictively, to include only technology, the term “socio-technical system” is used to refer to the combination of technology, people, and processes.

-
-
-
-
evidence = Grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood. Note 1: Evidence can be objective or subjective. Evidence is obtained through measurement, the results of analyses, experience, and the observation of behavior over time. Note 2: The security perspective places focus on credible evidence used to obtain assurance, substantiate trustworthiness, and assess risk.

-
-
-
-
likelihood = Chance of something happening.

likelihood = chance of something happening.

attack potential = perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker’s expertise, resources and motivation

-
-

requirement = Statement that translates or expresses a need and its associated constraints and conditions. A condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification, or other formally imposed documents.
security requirement = A requirement that specifies the functional, assurance, and strength characteristics for a mechanism, system, or system element. system security requirement = System requirements that have security relevance. System security requirements define the protection capabilities provided by the system, the performance and behavioural characteristics exhibited by the system, and the evidence used to determine that the system security requirements have been satisfied. Note: Each system security requirement is expressed in a manner that makes verification possible via analysis, observation, test, inspection, measurement, or other defined and achievable means.

requirement = need or expectation that is stated, generally implied or obligatory Note 1 to entry: "Generally implied" means that it is custom or common practice for the organisation and interested parties that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example in documented information.

-
-
-
-
-

objective = result to be achieved Note 1 to entry: An objective can be strategic, tactical, or operational. Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organisation-wide, project, product and process (3.54)]. Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target). Note 4 to entry: In the context of information security management systems, information security objectives are set by the organisation, consistent with the information security policy, to achieve specific results.

-
-

mission/business function = An activity, process, or set of related activities or processes intended to achieve a mission or business objective.

-

-
-
-
-
-
-
-
-

subject of care = one or more persons scheduled to receive, receiving, or having received a health service.

-
-

+++

security dependency maps mission-assets dependency maps Understanding recovery objectives relies upon understanding the inter-dependencies among resources. These dependencies should be categorised by organisational value. Prioritising resources by their relative importance to meeting the organisation's mission objectives

Fundamental assumption The fundamental principle underlying threat modelling is that there are always limited resources for security and it is necessary to determine how to use those limited resources effectively.

+++

advisory notice = notice issued by the organization, subsequent to delivery of the medical device, to provide supplementary information or to advise on action to be taken in the: — use of a medical device, — modification of a medical device, — return of the medical device to the organization that supplied it, or — destruction of a medical device Note 1 to entry: Issuance of an advisory notice can be required to comply with applicable regulatory requirements.

implantable medical device = medical device which can only be removed by medical or surgical intervention and which is intended to: — be totally or partially introduced into the human body or a natural orifice, or — replace an epithelial surface or the surface of the eye, and — remain after the procedure for at least 30 days Note 1 to entry: This definition of implantable medical device includes active implantable medical device

medical device = instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of: — diagnosis, prevention, monitoring, treatment or alleviation of disease; — diagnosis, monitoring, treatment, alleviation of or compensation for an injury; — investigation, replacement, modification, or support of the anatomy or of a physiological process; — supporting or sustaining life; — control of conception; — disinfection of medical devices; — providing information by means of in vitro examination of specimens derived from the human body; and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means Note 1 to entry: Products which may be considered to be medical devices in some jurisdictions but not in others include: — disinfection substances; — aids for persons with disabilities; — devices incorporating animal and/or human tissues; — devices for in vitro fertilization or assisted reproduction technologies.

product = result of a process Note 1 to entry: There are four generic product categories, as follows: — services (e.g. transport); — software (e.g. computer program, dictionary); — hardware (e.g. engine mechanical part); — processed materials (e.g. lubricant). Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element. For example, the offered product "automobile" consists of hardware (e.g. tyres), processed materials (e.g. fuel, cooling liquid), software (e.g. engine control software, driver's manual), and service (e.g. operating explanations given by the salesman). Note 2 to entry: Service is the result of at least one activity necessarily performed at the interface between the supplier and customer and is generally intangible. Provision of a service can involve, for

Table B.2: Aggregation of treatments by publication year (continuation)

