electronics

MDPI

Article

Cyber Resilience Meta-Modelling: The Railway Communication Case Study †

Emanuele Bellini, Stefano Marrone * and Fiammetta Marulli

Dipartimento di Matematica e Fisica, Universitá della Campania "Luigi Vanvitelli", 81100 Caserta, Italy; emanuele.bellini@unicampania.it (E.B.); fiammetta.marulli@unicampania.it (F.M.)

* Correspondence: stefano.marrone@unicampania.it; Tel.: +39-0823-27-5101

† This paper is an extended version of a conference paper.

Abstract: Recent times have demonstrated how much the modern critical infrastructures (e.g., energy, essential services, people and goods transportation) depend from the global communication networks. However, in the current Cyber-Physical World convergence, sophisticated attacks to the cyber layer can provoke severe damages to both physical structures and the operations of infrastructure affecting not only its functionality and safety, but also triggering cascade effects in other systems because of the tight interdependence of the systems that characterises the modern society. Hence, critical infrastructure must integrate the current cyber-security approach based on risk avoidance with a broader perspective provided by the emerging cyber-resilience paradigm. Cyber resilience is aimed as a way absorb the consequences of these attacks and to recover the functionality quickly and safely through adaptation. Several high-level frameworks and conceptualisations have been proposed but a formal definition capable of translating cyber resilience into an operational tool for decision makers considering all aspects of such a multifaceted concept is still missing. To this end, the present paper aims at providing an operational formalisation for cyber resilience starting from the Cyber Resilience Ontology presented in a previous work using model-driven principles. A domain model is defined to cope with the different aspects and "resilience-assurance" processes that it can be valid in various application domains. In this respect, an application case based on critical transportation communications systems, namely the railway communication system, is provided to prove the feasibility of the proposed approach and to identify future improvements.

Keywords: cyber resilience; domain model; critical infrastructure; adaptive capacity; secure communications

Citation: Bellini, E.; Marrone, S.; Marulli, F. Cyber Resilience Meta-Modelling: The Railway Communication Case Study. *Electronics* **2021**, *10*, 583. http://doi.org/10.3390/electronics10050583

Academic Editor: Rashid Mehmood

Received: 29 December 2020
Accepted: 23 February 2021
Published: 2 March 2021

1. Introduction

Currently, the cyber layer is becoming pervasive and ubiquitous, and it supports many critical functions of the society, such as transport, energy, finance, commerce, health, telecommunication, etc. We are living in Human-Cyber-Physical Systems (HCPS), where smart technologies are deeply intertwined with physical components and human behaviour supporting the society functioning. Although this evolving trend aims to build a more sustainable and friction-less society, the surface of the cyber infrastructures exposed to cyber threats is dramatically augmented. In a HCPS, cyber threats put public health, safety and prosperity at risk, as information technologies are integrated into critical infrastructures. Because of its tight inter-dependency and pervasiveness, a fault in the cyber layer can rapidly provoke cascade effects in several vital services and activities mobility, energy, telecommunication, transport, financial, water, etc. [1]. A fault in the cyber layer may be due to:

1. the emerging threats characterised by the deliberate attempt to disrupt or obfuscate the expected information flows [2];
2. triggered by a cyber-breach as a result of an attack (e.g., Distributed Denial of Service

(DDoS) denying to legitimate users the access to services [3]; or
3. simply can be the results of software glitches, hardware failures or disruption, loss of connections or energy, etc.

Hence, to correctly frame the cyber resilience, it is necessary to focus the attention on all the events generated in the ecosystem under investigation (not necessarily caused by cyber-attacks), to identify vulnerabilities with "local" effect and vulnerabilities with "systemic" effects during the preparation phase to implement appropriate countermeasures and strategies for adaptation in case of unwanted changing conditions.

For instance, critical infrastructure such as the transport system is prone to suffering from various kinds and levels of disruption, which often result in lowering the level of the service provided and putting at risk the security of the infrastructure and equipment, as well as the safety of the users [4]. In particular, since the HCPS operation relies on the collection and exchange of dependable data that contain vital information for monitoring and control (e.g., location, condition of physical assets and associated infrastructure) [5,6], a cyber attack may provoke the disruption and suspension of the service for several weeks (e.g., see the ransomware attack on the Colorado Department of Transport (CODOT) in February 2018). A cyber attack on a transport system affects the safety and security of the operations such as physical asset damage and associated loss of use (e.g., traffic lights and electronic traffic signals), unavailability of IT systems and networks (e.g., interruption of ticketing services and traffic management systems), loss of operational control causing safety issues, etc.

Usually, such risks are managed through cyber risk management and security strategies to avoid a cyber breach. New technological solutions have been introduced to secure the cyber layer in HCPS such as blockchain [6,7], moving target defence techniques [8], etc. However, unlike the concept of resilience, the concept of risk is not focused on defining how well the system can absorb a cyber-attack or how quickly and how completely the system can recover from it. Whenever risks are identified, and actions are taken to reduce risk, there remains a residual risk. Resilience addresses both that remaining known, but unmitigated, risk as well as the unknown or emerging threats. Unfortunately, the concept of resilience and its related quantification is far from being standardised. Different definitions have emerged in every discipline, and there are difficulties to reach a common understanding on what are the system's parameters and indicators entitled to quantify such an emerging behaviour. In the literature, it is possible to recognise two main approaches: functionality-based and capacity-based. Both approaches have been explored in the context of HCPS, but they have remained substantially separated thus far.

Recently, a promising attempt to merge these two views into a coherent and unified conceptualisation of resilience has been proposed [9]; however, this new concept has onlt been sketched. This paper aims at presenting a meaningful extension of [9]. With respect to this work, the present paper introduces resilience-related matters into a domain model, translates such knowledge in the CR Unified Modelling Language (UML) Profile and then formalises the UML-to-Bayesian Network (BN), approach applying it to the proposed case study.

To this end, the specific objective of this paper is to provide a formalisation of the Cyber-Resilience concepts and a model-driven method able to support the analysts and designers of critical systems in order to reach the required level of resilience. To this aim, a classical multi-step model-driven process is proposed: it starts from a high level model of the system, in conformance to UML, which is then transformed into a "low-level" formalism able to be analysed formally to get quantitative information on the system. More concretely, in the paper, a UML Profile is defined, named CR UML Profile; as a quantitative formalism, the BN formalism is chosen for its ability to model conditional dependency between system entities and to be easily solved. The proposed approach is applied to a railway metro system case study.

The paper is organised as follows. In Section 2, a background on cyber-resilience recalling the most widespread definitions and concepts is presented. Section 3 states the

main features of cyber-resilience and formalises them in a domain model and a UML Profile. Section 4 is on how to integrate the presented UML Profile in design and/or Verification and Validation (V&V) processes. A case study related to secure railway communication system is presented in Section 5. Section 7 ends the paper.

2. Background on Cyber-Resilience

Resilience is considered a multi-faced concept and some different definitions have been developed across scientific domains (e.g., [10,11]), while the introduction of resilience in the cyber domain is relatively recent. Cyber resilience is focused on the data and interconnected hardware, software and sensing components of cyber infrastructure in the HCP system [12]. Intuitively, cyber resilience it is not (or not only) about resisting the breach, but rather it is about learning from the breach attempt and continuously adapt the system to the changing conditions to dampen its impact for service survivability. In other words. its aim is to sustain operations of the system while ensuring mission execution. In this respect, the cyber aspect of resilience is attracting interest, and several frameworks have been proposed by NIST [13] and Accenture [14]; this last combines NIST features with principles inspired by the resilience engineering domain [15,16]. Other frameworks have been proposed by CISCO [17], MITRE [18], CPMI-IOSCO [19], etc. Similar to what is stated in [20], for vulnerability, resilience is a theoretical concept, thus it could be more accurate to speak about making the concept operational instead of measuring it. In fact, the major issue related to such a high level frameworks is the difficulty of translating them into an operational tool. Making a theoretical concept operational consists in providing a formalisation to capture observable variables into a coherent schema for quantification and interpretation. Questions about how well a system is able to absorb a cyber-attack or how timely the system is able to recover from a cyber-attack remain difficult to answer without a formalisation that allows quantification methods for evidence driven decision making. Moreover, these frameworks are derived from the classical resilience conceptualisation that adopt a partial perspective based on one of the two relevant approaches developed in the literature for the resilience assessment of a system:

- Functionality-based: A direct quantification through the assessment of system component's functionality during a critical event [21,22]
- Capacity-based: An indirect quantification through the potential (capability) for resilience [23]

2.1. Functionality-Based Approach

The "functionality-based" approaches are mostly related to the National Academy of Science (NAS) resilience definition, which identifies four time-dependent phases, as proposed in [24]:

- Plan/Prepare: It includes all actions needed to keep the system functionality within an acceptable range of functioning during known and unknown critical events.
- Absorb: It is related to the mitigation of the impact of the assets and services disruption applying countermeasures as isolation,
- Recover: It is related to the system's functionality restoration to the status before the disruption (bounce-back).
- Adapt: It evolves the system to a new level (bounce forward) using the new knowledge coming from the lesson learnt. Adaptation strategies may include new configurations of the system, personnel training, different decision making structures, etc.

The functionality-based approach considers resilience as "a function indicating the capability to sustain a level of functionality or performance [...] over a period defined as the control time that is usually decided by owners, or society" [22]. A similar perspective is also adopted in [11,25–30], where resilience is quantified looking at the functionality level dynamics evaluated within a pre-defined time frame. For instance, in a complex system such as the smart city, the resilience performance can be assessed considering a portfolio of functionalities composing the system (city), e.g., economic performance,

material production performance, social and societal performance, etc. [31]. The results of such an approach generate the typical chart presented in Figure 1, where the area R below the curve is considered the quantification of the resilience of a system Hence, resilience R is quantified by the following equation:

$$R = \int_{T0}^{Tm} F(t)dt \quad (1)$$

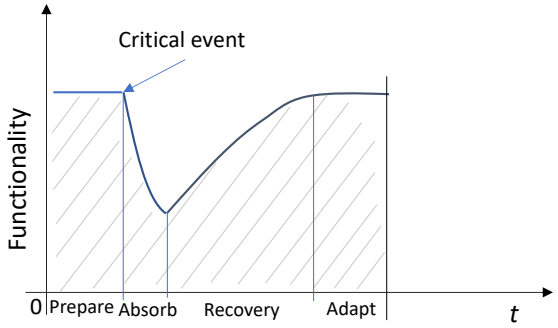

Figure 1. Critical functionality-based resilience analysis (inspired by Linkov et al. [2]).

However, it is essential to note that the high intrinsic complexity of HCP systems is related to the under-specified nature of the operations [32]. This means that the resulting measurement will not eliminate the uncertainty about how the system will behave in the future in the face of similar events. Thus, the approach is useful to understand how the systems or their components performed during the event, supporting a retrospective analysis. On the other hand, for events not well understood because of their very low frequency or not considered yet because they have never occurred before (unknown unknowns), the actual capacity of the system to cope with unexpected events before they occur can be explored only through scenario simulation.

2.2. Capacity-Based Approach

The capacity-based perspective is mainly developed within the resilience engineering domain. It considers resilience an emerging property of the system [33], and it is not possible to measure it directly [34] because only the processes the system develops towards resilience can be assessed in time. The assumption is that, if a system experiences a failure, it can still exhibit a resilient behavior in the form of survival and recovery from that failure. For instance, Sutcliffe and Vogus [35] stated that resilience requires the presence of latent resources that can be activated or recombined as new situations and challenges arise. Therefore, assessing the number of latent resources, whether this is time, financial or technical resources, can be considered a proactive and indirect approach to measure resilience.

Thus, what can be actually quantified is the potential for resilience that can be assessed against the "four resilience cornerstones" [36]:

- Respond: Knowing what to do
- Monitor: Knowing what to look for
- Anticipate: Knowing what to expect
- Learn: Knowing what has happened

Examples can be found in [4,15,23,37,38], where methods are defined to quantify the four resilience cornerstones and applied to a HCPS as the Urban Transport System.