Type	Concept	Health-related standards			Cyber resiliency frameworks	
		NIST SP 800-66r1	ISO 27799:2016	NIST SP 1800-1	MTR140499R1	MTR110237
	event	-	-		adverse cyber event	adverse condition stresses
	incident	-	-		-	-
	recover	-	-		-	-
	CIRP	-	-		-	-
	resilience	-	-		-	cyber resiliency
	asset	-	-		resource	cyber resource
	CIRT	-	-		-	-
	incident response	-	-		CCoA	-
	indicator	-	-		-	-
	precursor	-	-		-	-
	threat	-	-		-	-
	vulnerability	-	-		-	-
	attack	-	-		-	cyber attack
	measure	-	-		TTPs	-
	security control	technical safeguards physical safeguards	-	tool	-	-
	threat source	-	-		-	-
	domain	covered entities	healthcare		-	-
	risk	-	-		-	-
	impact	-	-		-	-
	constraints	-	-		-	-
	cyber-physical system	information system	health information system		system	-
	evidence					
	likelihood	-	-		-	-
	requirement	-	-		-	-
	objective	-	-		mission business function	-
	subject of care	-	subject of care		-	-

example, the following: — an activity performed on a customer-supplied tangible product (e.g. automobile to be repaired); — an activity performed on a customer-supplied intangible product (e.g. the income statement needed to prepare a tax return); — the delivery of an intangible product (e.g. the delivery of information in the context of knowledge transmission); — the creation of ambience for the customer (e.g. in hotels and restaurants). Software consists of information and is generally intangible and can be in the form of approaches, transactions or procedures. Hardware is generally tangible and its amount is a countable characteristic. Processed materials are generally tangible and their amount is a continuous characteristic. Hardware and processed materials often are referred to as goods.

harm physical injury or damage to the health of people, or damage to property or the environment

hazard potential source of harm

intended use intended purpose use for which a product, process or service is intended according to the specifications, instructions and information provided by the manufacturer

in vitro diagnostic medical device IVD medical device medical device intended by the manufacturer for the examination of specimens derived from the human body to provide information for diagnostic, monitoring or compatibility purposes EXAMPLE: Reagents, calibrators, specimen collection and storage devices, control materials and related instruments, apparatus or articles. Note 1 to entry: Can be used alone or in combination with accessories or other medical devices. Note 2 to entry: Adapted from ISO 18113-1:—, definition 3.29.

2.8 manufacturer natural or legal person with responsibility for the design, manufacture, packaging, or labelling of a medical device, assembling a system, or adapting a medical device before it is placed on the market or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party Note 1 to entry: Attention is drawn to the fact that the provisions of national or regional regulations can apply to the definition of manufacturer. Note 2 to entry: For a definition of labelling, see ISO 13485:2003, definition 3.6. 2.9 medical device any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of

— diagnosis, prevention, monitoring, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of or compensation for an injury, — investigation, replacement, modification, or support of the anatomy or of a physiological process, — supporting or sustaining life, — control of conception, — disinfection of medical devices, — providing information for medical purposes by means of in vitro examination of specimens derived from the human body,

and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means Note 1 to entry: This definition has been developed by the Global Harmonization Task Force (GHTF). See bibliographic reference [38]. [SOURCE: ISO 13485:2003, definition 3.7] Note 2 to entry: Products, which could be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:

— aids for disabled/handicapped people, — devices for the treatment/diagnosis of diseases and injuries in animals, — accessories for medical devices (see Note 3), — disinfection substances, — devices incorporating animal and human tissues which can meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a “parent” medical device to enable that medical device to achieve its intended purpose, should be subject to this International Standard. 2.10 objective evidence data supporting the existence or verity of something Note 1 to entry: Objective evidence can be obtained through observation, measurement, testing or other means. [SOURCE: ISO 9000:2005, definition 3.8.1]

residual risk risk remaining after risk control measures have been taken Note 1 to entry: Adapted from ISO/IEC Guide 51:1999, definition 3.9. Note 2 to entry: ISO/IEC Guide 51:1999, definition 3.9 uses the term “protective measures” rather than “risk control measures.” However, in the context of this International Standard, “protective measures” are only one option for controlling risk as described in 6.2. 2.16 risk combination of the probability of occurrence of harm and the severity of that harm

severity measure of the possible consequences of a hazard

use error act or omission of an act that results in a different medical device response than intended by the manufacturer or expected by the user Note 1 to entry: Use error includes slips, lapses and mistakes. Note 2 to entry: See also IEC 62366:—, Annexes B and D.1.3. Note 3 to entry: An unexpected physiological response of the patient is not by itself considered use error.

compensating control = A cybersecurity compensating control is a safeguard or countermeasure deployed, in lieu of, or in the absence of controls designed in by a device manufacturer. These controls are external to the device design, configurable in the field, employed by a user, and provide supplementary or comparable cyber protection for a medical device¹². For example, a manufacturer’s assessment of a cybersecurity vulnerability determines that unauthorized access to a networked medical device will most likely impact the device’s safety or essential performance. However, the manufacturer determines that the device can safely and effectively operate without access to the host network, in this case the hospital network. The manufacturer instructs users to configure the network to remove the ability of unauthorized/unintended access to the device from the hospital network. This type of counter measure is an example of a compensating control.

patient harm = Harm¹⁵ is the physical injury or damage to the health of people, or damage to property or the environment. Patient harm is defined as physical injury or damage to the health of patients, including death. Risks to health posed by the device may result in patient harm. This guidance outlines the assessment of whether the risk¹⁶ of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device’s safety and essential performance, and the severity of patient harm if exploited (see section VI).

Appendix C

Survey constructs

C.1 Invitation for participation

Dear (computer science expert),

We are conducting a study as part of a research study to increase our understanding of how our methodology and tool is perceived and experienced by users. As a computer scientist you are in an ideal position to give us valuable first hand information from your own perspective.

The meeting will take around an hour and is conducted in three stages. Firstly we will present the BINA methodology. Secondly, you will be asked to download, install and use a software tool to implement the methodology in a simple case study. Thirdly you will be asked to feel in a questionnaire about your experience. Your responses to the questions will be kept confidential. Each meeting will be assigned a number code to help ensure that personal identifiers are not revealed during the analysis and write up of findings.

There is no compensation for participating in this study. However, your participation will be a valuable addition to our research and findings could lead to improvements in the methodology, tool and process.

I have included a participant information sheet for a more detailed description about the study with this letter, together with a consent form.

If you are willing to participate please read them carefully and sign the content form. Then you can email us the consent form back and suggest a day and time that suits you and I'll do my best to be available. If you have any questions please do not hesitate to ask.

Thanks! (interviewer)

C.2 Participation Information Sheet

Title of Study

Model-based Management of Healthcare Systems Cyber Resiliency.

Introduction and what is the purpose of the study/project?

My name is Myrsini Athinaïou, I am a Doctoral student at the University of Brighton, and I

am carrying out this research for my dissertation. The purpose of this research is to design and evaluate a methodology to support the development of resilient cyber systems by design. The project is primarily educational, but the methodology is implementable to corporate projects pilots.

Invitation paragraph

We would like to invite you to take part in our research study. Before you decide we would like you to understand why the research is being done and what it would involve for you. One of our team will go through the information sheet with you and answer any questions you have. This should take about an hour. Talk to others about the study if you wish, and ask us if there is anything that is not clear. You will be given time to think about whether you wish to take part before making a decision, and may take this sheet away with you.

Why have I been invited to participate?

You have been invited to participate because of your expertise in the areas of software development methodologies, cybersecurity and virtual learning environments.

Do I have to take part?

Your participation in the testing of the methodology is voluntary. If you choose to participate, you will maintain your freedom to withdraw at any time without giving a reason. However, in the case of your withdrawal, we won't be able also to withdraw your data from the study. This is because the data will be anonymised and aggregated from their collection. If you decide not to take part, we ensure that they will be no negative consequences in terms of our collaboration in the future or your participation in other projects and work activities.

What will happen to me if I take part?

You will be given a 15 minutes presentation on the methodology and use of a digital tool that applies the methodology. After that, you will be given a simple case study, and you will be asked to conduct an analysis using the tool. For that task, you will have 30 minutes. During that time we will support you with any questions or clarifications you might need. After that, we will ask you to complete an anonymised online questionnaire about the usability of the methodology. The questionnaire can be completed in 15 minutes. If you decide to be a participant, it is essential that you attend an online meeting, install the tool in a local device and fill in our questionnaire. It is also necessary that you are available for an hour.

Will I be paid for taking part?