Such potential is linked to the resources available in the system. Thus, the quali-quantitative assessment of the assets (including human, technological, organisational and financial) can provide valuable insights on how the system will behave in the case of a critical event, without waiting for that event to actually occur. The potential for resilience

can be considered a proxy indicator of resilience. In resilience engineering, the emergence of a resilient behaviour is represented by the exhibited ability of the system to cope with the operations variability and uncertainty, as discussed in [36].

To this end, the quantification of the potential of resilience requires the understanding of the internal performance variability of the interdependent functions composing the system itself. In particular, it depends on the combination of the output variability of an upstream function with the variability acceptance capacity of the function receiving varied inputs. The function dampens the inbound variability in order to continue to provide output without variation. In the case the incoming variability exceeds the damping capacity of the function (Functional Dumping Capacity (FDC)), the function will provide an output different from the normal behaviour. In [15], the factors composing the FDC are identified as: Function Buffer Capacities (FBC), Function Flexibility (FF), Function Margin (FM) and Function Tolerance (FTO).

When the amount of not dampened variability increases in an uncontrolled way in the system, we are in the presence of the so-called resonance effect where a disruption starts from one function, and it is propagated along its inter dependencies causing a cascade effect that leads to systemic trouble. This view realises the shift from the efficiency of the function perspective towards the existence of the function presented in [39].

Even if these two views are well established in the literature, they present some limitations. In the functionality-based view, the aspect of capacity building is missing. The relation between performance and the available and consumed resources is not properly addressed. In this sense, the preparation phase, instead of being focused in "expecting the unexpected", is more focused in implementing countermeasures and mitigation strategies according to the adaptation process occurring after the recovery phase.

The capacity-based view is focused on the potential for resilience, but the aspects related to how such potential is actually exploited during an event is slightly neglected. Moreover, the assumption that only the potential of resilience can be measured and not the resilience itself places the concept at an epistemic level of uncertainty that could limit its usefulness in the decision making. The current research hypothesis of merging the two views in a unified concept aims at better understanding the systems resilience and providing a valuable tool for both ex-ante and ex-post quantitative analysis.

2.3. Merging the Views: Resilience as an Emerging Property of a Synergistic Dynamic Dual System

The idea of merging the two aforementioned views is very recent and under development [4,9,38], where a new and comprehensive conceptualisation of resilience as a synergistic dynamic dual system (SDDS) has been proposed. The idea is not to consider the concepts of Adaptive Capacity (grounded on the capacity-based perspective) and the Coping Ability (grounded on the functionality-based perspective) as synonyms of resilience but as synergistic elements composing a dynamic dual systems where the resilience emerges from a dynamic interaction between them and through which successful performance is continually pursued. In fact, the potentiality is an enabling of the Coping Ability that is expressed in terms of performance in securing service survivability. However, the Coping Ability is exhibited and consequently can be assessed only in the case a critical event occurs. This condition limits the possibility of analyse the resilience of the system adopting only this one perspective since several vulnerabilities may remain latent for years (e.g., software bug) preventing an appropriate preparation. Thus, to gain a better understanding of the resilience, it is necessary to integrate the two perspectives into a holistic view. The concept is depicted in Figure 2.

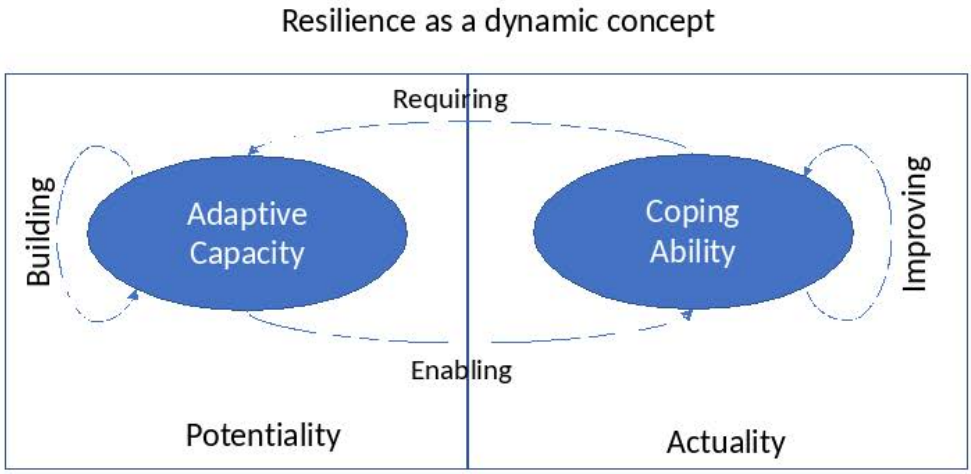

Figure 2. Combining Adaptive Capacity and Coping Ability in a synergistic dynamic dual system.

This concept has been further elaborated in a mind map presented in [9] and here slightly improved (see Figure 3).

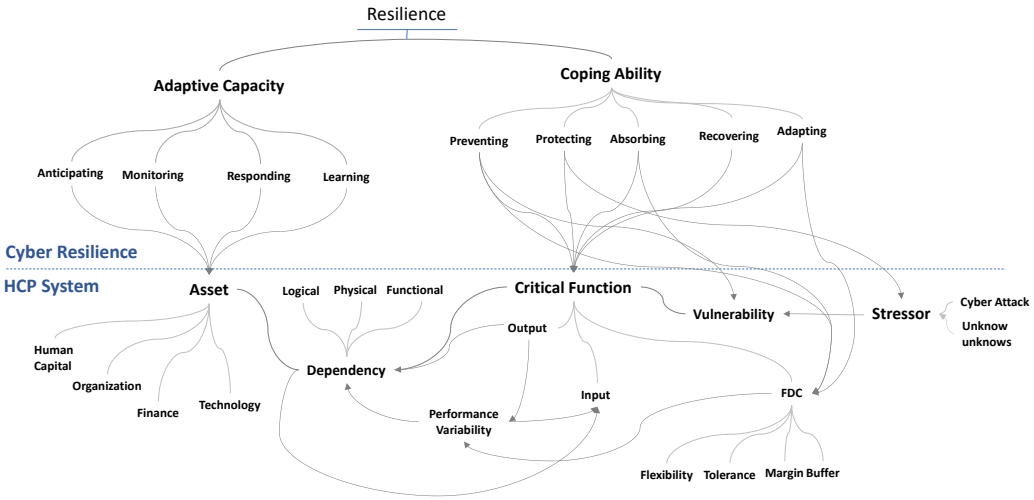

Figure 3. Resilience Ontology.

Adaptive Capacity

There are four considered adaptive capacities. Anticipating is the ability to detect hazards, evaluate risks and plan proper countermeasures also by means of continuous learning activities. The capacity of Responding is related to the ability of a system to avoid disruption given a stressing event. Monitoring deals with the ability of the system to collect relevant data on its functioning: it should be adaptable in both frequency (i.e., the collection should be more frequent when an attack is suspected) and content (i.e., some data that are not usually collected could become relevant in some situations). The capacity of Learning is related to the presence of assets able to process and transform collected data to extract non-evident knowledge useful for the system functioning.

Coping Ability

Each coping ability may need one or more enabling adaptive abilities.

Prevention is in charge of continuously detecting valuable assets to protect, evaluating the risk the infrastructure is taking and finding the most appropriate countermeasures.

Protection refers to the ability to detect anomalies and creating passive or active barriers to avoid the damaging of the system. If the protection fails, Absorption comes into the play by trying to resist the attack to avoid critical function interruption. If the absorption actions totally/partially fails, two actions can intervene: (1) Recovery (bounce back) is related to the ability to move, from a degraded state to a previous state, where the Function Dumping Capacity (FDC) values of the critical functions are reported into acceptable limits; and (2) Adaptation (bounce forward) is similar to Recovery, but, instead of pursuing a previous state, it tries to find a new state where FDC values are acceptable.

Assets

The Adaptive Capacity is directly related to the availability of a set of specific Assets (resource) that is a pre-requirement to exhibit a resilient behaviour. An asset is everything which constitutes a valuable element for an organisation or system. Some examples of considered assets are hardware, services, operators and infrastructures: they are classified into four fundamental main sub-cases of the Asset concept.

- Human: It includes technical skills, expertise and competencies (knowledge), as well as cognitive resources, particularly those relating to decision-making processes. These resources should be investigated within all relevant operational and managerial contexts. From an end-user perspective, both individual and collective behaviours (i.e., risk awareness , perceptions and aversion, among other aspects) are critical factors to be considered, as they may critically impact on the effectiveness and application of key outputs.
- Technology: It comprises ICT as well as built artefacts and infrastructure as implemented by the utilities (energy, oil and gas and water networks), transport networks, signalling systems, traffic control and ticketing related assets.
- Organisation: It includes hierarchical structures and formal procedures and regulations, as well as logistics elements.
- Finance: It includes the number of financial resources available in the system and their dynamics and the risk managed (assurance).

Therefore, a subset of the all the possible assets available in a system has to be recognised as useful for resilience and classified according to the four resilience cornerstones identified in the capacity-based approach. In this respect, system resources assessment and assets management constitute a fundamental domain of analysis in resilience in general and cyber resilience in particular.

Critical Functions

Every asset in the system is related to its enabled services. Some of these services are classified as Critical Functions as the system needs them to accomplish its primary objective. For instance, the Urban Transport System (UTS) can be considered a critical function, adopting the city as a unit of analysis. However, within a UTS, many critical functions should be considered if the subject of study become the UTS [4] itself such such as traffic light system, monitoring system, etc.

According to Bellini et al. [15], a Critical Function has a property called FDC, considered one of the key proxy indicator to assess system resilience. FDC is defined in [23] as the capacity of the system 's function to dampen the performance variably of an input. Such a variability is generated by a Stressor that exploits the system's Vulnerabilities, and it is propagated through the function's Dependencies, from the upstream function Output to the downstream functions Input [9].

The overall FDC index considers four different sub-indices:

- Buffer Capacities (BC) refers to the kind/quantity of damage a system can absorb without a critical function failure.
- Flexibility (FX) reflects the capability of the system to balance between opposite critical features. An example is constituted by the need of the balance between an efficient centralised organisation and a flexible distributed one.

- Margin (MA) deals with how far the system is pushed to its limit in accomplishing its task. In other words, it is used to compute the capability of the system to tolerate some variations in parameter values.
- Tolerance (TO) is related to the distance between the system nominal performance/quality index and the actual ones. It determines if the system is able to respond to a stressor properly.

Need of Formalisation

Despite the improvement in the comprehensiveness of resilience definition given by the semantic systematisation of its building blocks presented in [9], the lack of formalisation prevents its applicability as an operational tool for decision making.

To this end, the main contribution of the present work is to move ahead the synergistic dynamic dual system perspective for Resilience providing a formalisation of the Cyber Resilience based on the mind map proposed in [9].

3. The Cyber-Resilience Meta-Model

The Cyber-Resilience Domain Model

The domain model is derived from the experience gained in CIP_VAM [40]; this notwithstanding, there are some differences between the two approaches: the CIP_VAM approach is more oriented to physical protection while the domain here introduced to cyber aspects; furthermore, CIP_VAM focuses on protection rather than on resilience.

The domain model is structured in two main UML packages: the first (datatypes) contains the definition of the data types used by the meta-classes described in the model elements package. Figure 4 depicts such a diagram.

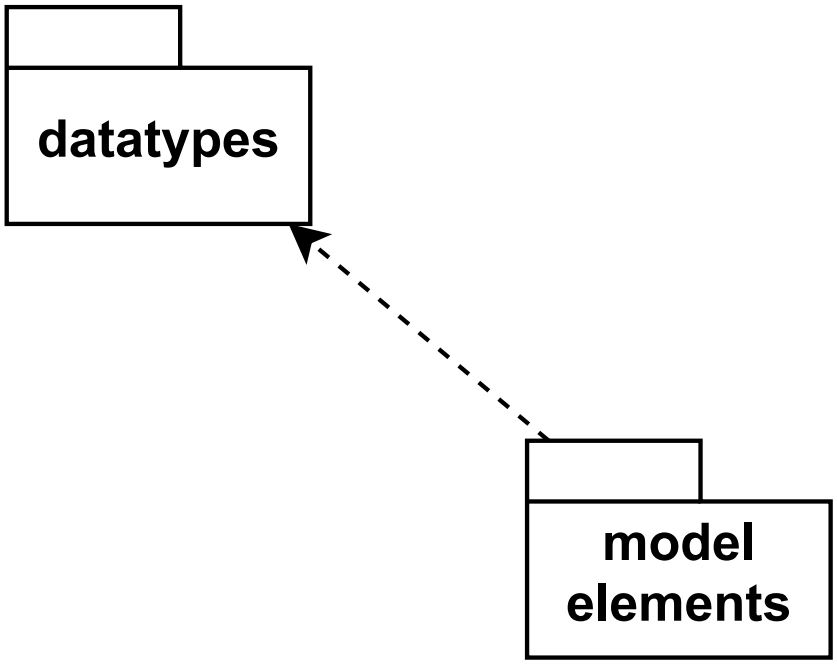

Figure 4. The cyber-resilience domain model—package-level view.

Figure 5 reports the enumeration data types that are considered in the domain model: they are in general related to abstraction as the kinds of the different dependencies (e.g., logical, physical and temporal), assets (e.g., human, organisational and financial), stressors (e.g., cyber, physical and economical), etc.

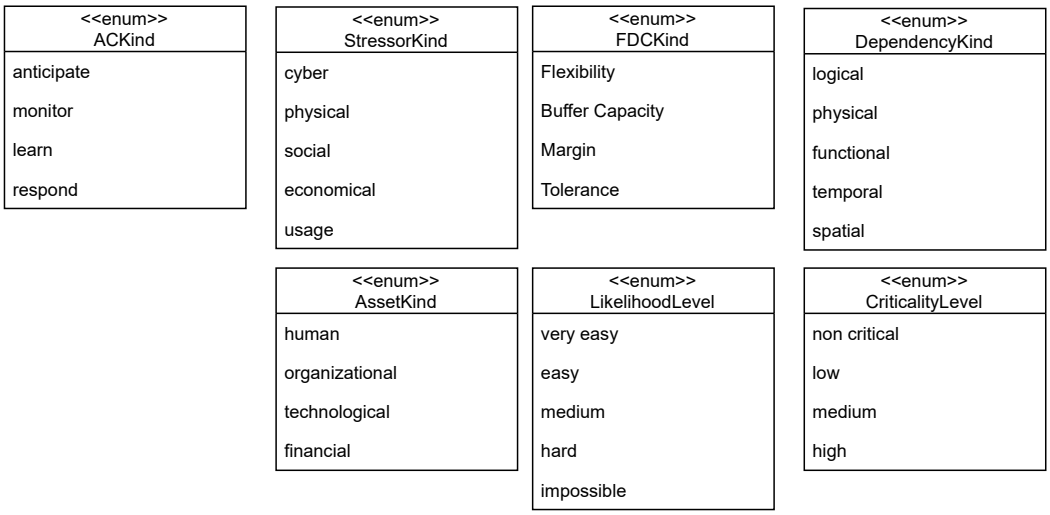

Figure 5. The cyber-resilience domain model—the datatypes package.

Figure 6 reports the different meta-classes. It is easy to recall the different concepts reported in the description of Section 2.

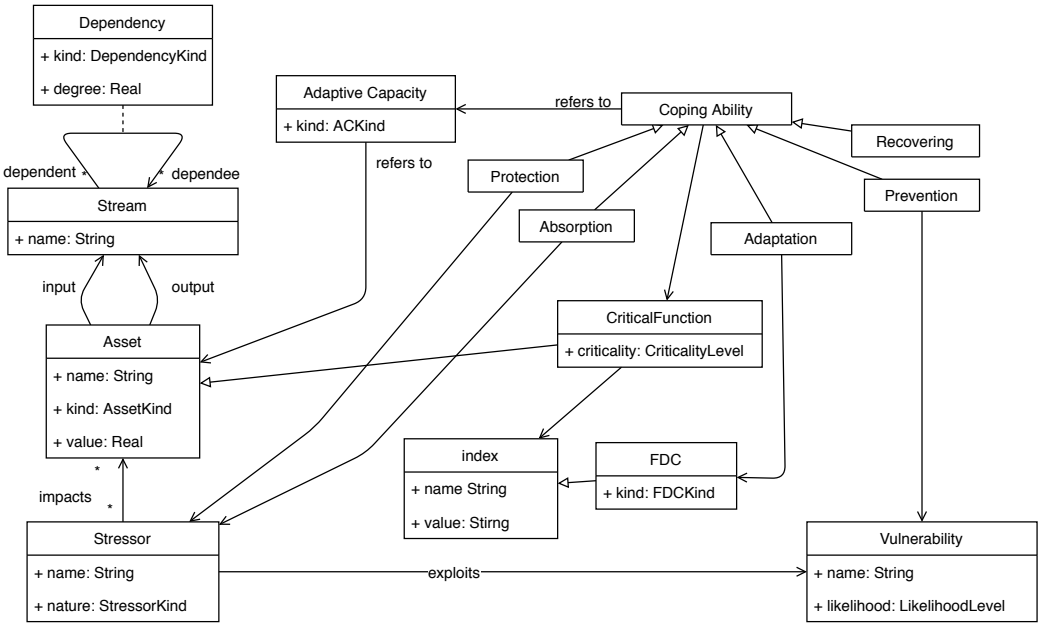

Figure 6. The cyber-resilience domain model—the model elements package.

Based on this domain model, a UML Profile is defined, making the first concrete. While the elements contained in the datatypes package of the domain model are implemented as UML's enumeration and are not explicitly reported in the schema, the domain element contained in the model elements package is depicted in Figure 7.

Some of them are translated into UML stereotypes, others into UML data types and still others are not directly translated since native UML elements can be used. The UML meta-classes used to implement the domain model are chosen in order to realise an annotated model of the system under study with both use-case diagrams and class diagrams. Further details on the usage of this profile are described in Section 4.

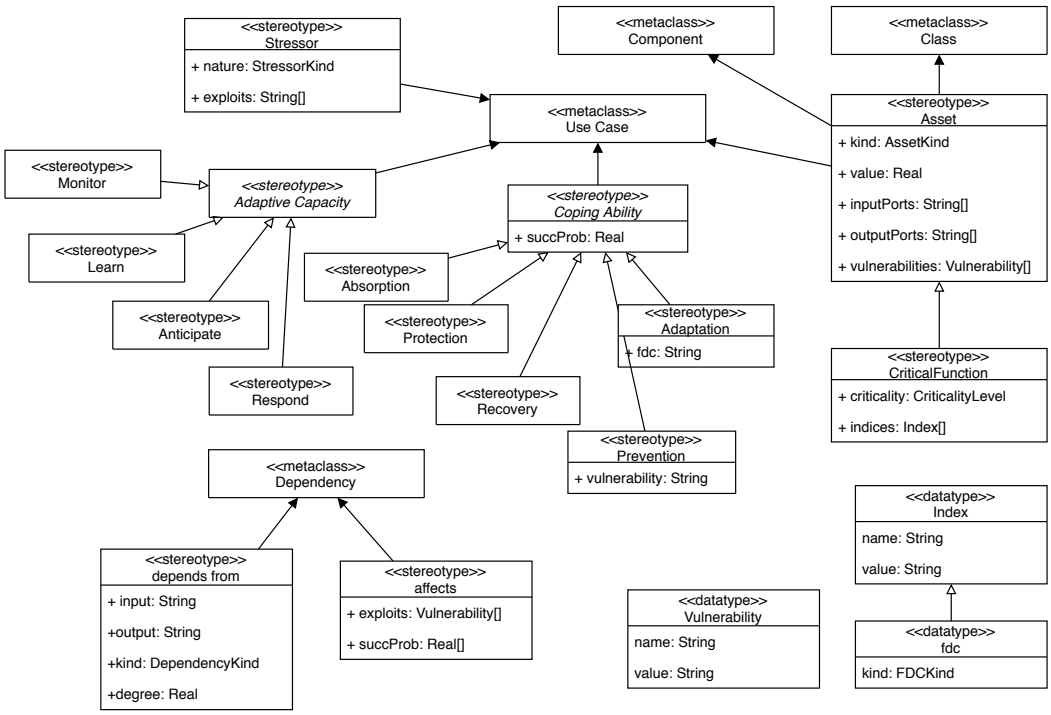

Figure 7. The cyber-resilience UML Profile.

4. Integrating and Using the Meta-Model

In our experience, describing a problem by a domain model and providing a Domain Specific Modelling Language (DSML) (e.g., a UML Profile) to support modelling are not sufficient. The key to maximising the impact of the contribution on the academic and industrial communities is to provide a modelling guideline and an automatic process supporting the design or the V&V of a critical process.

4.1. A Model-Driven Process

In past research, various processes have been provided: a method based on formal quantitative models is provided to analyse Physical Protection System (PPS) for critical infrastructure is [41], functional testing and non-functional analysis are found in [42], a security testing approach and vulnerability detection mechanism is presented in [43] early phase security elicitation process is shown in [44].

The approach here proposed takes the modelling principles presented in [44], combining them with the quantitative analysis defined in [41]. An overview of this approach is depicted in Figure 8.

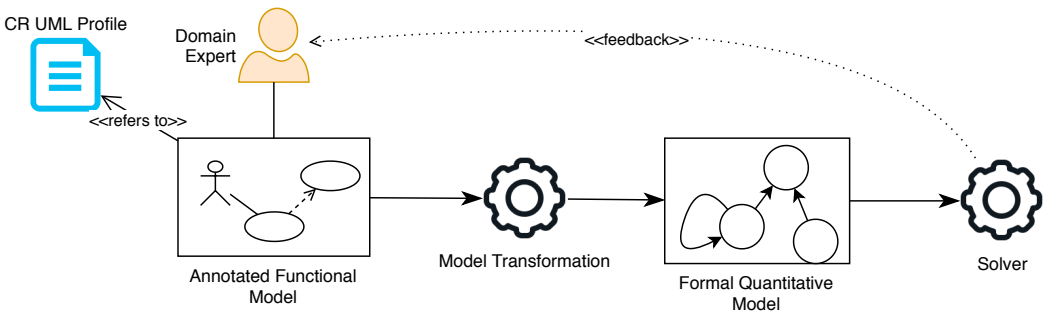

Figure 8. Risk assessment process of cyber-resilient infrastructure.

In this process, a user (i.e., the Domain Expert) is in charge of creating a high level model based on the CR UML Profile: the Annotated Functional Model. This model describes the system to analyse, and then a Model Transformation generates a Formal

Quantitative Model. Such a model is then capable of being analysed according to the most proper available solver. Two examples of these formalisms in which the Formal Quantitative Model can be expressed are Generalised Stochastic Petri Nets (GSPN) and BN.

4.2. The Annotated Functional Model

Let us focus on giving the details on how to create and annotate the high level model. Starting from the experience on meta-modelling and modelling [44], this paper assumes the UML Use Case diagram as a viable and assessed way to represent the functional aspects of the system to study. This notwithstanding, concerning the work here cited, this paper introduces the possibility to also model structural facilities and components at the support of the functional view. This situation is represented using a sample application of the CR UML Profile on a toy abstract example.

The model is composed of two diagrams: a functional view, represented as a UML Use Case diagram, and a UML Component diagram reporting the structure of components associated with the function.

For what concerns the functional view, as graphically represented in Figure 9, let us consider first the services which are valuable inside our system: the "Assets" and, in particular the "Critical Functions". Critical functions and assets are related to each other: (1) it is possible to specify the components that offers the functions by exploiting the UML use case's tag provided by (e.g., CF1 is provided by C1 and CF2 by C2); and (2) using the "include" dependency, the modeller can specify that a use case needs another use case to be accomplished (e.g., CF needs CF1 and CF2). A further specification of this last concept is in the "depends from" dependency. By means of this stereotype, one can define the specific input and output ports constituting the dependency between the two functions and quantify the degree of such a dependency with a real number between 0 and 1.