You won't be paid to participate in this research.

What are the potential disadvantages or risks of taking part?

You are going to be testing a new methodology through a software tool that you are not familiar with, using a small scale case study. You might experience feelings of discomfort, distress or inconvenience. However, a member of our team will always be available to answer questions and support you through the process. Furthermore, the time limit is in place to prevent the testing from being time-consuming and not to test you. As a participant, you will be assessing our methodology. In other words, you are the one testing our work and we will be grateful for that. Bear in mind that you can always stop or choose to withdraw from the process at any point.

What are the potential benefits of taking part?

By participating in this research, you will see how software development is progressing to

incorporate cyber resiliency. You will interact and exchange ideas with researchers that have similar research interests and support our educational journey as researchers.

Will my taking part in the study/project be kept confidential?

As a participant, you won't be personally identifiable as your data will be anonymised. The research institution or company you work for, as well as the role or job that you have, can lead to your identification and for that reason, these data will be accessible only to the researcher, the supervisors and the examiners of the research project in case they ask for such access. In that case, they will also be informed for confidentiality and privacy responsibility. As this is a student project, your data will be maintained in the University's GDPR compliant systems. Your data will be kept until the student's degree has been awarded. For further information on data protection, please see the link to the University's University's Research Privacy Notice <https://staff.brighton.ac.uk/reg/legal/other/Template%20Privacy%20Notice.docx>.

What will happen if I don't want to carry on with the study?

As a participant, you may withdraw at any time without giving a reason. The data already collected cannot be removed as they are automatically anonymised and aggregated at the point of the questionnaire completion. If you withdraw before the stage of the questionnaire, your data can and will be withdrawn too.

What will happen to the results of the project?

The results of this research will be published in the dissertation and potentially in academic papers accessible both online. As a participant, if you wish, we can send you a direct copy of the dissertation or the results analysis section to see the results of the study.

Who is organising and funding the research? (not required for student research where no funding involved)?

This research is organised by the University of Brighton and is funded by the Engineering and Physical Sciences Research Council (EPSRC). Contact details: For further information about the project, please contact Myrsini at M.Athinaiou@brighton.ac.uk.

What if I have a question or concern?

In the event of any problem or concern, please contact Dr Lucy Redhead (L.Redhead@brighton.ac.uk). She is acting as the Chair of the ethics committee that has reviewed the ethics application of this project. As an independent party from this project, she can assist you with any further questions or concerns.

Who has reviewed the study?

This study has been reviewed and given a favourable ethical opinion by the Life, Health and Physical Sciences Cross-School Research Ethics Committee.

C.3 Consent Form

C.4 Questionnaire

From a scale of strongly disagree, disagree, agree and strongly agree, answer the following:

- The graphical notation employed by the language is intuitive.



University of Brighton

Participant Consent Form

Title of Project: Model-based Management of Healthcare Systems Cyber Resiliency.

Name of Researcher: Myrsini Athinaiou

I have read and understood the information sheet for the above study, and have had the opportunity to consider the information and ask questions.

The researcher has explained to my satisfaction the purpose, principles and procedures of the study and any possible risks involved.

I am aware that I will be required to listen to a 15 minutes presentation.

I am aware that I will be required to download and install a software tool.

I am aware that I will be required to use a software tool to model a case study.

I am aware that I will be required to answer a questionnaire.

I understand that my participation is voluntary and that I am free to withdraw from the study at any time without giving a reason and without incurring consequences from doing so.

I understand how the data collected will be used, and that any confidential information will normally be seen only by the researchers and will not be revealed to anyone else.

I agree to take part in the above study.

.....
Name of Participant, Date, Signature

.....
Name of Researcher, Date, Signature

- The modelling language includes redundant concepts.
- The language concepts are well defined.
- The modelling language is powerful enough to support cyber resiliency modelling and analysis.
- The tool requires further improvement.
- The cyber resiliency related functions of the tool are satisfying.
- The tool is easy to use.
- The use of the methodology explicitly captures cyber resiliency assumptions.
- The methodology successfully captures cyber resiliency requirements.
- The methodology successfully assesses the system cyber resiliency.
- It is easy to follow the activities of the methodology.

Open end question:

- Do you have any recommendations for improvement regarding the language, methodology, tool and/or activities?