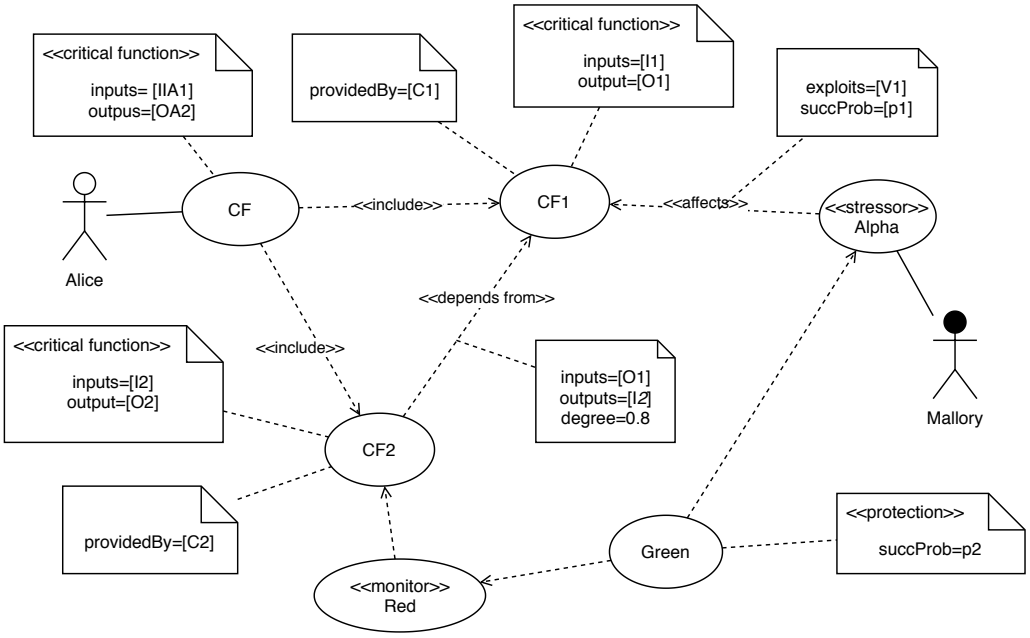

Figure 9. The functional view.

After the specification of the assets, the attack parts can be added by specifying both "stressors" (e.g., Alpha in the model) and relating them with the assets they affect (e.g., Alpha is related in the diagram to CF1 with the "affects" dependency). In general, a stressor can affect more than an asset: for each of these assets, a specific "affects" element can be added, also specifying the vulnerability the stressor exploits and the probability of having success in such an operation.

In the end of our functional view, both adaptive capacities and coping abilities can be added to the model, depicting which are the protection mechanisms the system has. In this

specific model, the Red "monitor" coping ability patrols the CF2 critical function, while the Green "protection" mechanism (which needs eed to operate) is in charge of protecting the system against the Alpha stressor. The probability of success of Green in the case of Alpha is reported in the succProb tagged value of the Green use case.

On the other hand, a structural view is in charge of highlighting the relationships between the components offering the services of the functional view. In Figure 10, an example of such a component diagram is reported. There are two assets C1 and C2 as they are shown in the functional diagram as offering components, respectively, for the critical function CF1 and CF2. Another important modelling possibility the UML component diagram allows is to add sub-components into a more general one graphically. In the diagram, C1A and C2A are C1's sub-components: in this way, an attack brought on C1A can compromise the C1 component blocking the capability to provide the critical function it offers.

It is worthy of underlining that the CR UML Profile contains many more tagged values than the one used in this modelling and analysis process. Many of these processes may be defined and automated with model-driven techniques, having in mind the generation of formal models as well as simulation code. As an example, another possible scenario is constituted by the generation of an event-based simulation model, based for example on the well-known SimPy framework, to determine the dynamic evolution of a system-under-attack. In such a scenario, the FDC features of critical functions and their protection mechanisms can be fully explored.

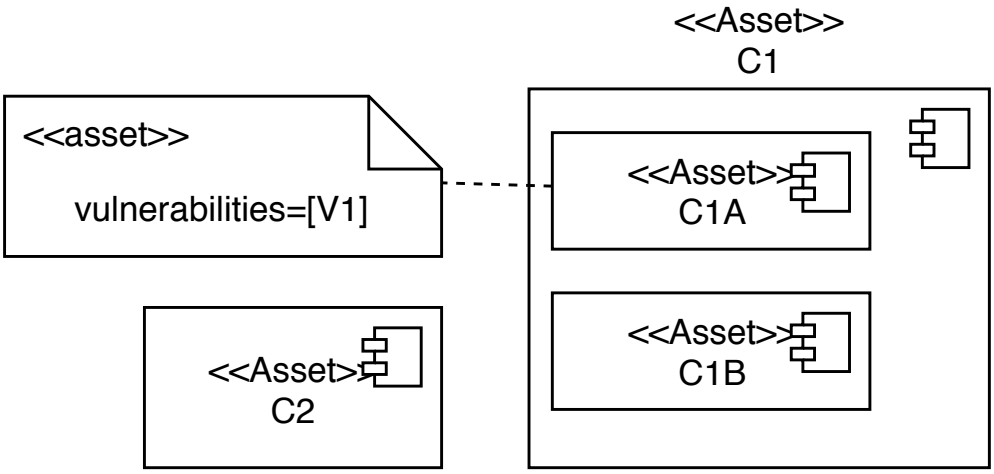

Figure 10. The structural view.

4.3. Generating the Formal Quantitative Model

In this subsection, some hints on the generation of Formal Quantitative Model are provided. First, let us discuss about the choice of the formalism the best fits into the process described above. As the objective of the concrete process, we describe is to provide a probability of disruption of one or more critical functions, we propose BN as a formalism to evaluate it.

Here, a brief introduction to the BN is reported. BN [45] provides a graphical representation of a joint probability distribution over a set of random variables with a possible mutual causal relationship: the network is organised as a Direct Acyclic Graph (DAG) whose nodes represent random variables and arcs represent causal influences between pair of nodes. A conditional probability distribution is defined for each node of the network: in the common case of discrete random variables, the conditional probability function is often represented by a table Conditional Probability Table (CPT). BN have been extensively included in a lot of scientific works in the field of system dependability and risk prediction [46] as well as network security [47].

Before applying the transformation, some checks are needed to the Annotated Functional Model. As an example, use cases must not be connected into cycles (i.e., no mutual dependencies between critical functions); another example is that an "protection" mechanism (or another Coping Ability) must be ever supported by an Adaptive Capacity (i.e., a "monitor" in the reported model).

Let us now show how a BN model can be generated from the CR UML Profile. It is not in the scope of this paper to define such a model transformation in a formal way, and, hence, this transformation is introduced graphically, on the toy example introduced before: Figure 11 reports such a generation process.

On the left side of this schema, there is a high-level model that plays the role of source model; on the right side, the generated BN model plays the role of the target model. Six dotted arrows connect some elements from source to target model; for each of these arrows, let us define a transformation rule.

R1 Each annotated use case or component generates one binary BN variable (e.g., an {on,off} variable according to the activation state of the function/component). The only exception is constituted by adaptive capacities.

R2 Each "include" tagged dependency makes in a hierarchical relation two use case, and hence two BN variables. A failure of an "included" use case determines a failure of the "including" use case that includes. On the BN model side, the variable generated by the included use case is a parent for the BN variables related to the including ones.

R3 The same situation as R2 is for the "depends on from" dependency. In this case, the depending use case plays the role of the including one. The corresponding BN variables are in the parent–child relationship as in the previous case.

R4 Another situation where parent–child relationships are created in the BN model is when an "asset"-annotated component is contained into another "asset" one.

R5 This rule takes care of the "affects" dependency relationships occurring between a "stressor" and the "asset" that is under attack. In this case, the tagged values related to the "affects" stereotype (see Figure 7) are used to define the parent–child relationship in the BN model. First, the `exploits` tagged value is used to determine the component that exposes the reported vulnerability (i.e., in the example, V1). Second, the `succProb` is used in the CPT of the parent BN variable to determine the impact of the attack to the critical function/asset under attack. As a sample, the CPT of the C1A is reported in Table 1: $p1$ is the success probability of Alpha while $p2$ is the one of Green.

R6 The last rule is related to the resilience-related mechanisms. As an example, the relationship in the high-level model from the "protection"-annotated use case (i.e., Green in the model) to the "stressor" Alpha determines the generation of two links in the BN model. The first is related to the parent–child relationship from Alpha BN node to Green: this BN link represents the activation of the protection mechanism. The second link is instead related to the effect of the protection system to the healing effects of the resilience mechanisms, and is represented in the BN model by the link from Green to C1A (that is, the subject of the attack).

Table 1. The CPT of C1A node.

Alpha	Green	*ok*	*ko*
ko	*ko*	1	0
ko	*ok*	1	0
ok	*ko*	1–p1	p1
ok	*ok*	p2	1–p2

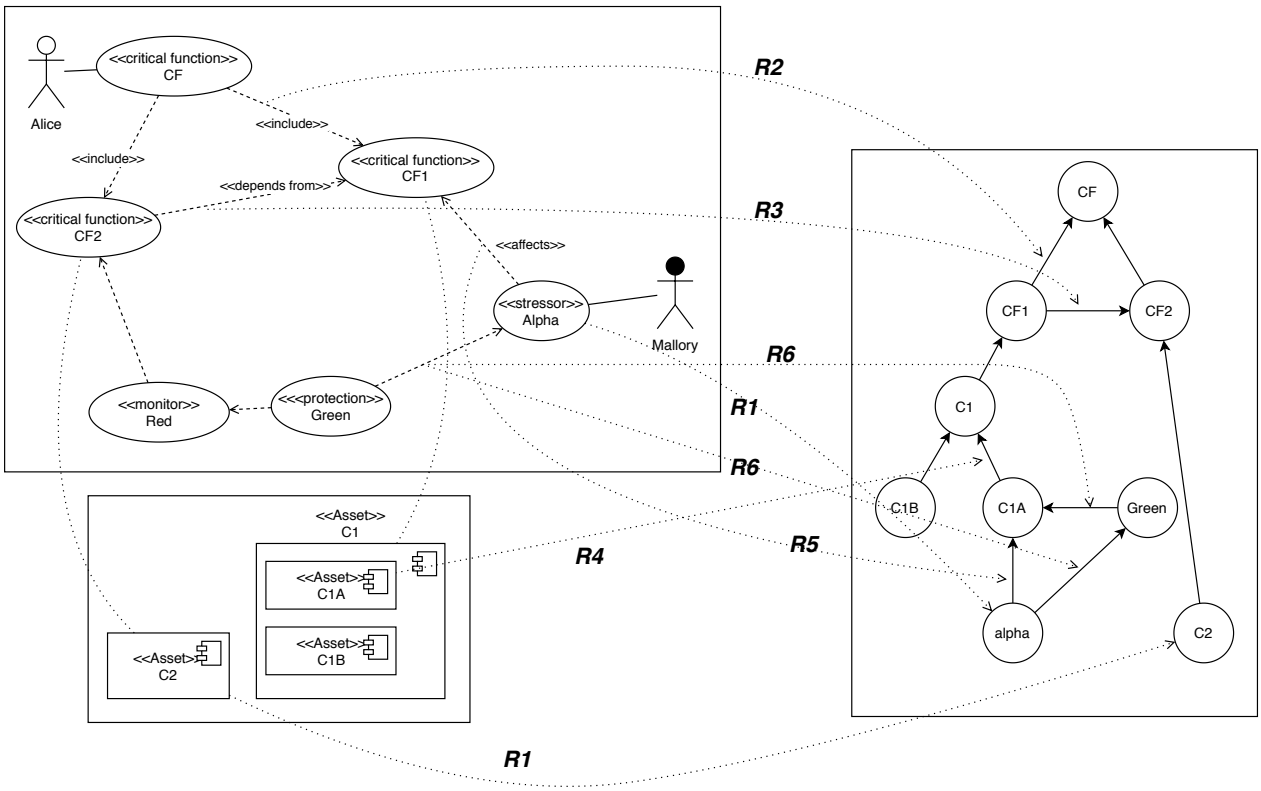

Figure 11. Generating BN model from CR UML Profile.

Algorithm 1 translates the set of the rules here reported in form of pseudo-code. The working hypothesis is the availability of the following functions/classes:

- The names of both UML's Use Cases and Components can be inferred by the *name* property.
- *getSourceUC()-getDestUC()* are methods of an "include" relationships functions returning the source and the destination use case.
- *getChildern()* is a method of the UML's components returning the list of sub-components.
- *getProvidedBy()* is a method of the use cases able to retrieve the list of the components reported in the `providedBy` property.
- *isStressor()* and *isProtection()* are methods to understand whether the use case is tagged with the relative stereotypes.
- *getAffected()* is a method of the UML's use case able to return the components and the use cases that are affected by the "stressor".
- *getSuccessProb()* extracts the value of the `successProb` tagged value of a "stressor".
- Given a "protection" , the *activations()* and *u.protected()* methods, respectively, return the lists of the use cases that activate (i.e., the stressors) and are protected by (i.e., the critical functions) the protection mechanism.
- *addNode()-addLink()*, given a BN, add a node and a link between two nodes, respectively.
- *getNode()* retrieves the node of a BN from the name while *setCPT()* builds and sets to a node a CPT according to the schema defined in Table 1 and on the base of a specified value of probability.

All these functions can be implemented according to the specific modelling and programming considered environment. A deeper description of the implementation level details of this model transformation is out of the scope of this paper. An example of an implementation of a similar transformation is presented in [48].

Algorithm 1: Generation of the BN model pseudo-algorithm.

```
Data: uml: the annotated High-level model
Result: bn: the BN model
ucs: list of uml's use cases;
asts: list of uml's assets;
incs: list of uml's include relationships;
deps: list of uml's depends from relationships;
affs: list of uml's affects relationships;
foreach e ∈ ucs ∪ asts do
    node = new BnNode(e.name);
    bn.addNode(node);
end
foreach u ∈ ucs do
    foreach a ∈ u.getProvidedBy() do
        bn.addLink(a.name,u.name);
    end
end
foreach r ∈ incs ∪ deps do
    fromNode = getNode(r.getSourceUC().name);
    toNode = getNode(r.getDestUC().name);
    bn.addLink(fromNode,toNode);
end
foreach a ∈ asts do
    foreach c ∈ a.getChildren() do
        bn.addLink(c.name,a.name);
    end
end
foreach r ∈ affs do
    u = r.getDestUC();
    if u.isStressor() == true then
        p = u.getSuccessProb();
        foreach x ∈ u.getAffected() do
            bn.addLink(u.name,x.name);
            bn.getNode(x.name).setCPT(p);
        end
    end
end
foreach u ∈ ucs do
    if u.isProtection() == true then
        foreach ac ∈ u.activations() do
            bn.addLink(ac.name,u.name);
        end
        foreach def ∈ u.protected() do
            bn.addLink(u.name,def.name);
        end
    end
end
```

It is important to underline again that this description is not exhaustive and it serves as a baseline to define a formal model-transformation from the CR UML Profile annotated model to the BN model. Such a definition will be the subject of future research efforts.

5. The Secure Metro Communication Case Study

Rapid transit metro systems are a kind of electric passenger railway systems operating in urban areas with high capacity and frequency. The Communication-Based Train Control (CTBC) is an innovative automatic system for the management of such systems. It is particularly used for metropolitan projects to overcome the limitations of conventional fixed-block systems optimising the transportation levels, ensuring safety and shortest headway. The IEEE Standard 1474.1 [49] regulates CTBC performance and functions, defining a cornerstone for future mass transit systems worldwide.

In a metro system, there are several subsystems:

- Signalling: The combination of the interlocking and communication system that transmits the information necessary to control the train movement to the on-board subsystem
- Automation: Trains scheduling and interface with the central operator
- Power Supply: Line electrification and supply of all civil loads in a metro system (e.g., station lighting and elevators)
- Platform Screen Doors: Doors on the platform to screen it from the train
- Passengers Information System: Communication system from centre to passengers devoted to providing timely and correct information (video-walls, monitors, speakers, etc.)

The key to automation is the system. CTBC technology, used to implement the Automatic Train Control (ATC) system, ensures that the trains stop at the right place at the stations, open and close the doors, leave the stations, keep the correct speed, keep the safe distance between the trains, etc., utilising systems integrated into the trains, on the tracks, on the stations and in the control room that can continuously exchange real-time data (the main system architecture is shown in Figure 12).

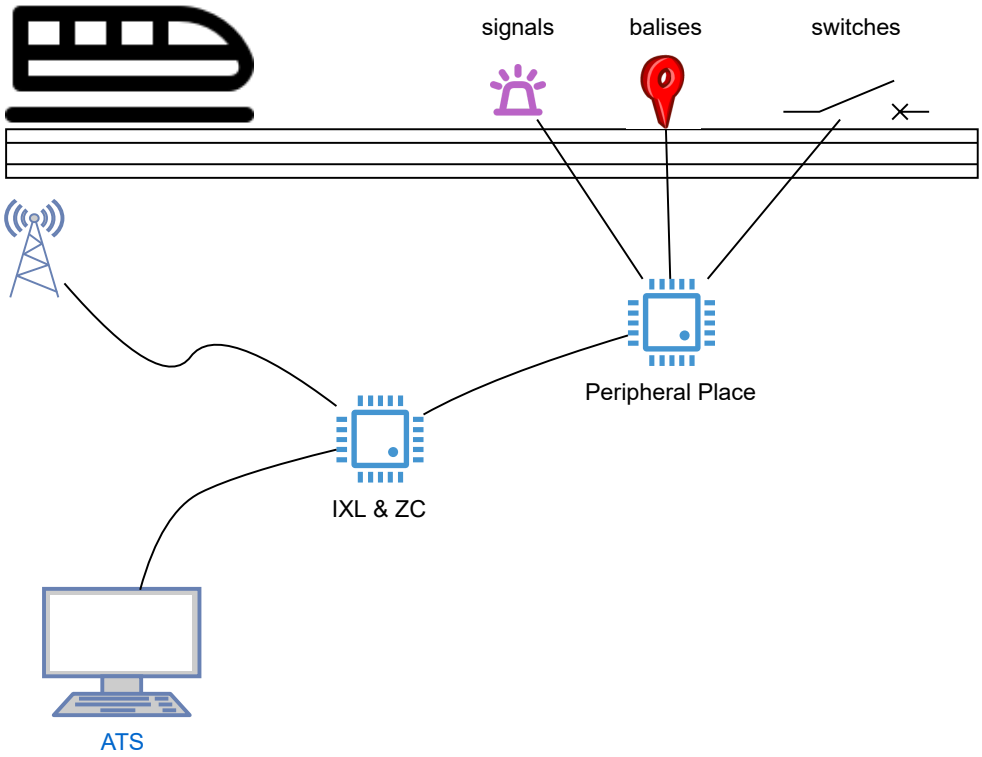

Figure 12. Overview of CTBC.

The ATC consists of three subsystems, each having its own functionalities: (1) Automatic Train Protection (ATP) constantly supervises the position and the speed of the

trains, ensuring the correct distance between them, and is able to automatically intervene to adjust the speed or to stop the train for safety reasons; (2) Automatic Train Operation (ATO) system is can survey the entire operation and monitoring the status of each vehicle on the track (e.g., it ensures that the trains stop at the right position at the platform); and (3) Automatic Train Supervision (ATS) controls and coordinates all traffic and maintains a schematic review of the entire metro for the operators in the control room.

To accomplish to such functions, a reference architecture for CTBC is reported in Figure 13. The Zone Controller (ZC) manages the Movement Authority Limits (MALs) of all trains. Each ZC unit is integrated with adjacent ZCs and communicates with Interlocking (IXL) and Carborne Controller (CC) to guarantee that specific headway requirements are met. CC determine the train position with the highest accuracy. This information is then relayed back to the ZC. Based on the MALs received from the ZC, the CC calculates its braking curves and enforces speed restrictions. IXL and Object Controller (OC) determine the traffic schedule and the minimum headway. Platform Screen Doors (PSDs) have a controller that monitors the status of the doors and, interacting with the CC by means the ZC, enable them to open and close. To ensure the correct integration of the above subsystems and the necessary safety requirements, it is necessary to perform an intense analysis and testing activity on the CTBC functions.

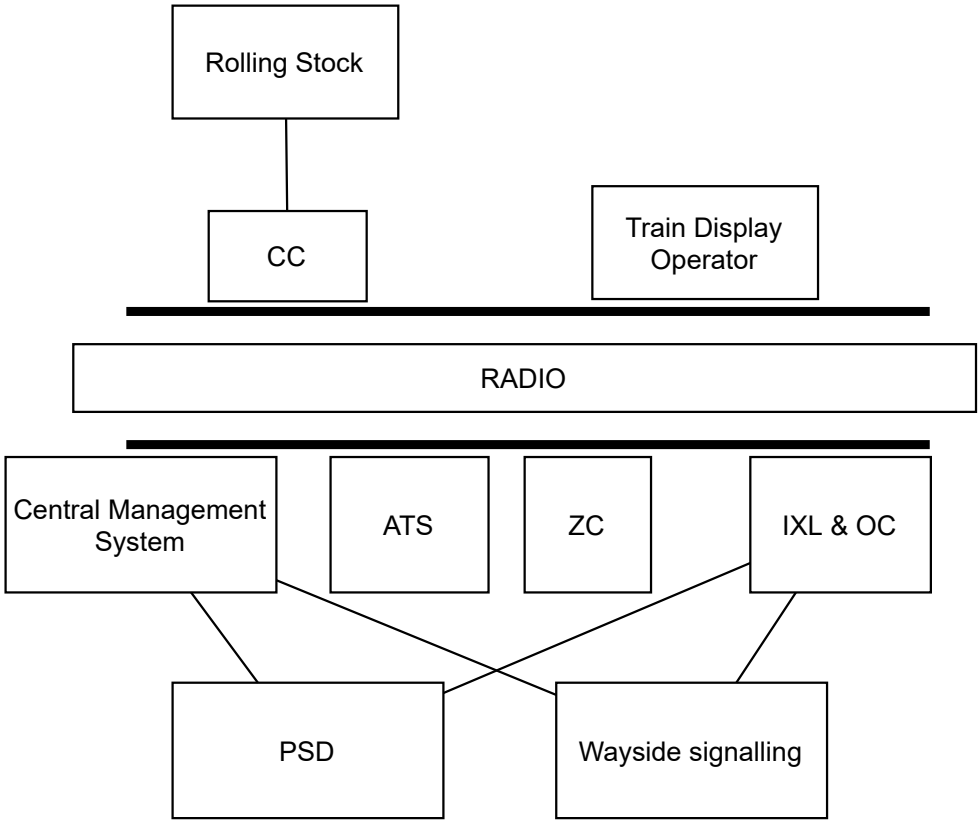

Figure 13. A reference architecture for CTBC.

Applicability Evaluation

To demonstrate the applicability of the CR UML Profile and the value of the proposed UML-to-BN approach, let us model the functions of the radio subsystems; concretely, the demonstration is oriented just to generate the BN model—a full quantitative analysis is out of the scope of this paper and its validity is tied to the presence of a real implementation of a CTBC system. Figure 14 reports the model. Two main scenarios are considered:

a. The delivery of MALs from ZC to CC
b. The possibility of having timely and correct information in the case of emergency evacuation

In the model, it is possible to see the functional breakdown, represented by the different "critical functions " (e.g., voice transportation, data transportation and radio communication) connected by "include " and "depends " from dependencies.

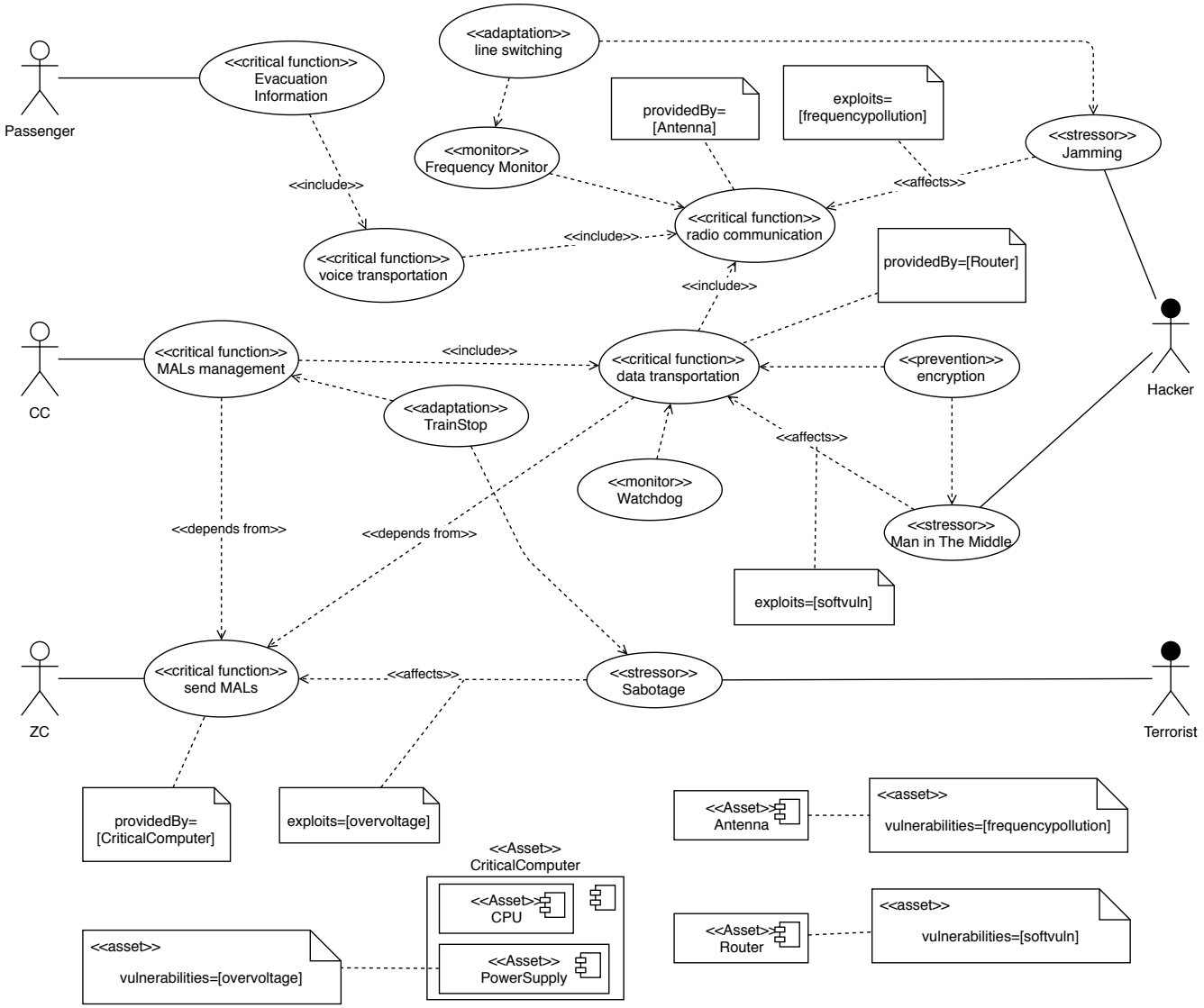

Figure 14. The annotated CT-UML model of the CTBC radio subsystem.

Some of the critical functions are explicitly supported by "assets ", as depicted in the small component diagrams in the figure.

Three "stressors " are considered:

1. A man-in-the-middle attack, exploiting software vulnerabilities of the router to intrude into the communication between ZC and CC
2. A jamming attack devoted to disturbing the frequency of radio communication
3. A physical sabotage oriented to interrupt the power supply to critical wayside computers (i.e., the ZC)

Some protection mechanisms are considered: strong end-to-end encryption to prevent man-in-the-middle attacks, switching to a fixed communication line, in the case of radio disturbance, and vitality mechanisms of the messages from the wayside to the car-borne, to put the train in a safe state when the network is over.

By applying the rules of the model transformation on this high-level model, a BN model can be generated, as depicted in Figure 15.

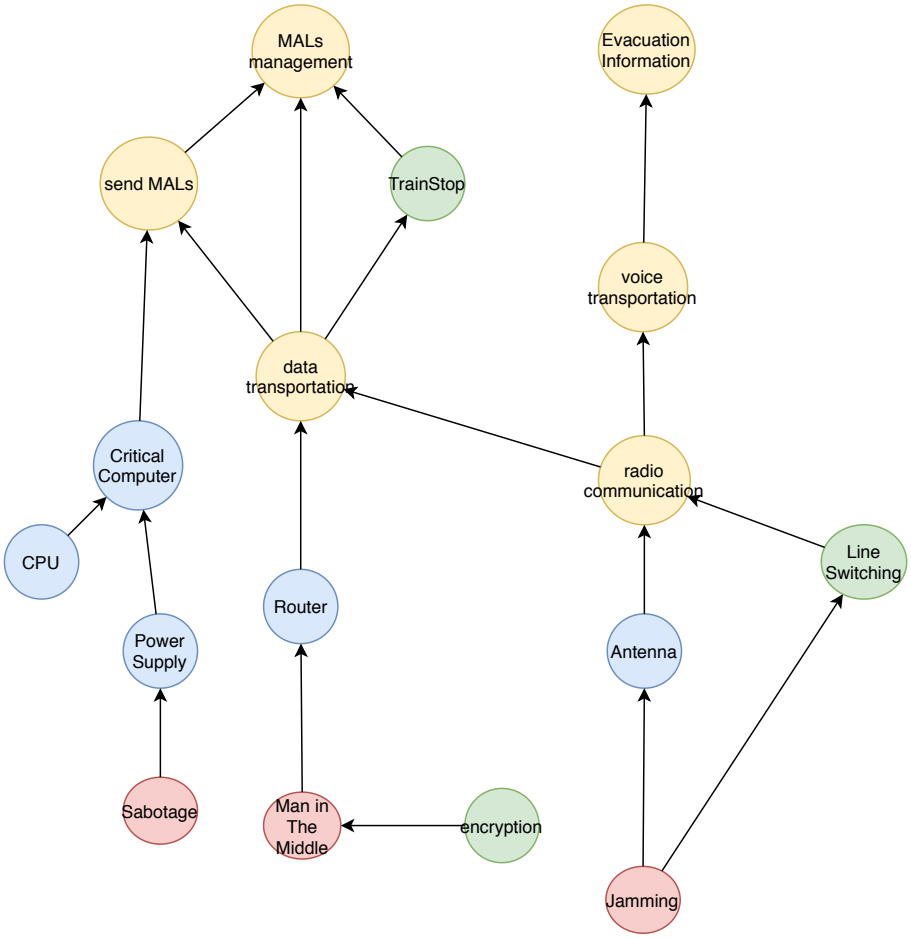

Figure 15. The BN model of the CTBC radio subsystem.

In the model, four BN node kinds are present, in relation to the different kinds of CR UML Profile's stereotypes: the yellow nodes are generated from the critical functions from the use case diagrams, the blue nodes are generated from the assets from the component diagram, the red nodes are generated from the stressors and the green nodes are from protection mechanisms.

6. Related Works

Capturing, modelling and ensuring resilience of interdependent critical infrastructures (including the power grid and transportation networks), is not trivial.

Of greatest concern is resilience to large-scale disasters having the potential to destroy an area of the network and attacks that result in correlated failures to the most vulnerable parts of the network, and are thus most likely to partition part of the network and severely impact services.

Modelling resilience to attacks and large-scale disasters requires a graph-theoretic approach, as well as a simulation-based approach to model the protocols, traffic and application scenarios. These significant challenges in modelling are discussed in [50], where the concepts of islands of resilience and corridors of resilience are introduced as parts of a model that should allow continuing to function even when local parts of the infrastructure are severed from core critical infrastructure. In this work, a protocol and traffic-based resilience analysis is performed by the open-source ns-3 discrete-event simulator [51], in order to evidence the difficulties of having sufficient simulation models and protocols that captures the complexity and heterogeneity of these environment for obtaining an adequate level of resilience.

Modelling and analysis in cyber resilience is a flourishing research topic: the scientific community has transformed the original dependability concepts into a complex body of knowledge, taking into account also security and resilience matters. The perfect synthesis of this evolution is represented by the paper of Avižienis et al. [52]. From this work, the dependability modelling scientific community has spent a huge research effort in refining old and defining new principles, processes and techniques. Formal modelling and analysis is a key cornerstone of this research topic: GSPN [53], Fault Tree (FT) [54] and BN [55] have been extensively used to quantitative evaluate resilience, while model checking has been adopted in the qualitative analysis of resilience properties [56,57].

Few works in the application of model-driven engineering principles and meta-modelling have also been used in this field: few works focus on the design and development of UML Profiles for modelling CI vulnerability and protection. In [58], the UML-CI profile is introduced, which is a UML Profile aimed at defining different aspects of an infrastructure organisation and behaviour. The CORAS method http://coras.sourceforge.net/index.html (accessed on 10 September 2020) is oriented to model-driven risk analysis of changing systems [59]; the CORAS language (now an OMG profile for QoS and Fault Tolerance characteristics and mechanisms specification) is used to support the analysis of security threat and risk scenarios in security risk analyses. UMLsec allows for expressing security information in system specification [60], the UML Profile for Modelling and Analysis of Real-Time and Embedded systems (MARTE) [61] is an OMG-standard profile that customises UML for the modelling and analysis of Non-Functional Properties (NFP) of real time embedded systems and the Dependability Analysis and Modelling (DAM) [62] profile is a specialisation of MARTE to enable dependability analysis. CIP_VAM [41] correlates infrastructures and vulnerabilities with the appropriate protection strategies to best defend the asset(s).

Another emerging formalisation in resilience modelling is related to game theory. Game theory is usually based on Nash equilibrium, a set of strategies, one for each player, in which none of the players can improve his payoffs by changing/deviating from the prescribed strategy [63,64]. Several game models and approaches have been studies to solve cyber security problems, as depicted in [63], and the mechanism for continuous adaptation in the face of survivability is promising. The use of the game-theoretic approach introduces the right flexibility to adapt the modelling by allowing for different attacker models and behaviours in various settings and provides a practical method to characterise the impacts of different types of cyber attacks. It helps to identify mitigation measures, either in terms of cyber layer security reinforcements or in terms of developing new operational planning approaches to reduce attack impacts, depending on problem formulation.

Cyber resilience formalisation and quantification has also been explored through bio-inspired analysis [65]. In particular, how an attack infects a system varies with user interaction (e.g., downloading a legitimate program that has been altered to contain malware), system misconfiguration and system vulnerabilities and can be expressed in terms of probability [66,67]. In the presented approach, IoT is considered a network of devices where the probability of infection and interactions (communication) needs to be balanced in order to reduce the malware outbreak while maintaining the network functionalities at an acceptable level. The approach exploits the concept of risk perception and the memory within the SIS (susceptible–infected–susceptible) model [68].

The use of ad-hoc safety-net functions represents another interesting formalisation approach to Cyber Resilience. Safety-net functions comprise transitioning a malfunctioning system to safe and sustainable operation, thereby enabling time for human intervention. Researchers have explored a variety of promising, formally check-able representations that show promise in realising more rigorously defined resilience. Madni et al. [69] pursued a variant of Contract Based Design (CBD) [70–72] that is rigorous and extensible in dealing with unknown-unknowns. CBD is a means for defining system requirements, constraints, behaviours and interfaces by a pair of assertions, $C = (A, G)$, in which A is an assumption made on the environment and G is the guarantee a system makes if the assumption is met.

Assumptions are system invariants and preconditions while guarantees are system post-conditions. More precisely, invariant contracts describe a system that produces an output $o \in O$ when in state $s \in S$ for an input $i \in I$, where O is the set of all outputs, S is the set of all system states and I is the set of all inputs. An implementation, M, satisfies a contract if it satisfies all contract guarantees when their associated assumptions hold. Assuming no disruptions, an invariant contract is one that must always be satisfied when the assumption is true. Invariant contracts can be represented by deterministic Büchi automatons and by temporal logic [73]. However, most HCP systems are non-deterministic, and the invariant constructs are not suitable to model unknown and unexpected disruptions that might arise from unpredictable and undiscovered interactions with the operational environment. In a Resilience Contracts (RC), the assert–guarantee couple construct that underlies traditional contracts in CBD is replaced by a probabilistic "belief–reward" couple implementing a hybrid modelling construct that combines invariant and flexible assertions. This is represented by a Partially Observable Markov Decision Process (POMDP), a special form of a Markov Decision Process (MDP) that includes hidden states and state transitions. The POMDP formalism introduces the needed flexibility into a formal contract by allowing incomplete specification of inputs and flexible definition of post-condition corrections. A POMDP model represents a decision process in which system dynamics are assumed to be a belief MDP, a memory-less decision process with transition rewards.

Table 2 summarises the main works here reported and highlights the differences between these papers and the contribution of this paper.

Table 2. This paper vs. related works.

Reference	Topic	Improvement of This Paper
[74]	The work provides a method for modelling and evaluation of cyber resilience with BNs.	This paper introduces a wider model-driven approach.
[63,64]	The work is based on game theory.	This paper provides a modelling framework easier to use.
[40]	The work presents a UML Profile for modelling and analysis of physical security.	This paper also deals with cyber assets.
[41]	Model-driven approach for survivability evaluation by means of UML and BN.	The scope of the introduced domain model/UML Profile is wider than the presented scope.
[53]	The work is based on GSPNs	The presented work introduces a model-driven approach.
[54]	This work is based on FT.	FT demonstrated their limitation since they allow just few analysis and do not have advanced modelling features (i.e., common cause, multi-state variables, etc.).
[55,75]	The work uses BNs	The work does not apply any model-driven principle. Low level modelling is an error-prone activity.
[76]	It defines a conceptual model for cyber resilience	This paper does not provide any practical modelling and analysis approach.
[77]	It defines a DSML for the modelling of a computer-based infrastructure.	This work is based on simulation while the presented work is based on a formal—more powerful—analysis method.
[78]	This work presents a model-driven approach for generating code skeletons for injecting security in complex software-based systems	The presented approach can be used during the design-time phases.

7. Conclusions and Future Works

Cyber resilience is a concept that helps us in planning for adverse events, absorbing stress, recovering and predicting and preparing for future stressors. Current cyber-resilience definitions and frameworks do not take into account holistic visions of systems: technologies, people and processes are dealt with in separate ways. As security matters cannot be contained into separate bulkheads, a unifying, holistic approach, must be pursued.

This paper starts from the conceptual separation between Adaptive Capacity and Coping Ability, considered as the two main building blocks of the Cyber Resilience concept, allowing a better definition of the contribution of the assets available in the system. Founded on these pillars, this paper designs a full model-driven approach, consisting of: (1) a domain model; (2) a UML Profile' and (3) an automatable modelling-transformation-analysis process to generate a BN model.

In fact, as model-driven engineering techniques—in general—and Bayesian Networks—in particular—have proved their abilities to cope with heterogeneous and diverse concerns, this paper gives a contribution in this field. This contribution is of course not limited to the approach here designed. In fact, as the proposed UML Profile is the "implementation" of the conceptualisation previously introduced, its scope is not just limited to the presented Model-Driven Engineering (MDE) approach. The information that can be captured from a CR-UML Profile compliant model can be used in several contexts.

The application of the presented methodologies and techniques to the railway domain case study demonstrated that is now possible to represent a complex system in terms of its functions, threats and related protection mechanisms. The transformation in BN also enables a quantification of the residual risk of the system; furthermore, it also enables the adoption of proper countermeasures in the early phases of the system life-cycle.

By means of the approach introduced in this paper, a system assessor is able to conduct a preliminary analysis to detect the most critical points under the resilience aspect. The translation into a BN model allows not only evaluating risk given a set of observations (i.e., an attack hypothesis), but also to analyse the most probable causes given a possible attack's effects.

As all unifying modelling approaches, the proposed methodology suffers from some issues. First, this approach was demonstrated on a specific generational approach; second, the proposed approach is not supported by experimental data; and, third, it does not take into account timing issues (i.e., sequences of events and timing constraint between events). Furthermore, MDE is perfectly able to match these issues respectively by means of its flexibility, the capability to support to quantitative methods and the possibility to generate models conforming to formalisms that naturally support timing-related analysis (e.g., Generalised Stochastic Petri Nets and Dynamic Bayesian Networks).

The authors are aware that this paper is not the end of a path but its starting point. Future works are due to consolidate the work here presented, including :

- integration of the proposed modelling method into an existing industrial risk management process;
- usage of the UML Profile with another "analysis-level" formalism (e.g., Petri Nets); and
- definition of a final software package implementing the approach.

Author Contributions: Conceptualization, E.B. and S.M.; Formal analysis, F.M.; Methodology, S.M.; Writing, E.B., S.M. and F.M. All authors have read and agreed to the published version of the manuscript.

Funding: The work of Emanuele Bellini and Fiammetta Marulli is funded by the project "Attrazione e Mobilitá dei Ricercatori" Italian PON Program (PON_AIM 2018 num. AIM1878214-2).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ATC	Automatic Train Control
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
BC	Buffer Capacities
BN	Bayesian Network
Bot	Internet Robots
CBD	Contract Based Design
CTBC	Communication-Based Train Control
CC	Carborne Controller
C&C	Command and Control
CODOT	Colorado Department of Transport
CPT	Conditional Probability Table
DAG	Direct Acyclic Graph
DDoS	Distributed Denial of Service
DSML	Domain Specific Modelling Language
FBC	Function Buffer Capacities
FDC	Function Dumping Capacity
FF	Function Flexibility
FM	Function Margin
FRAM	Functional Resonance Analysis Method
FTO	Function Tolerance
FT	Fault Tree
FX	Flexibility
GSPN	Generalised Stochastic Petri Nets
HCPS	Human-Cyber-Physical Systems
IoT	Internet of Things
IXL	Interlocking
MA	Margin
MALs	Movement Authority Limits
MDE	Model-Driven Engineering
MDP	Markov Decision Process
NAS	National Academy of Science
OC	Object Controller
PSDs	Platform Screen Doors
POMDP	Partially Observable Markov Decision Process
PPS	Physical Protection System
RC	Resilience Contracts
TO	Tolerance
UML	Unified Modelling Language
UTS	Urban Transport System
V&V	Verification and Validation
ZC	Zone Controller

References

1. Vespignani, A. Complex networks: The fragility of interdependency. *Nature* **2010**, *464*, 984–985. [CrossRef]
2. Linkov, I.; Baiardi, F.; Florin, M.V.; Greer, S.; Lambert, J.; Pollock, M.; Rickli, J.M.; Roslycky, L.; Seager, T.; Thorisson, H.; et al. Applying Resilience to Hybrid Threats. *IEEE Secur. Priv.* **2019**, *17*, 78–83. [CrossRef]
3. Shiaeles, S.; Papadaki, M. FHSD: An improved IP spoof detection method for web DDoS attacks. *Comput. J.* **2015**, *58*, 892–903. [CrossRef]
4. Bellini, E.; Gaitanidou, E.; Bekiaris, E.; Ferreira, P. The RESOLUTE project's European Resilience Management Guidelines for Critical Infrastructure: Development, operationalisation and testing for the urban transport system. *Environ. Syst. Decis.* **2020**, *40*, 321–341. [CrossRef]

5. Bellini, E.; Bellini, A.; Pirri, F.; Coconea, L. Towards a Trusted Virtual Smart Cities Operation Center Using the Blockchain Mirror Model. In *Internet Science*; El Yacoubi, S., Bagnoli, F., Pacini, G., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 283–291.
6. Bellini, A.; Bellini, E.; Gherardelli, M.; Pirri, F. Enhancing IoT Data Dependability through a Blockchain Mirror Model. *Future Internet* **2019**, *11*, 117. [CrossRef]
7. Brotsis, S.; Kolokotronis, N.; Limniotis, K.; Shiaeles, S.; Kavallieros, D.; Bellini, E.; Pavué, C. Blockchain Solutions for Forensic Evidence Preservation in IoT Environments. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 110–114. [CrossRef]
8. Díaz-Verdejo, J.; Lei, C.; Zhang, H.Q.; Tan, J.L.; Zhang, Y.C.; Liu, X.H. Moving Target Defense Techniques: A Survey. *Secur. Commun. Netw.* **2018**. [CrossRef]
9. Bellini, E.; Marrone, S. Towards a Novel Conceptualization of Cyber Resilience. In Proceedings of the 2020 IEEE World Congress on Services (SERVICES), Beijing, China, 18–23 October 2020.
10. Jackson, S. *Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2009; pp. 1–297. [CrossRef]
11. Vugrin, E.; Warren, D.; Ehlen, M.; Camphouse, R. A Framework for Assessing the Resilience of Infrastructure and Economic Systems. In *Sustainable and Resilient Critical Infrastructure Systems*; Gopalakrishnan, K.; Peeta, S., Eds.; Springer: Berlin, Germany, 2010; pp. 77–116. [CrossRef]
12. Linkov, I.; Kott, A., Fundamental Concepts of Cyber Resilience: Introduction and Overview. In *Cyber Resilience of Systems and Networks*; Kott, A., Linkov, I., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 1–25. [CrossRef]
13. National Institute of Standards and Technology. *NIST Cybersecurity Framework*; NIST: Gaithersburg, MD, USA, 2018.
14. Accenture. *The Nature of Effective Defense: Shifting from Cybersecurity to Cyber Resilience*; Accenture: Dublin, Ireland, 2018.
15. Bellini, E.; Ceravolo, P.; Nesi, P. Quantify resilience enhancement of UTS through exploiting connected community and internet of everything emerging technologies. *ACM Trans. Internet Technol.* **2017**, *18*, 1–34. [CrossRef]
16. Bellini, E.; Nesi, P.; Pantaleo, G.; Venturi, A. Functional Resonance Analysis Method Based-Decision Support Tool for Urban Transport System Resilience Management. In Proceedings of the IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2016.
17. CISCO. *Cyber-Resilience: Safeguarding the Digital Organization*; CISCO: San Jose, CA, USA, 2016.
18. D.Bodeau, D., Graubart, R. *Cyber Resiliency Engineering Framework*; MITRE Corporation: McLean, VA, USA, 2011.
19. Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions. *Guidance on Cyber-Resilience for Financial Market Infrastructures*; Bank for International Settlements and International Organization of Securities Commissions: Basel, Switzerland, 2016.
20. Hinkel, J. Indicators of vulnerability and adaptive capacity: Towards a clarification of the science-policy interface. *Glob. Environ. Chang.* **2011**, *21*, 198–208. [CrossRef]
21. Ganin, A.; Massaro, E.; Gutfraind, A.; Steen, N.; Keisler, J.; Kott, A.; Mangoubi, R.; Linkov, I. Operational resilience: Concepts, design and analysis. *Sci. Rep.* **2016**, *6*, 1–12. [CrossRef] [PubMed]
22. Cimellaro, G.; Reinhorn, A.; Bruneau, M. Framework for analytical quantification of disaster resilience. *Eng. Struct.* **2010**, *32*, 3639–3649. [CrossRef]
23. Bellini, E.; Coconea, L.; Nesi, P. A Functional Resonance Analysis Method Driven Resilience Quantification for Socio-Technical Systems. *IEEE Syst. J.* **2020**, *14*, 1234–1244. [CrossRef]
24. Linkov, I.; Eisenberg, D.; Plourde, K.; Seager, T.; Allen, J.; Kott, A. Resilience metrics for cyber systems. *Environ. Syst. Decis.* **2013**, *33*, 471–476. [CrossRef]
25. Aven, T. *Quantitative Risk Assessment: The Scientific Platform*; Cambridge University Press: Cambridge, UK, 2011; pp. 1–211. [CrossRef]
26. Kahan, J.; Allen, A.; George, J. An Operational Framework for Resilience. *J. Homel. Secur. Emerg. Manag.* **2009**, *6*, 1–48. [CrossRef]
27. Como, G.; Savla, K.; Acemoglu, D.; Dahleh, M.; Frazzoli, E. Robust distributed routing in dynamical networks-part II: Strong resilience, equilibrium selection and cascaded failures. *IEEE Trans. Autom. Control.* **2013**, *58*, 333–348. [CrossRef]
28. Ouyang, M.; Dueñas-Osorio, L.; Min, X. A three-stage resilience analysis framework for urban infrastructure systems. *Struct. Saf.* **2012**, *36–37*, 23–31. [CrossRef]
29. Henry, D.; Emmanuel Ramirez-Marquez, J. Generic metrics and quantitative approaches for system resilience as a function of time. *Reliab. Eng. Syst. Saf.* **2012**, *99*, 114–122. [CrossRef]
30. Baroud, H.; Ramirez-Marquez, J.; Barker, K.; Rocco, C. Stochastic Measures of Network Resilience: Applications to Waterway Commodity Flows. *Risk Anal.* **2014**, *34*, 1317–1335. [CrossRef]
31. Jovanovic, A. S., Schmid, N., Klimek P., Choudhary A. *Use of Indicators for Assessing Resilience of Smart Critical Infrastructures*; Resource Guide on Resilience; EPFL International Risk Governance Center: Lausanne, Switzerland, 2016.
32. Wilson, J.; Ryan, B.; Schock, A.; Ferreira, P.; Smith, S.; Pitsopoulos, J. Understanding safety and production risks in rail engineering planning and protection. *Ergonomics* **2009**, *52*, 774–790. [CrossRef]
33. Ferreira, P.; Bellini, E. Managing Interdependencies in Critical Infrastructures: A Cornerstone for System Resilience; Safety and Reliability-Safe Societies in a Changing World. In Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018, Trondheim, Norway 17–21 June 2018; pp. 2687–2692.

34. Hollnagel, E.; Woods, D.; Leveson, N. *Resilience engineering: Concepts and Precepts*; Ashgate Publishing Limited: Hampshire, UK, 2006; pp. 1–397.
35. Sutcliffe, K.; Vogus, T.; Sutcliffe, K.M.; Vogus, T.J. Organizing for Resilience. In *Positive Organizational Scholarship: Foundations of a New Discipline*; Cameron, K.S. Dutton, J.E., Quinn, R.E., Eds.; Berrett-Koehler: San Francisco, CA, USA, 2003; pp. 94–110.
36. Hollnagel, E.; Pariés, J.; Woods, D.; Wreathall, J. *Resilience Engineering in Practice: A Guidebook*; CRC Press: Boca Raton, FL, USA, 2011; pp. 1–322.
37. Bellini, E.; Nesi, P.; Coconea, L.; Ferreira, P.; Simoes, A.; Gaitanidou, E.; Candelieri, A. Towards resilience operationalization in Urban Transport System: The RESOLUTE project approach. In Proceedings of the 26th European Safety and Reliability Conference on Risk, Reliability and Safety: Innovating Theory and Practice, Glasgow, Scotland, 25–29 September 2016.
38. Bellini, E.; Bellini, P.; Cenni, D.; Nesi, P.; Pantaleo, G.; Paoli, I.; Paolucci, M. An IoE and Big Multimedia Data Approach for Urban Transport System Resilience Management in Smart Cities. *Sensors* **2021**, *21*, 435. [CrossRef] [PubMed]
39. Sikula, N.; Mancillas, J.; Linkov, I.; McDonagh, J. Risk management is not enough: A conceptual model for resilience and adaptation-based vulnerability assessments. *Environ. Syst. Decis.* **2015**, *35*, 219–228. [CrossRef]
40. Marrone, S.; Nardone, R.; Tedesco, A.; D'Amore, P.; Vittorini, V.; Setola, R.; De Cillis, F.; Mazzocca, N. Vulnerability modeling and analysis for critical infrastructure protection applications. *Int. J. Crit. Infrastruct. Prot.* **2013**, *6*, 217–227. [CrossRef]
41. Drago, A.; Marrone, S.; Mazzocca, N.; Nardone, R.; Tedesco, A.; Vittorini, V. A model-driven approach for vulnerability evaluation of modern physical protection systems. *Softw. Syst. Model.* **2019**, *18*, 523–556. [CrossRef]
42. Flammini, F.; Marrone, S.; Mazzocca, N.; Nardone, R.; Vittorini, V. Model-driven V&V processes for computer based control systems: A unifying perspective. In *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 190–204. [CrossRef]
43. Nardone, R.; Rodriguez, R.; Marrone, S. Formal Security Assessment of Modbus Protocol. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2017; pp. 142–147.
44. Bernardi, S.; Gentile, U.; Marrone, S.; Merseguer, J.; Nardone, R. Security modelling and formal verification of survivability properties: Application to cyber–physical systems. *J. Syst. Softw.* **2020**, *171*, 110746. [CrossRef]
45. Charniak, E. Bayesian Networks Without Tears: Making Bayesian Networks More Accessible to the Probabilistically Unsophisticated. *AI Mag.* **1991**, *12*, 50–63.
46. Weber, P.; Medina-Oliva, G.; Simon, C.; Iung, B. Overview on Bayesian Networks Applications for Dependability, Risk Analysis and Maintenance Areas. *Eng. Appl. Artif. Intell.* **2012**, *25*, 671–682. [CrossRef]
47. Frigault, M.; Wang, L. Measuring Network Security Using Bayesian Network-Based Attack Graphs. In Proceedings of the 32th Annual IEEE International Computer Software and Applications Conference, Turku, Finland, 28 July–1 August 2008; pp. 698–703. [CrossRef]
48. Gentile, U.; Marrone, S.; Nardone, R.; Bellini, E. Computer-aided security assessment of water networks monitoring platforms. *Int. J. Crit. Infrastruct. Prot.* **2020**, *31*. [CrossRef]
49. IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements. In *IEEE Std 1474.1-2004 (Revision of IEEE Std 1474.1-1999)*; IEEE: Piscataway Township, NJ, USA, 2004; pp. 1–45. [CrossRef]
50. Sterbenz, J.P. Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities. In Proceedings of the 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero, Italy, 4–6 September 2017; pp. 1–6.
51. Campanile, L.; Gribaudo, M.; Iacono, M.; Marulli, F.; Mastroianni, M. Computer network simulation with ns-3: A systematic literature review. *Electronics* **2020**, *9*, 272. [CrossRef]
52. Avižienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secur. Comput.* **2004**, *1*, 11–33. [CrossRef]
53. Orojloo, H.; Azgomi, M. Modelling and evaluation of the security of cyber-physical systems using stochastic Petri nets. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 50–57. [CrossRef]
54. Albasrawi, M.; Jarus, N.; Joshi, K.; Sarvestani, S. Analysis of Reliability and Resilience for Smart Grids. In Proceedings of the 38th Annual Computer Software and Applications Conference, Vasteras, Sweden, 21–25 July 2014; pp. 529–534.
55. Hosseini, S.; Barker, K. Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Comput. Ind. Eng.* **2016**, *93*, 252–266. [CrossRef]
56. Camara, J.; De Lemos, R. Evaluation of Resilience in Self-Adaptive Systems using Probabilistic Model-Checking. In Proceedings of the 7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS), Zurich, Switzerland, 4–5 June 2012; pp. 53–62. [CrossRef]
57. LeMay, E.; Ford, M.; Keefe, K.; Sanders, W.; Muehrcke, C. Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE). In Proceedings of the 8th International Conference on Quantitative Evaluation of SysTems, Aachen, Germany, 5–8 September 2011; pp. 191–200. [CrossRef]
58. Bagheri, E.; Ghorbani, A.A. UML-CI: A reference model for profiling critical infrastructure systems. *Inf. Syst. Front.* **2010**, *12*, 115–139. [CrossRef]
59. Lund, M.S.; Solhaug, B.; Stølen, K. Risk analysis of changing and evolving systems using CORAS. In *Foundations of Security Analysis and Design VI*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 231–274. [CrossRef]

60. Jürjens, J. *Secure Systems Development with UML*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 1–309.
61. OMG. *UML Profile for MARTE: Modeling and Analysis of Real-time Embedded Systems*; Version 1.1, formal/11-06-02; Object Management Group: Needham, MA, USA, 2011.
62. Bernardi, S.; Merseguer, J.; Petriu, D.C. A dependability profile within MARTE. *Softw. Syst. Model.* **2011**, *10*, 313–336. [CrossRef]
63. Do, C.; Tran, N.; Hong, C.; Kamhoua, C.; Kwiat, K.; Blasch, E.; Ren, S.; Pissinou, N.; Iyengar, S. Game theory for cyber security and privacy. *ACM Comput. Surv.* **2017**, *50*, 30–37. [CrossRef]
64. Halpern, J. Beyond Nash Equilibrium: Solution Concepts for the 21st Century. In Proceedings of the 27th ACM symposium on Principles of distributed computing, Toronto, ON, Canada, 18–21 August 2008; pp. 1–9.
65. Bellini, E.; Bagnoli, F.; Ganin, A.A.; Linkov, I. Cyber Resilience in IoT Network: Methodology and Example of Assessment through Epidemic Spreading Approach. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; Volume 2642-939X, pp. 72–77. [CrossRef]
66. Bagnoli, F.; Bellini, E.; Massaro, E. A self-organized method for computing the epidemic threshold in computer networks. In *International Conference on Internet Science*; Springer: Cham, Switzerland, 2018; pp. 119–130. [CrossRef]
67. Bagnoli, F.; Bellini, E.; Massaro, E. Risk Perception and Epidemics in Complex Computer Networks. In Proceedings of the 2018 IEEE Workshop on Complexity in Engineering (COMPENG), Florence, Italy, 10–12 October 2018.
68. Farooq, M.J.; Zhu, Q. On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT). *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2618–2632. [CrossRef]
69. Madni, A.; Erwin, D.; Sievers, M. Constructing models for systems resilience: Challenges, concepts, and formal methods. *Systems* **2020**, *8*, 3. [CrossRef]
70. Sangiovanni-Vincentelli, A.; Damm, W.; Passerone, R. Taming Dr. Frankenstein: Contract-based design for cyber-physical systems. *Eur. J. Control.* **2012**, *18*, 217–238. [CrossRef]
71. Le Traon, Y.; Baudry, B.; Jézéquel, J.M. Design by contract to improve software vigilance. *IEEE Trans. Softw. Eng.* **2006**, *32*, 571–586. [CrossRef]
72. Cimatti, A.; Tonetta, S. A Property-Based Proof System for Contract-Based Design. In Proceedings of the 38th Euromicro Conference on Software Engineering and Advanced Applications, Cesme, Turkey, 5–8 September 2012; pp. 21–28. [CrossRef]
73. Büchi, J.R. Symposium on Decision Problems: On a Decision Method in Restricted Second Order Arithmetic. *Stud. Log. Found. Math.* **1966**, *44*, 1–11. [CrossRef]
74. Hossain, N.; Nagahi, M.; Jaradat, R.; Shah, C.; Buchanan, R.; Hamilton, M. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem. *J. Comput. Des. Eng.* **2020**, *7*, 352–366. [CrossRef]
75. Wang, Y. Resilience Quantification for Probabilistic Design of Cyber-Physical System Networks. *Asce-Asme J. Risk Uncertain. Eng. Syst. Part Mech. Eng.* **2018**, *4*. [CrossRef]
76. Patriarca, R.; Falegnami, A.; Costantino, F.; Di Gravio, G.; De Nicola, A.; Villani, M. WAx: An integrated conceptual framework for the analysis of cyber-socio-technical systems. *Saf. Sci.* **2021**, *136*. [CrossRef]
77. Katsikeas, S.; Hacks, S.; Johnson, P.; Ekstedt, M.; Lagerström, R.; Jacobsson, J.; Wällstedt, M.; Eliasson, P. An Attack Simulation Language for the IT Domain. In *International Workshop on Graphical Models for Security*; Springer: Cham, Switzerland, 2020; pp. 67–86. [CrossRef]
78. Gossen, F.; Margaria, T.; Neubauer, J.; Steffen, B. A model-driven and generative approach to holistic security. In *Resilience of Cyber-Physical Systems*; Flammini, F., Ed.; Springer: Cham, Switzerland, 2019; pp. 123–147. [CrossRef]