SINTEF

SINTEF A22301- Unrestricted

Report

Using Indicators to Monitor Risk in Interconnected Systems: How to Capture and Measure the Impact of Service Dependencies on the Quality of Provided Services

Author(s)
Olav Skjelkvåle Ligaarden, Atle Refsdal, and Ketil Stølen

SINTEF ICT
Networked Systems and Services
2012-10-01

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47 73593000
Telefax:+47 22067350

postmottak.IKT@sintef.no
www.sintef.no
Enterprise /VAT No:
NO 948 007 029 MVA

KEYWORDS:
Indicator,
Interconnected systems,
Power supply,
Risk analysis,
Risk monitoring,
Service dependency,
Quality of service

Report

Using Indicators to Monitor Risk in Interconnected Systems: How to Capture and Measure the Impact of Service Dependencies on the Quality of Provided Services

VERSION
Final version

DATE
2012-10-01

AUTHOR(S)
Olav Skjelkvåle Ligaarden, Atle Refsdal, and Ketil Stølen

CLIENT(S)
Research Council of Norway

CLIENT'S REF.
180052/S10

PROJECT NO.
90B245

NUMBER OF PAGES/APPENDICES:
126/4

ABSTRACT
Interconnected systems are collections of systems that interact through the use of services. Their often complex service dependencies and very dynamic nature make them hard to analyze and predict with respect to quality attributes. In this report we put forward a method for the capture and monitoring of impact of service dependencies on the quality of provided services. The method is divided into four main steps focusing on documenting the interconnected systems and the service dependencies, establishing the impact of service dependencies on risk to quality of provided services, identifying measurable indicators for dynamic monitoring, and specifying their design and deployment, respectively. We illustrate the method in an example-driven fashion based on a case study from the domain of power supply.

PREPARED BY
Olav Skjelkvåle Ligaarden

SIGNATURE

CHECKED BY
Mass Soldal Lund

SIGNATURE

APPROVED BY
Bjørn Skjellaug, Research Director

SIGNATURE

REPORT NO. SINTEF A22301

ISBN 978-82-14-05279-4

CLASSIFICATION Unrestricted

CLASSIFICATION THIS PAGE Unrestricted

Contents

1 Introduction **5**

2 Basic terminology and definitions **6**
2.1 System of systems and related concepts 6
2.2 Risk and related concepts 8

3 Methodological approach **9**
3.1 Step 1: Document interconnected systems 9
3.1.1 Step 1.1: Model interconnected systems 9
3.1.2 Step 1.2: Capture service dependencies 10
3.1.3 Step 1.3: Capture trust relations 12
3.2 Step 2: Analyze the impact of service dependencies on risk to quality of provided services 15
3.2.1 Step 2.1: Identify quality assets to be analyzed 15
3.2.2 Step 2.2: Construct high-level threat diagrams of the impact of service dependencies on identified quality assets 15
3.2.3 Step 2.3: Construct detailed threat diagrams of the impact of service dependencies on identified quality assets 20
3.3 Step 3: Identify indicators for interconnected systems 22
3.3.1 Step 3.1: Identify risks to be monitored 22
3.3.2 Step 3.2: Identify relevant indicators for the risks to be monitored . . . 22
3.4 Step 4: Specify design and deployment of identified indicators for interconnected systems 23
3.4.1 Step 4.1: Specify design of indicators for risk monitoring 23
3.4.2 Step 4.2: Specify deployment of indicators for risk monitoring 24

4 Demonstration of Step 1: Document interconnected systems **24**
4.1 Step 1.1: Model interconnected systems 24
4.2 Step 1.2: Capture service dependencies 27
4.3 Step 1.3: Capture trust relations 27

5 Demonstration of Step 2: Analyze the impact of service dependencies on risk to quality of provided services **27**
5.1 Step 2.1: Identify quality assets 27
5.2 Step 2.2: Construct high-level threat diagrams of the impact of service dependencies on identified quality assets 30
5.3 Step 2.3: Construct detailed threat diagrams of the impact of service dependencies on identified quality assets 30

6 Demonstration of Step 3: Identify indicators for interconnected systems **41**
6.1 Step 3.1: Identify risks to be monitored 41
6.2 Step 3.2: Identify relevant indicators for the risks to be monitored 42

7 Demonstration of Step 4: Specify design and deployment of identified indicators for interconnected systems **42**
7.1 Step 4.1: Specify design of indicators for risk monitoring 42
7.2 Step 4.2: Specify deployment of indicators for risk monitoring 44

8 Related work **44**

9 Conclusion **48**

References **49**

A Assets to be analyzed for provided services **51**

B Schematic construction of threat diagrams for provided services **53**
B.1 Control instructions service provided to Public telecom system 53
B.2 Electricity service provided to Distribution line 2 53
B.3 Electricity service provided to Distribution line 3 54
B.4 Electricity service provided to Transmission line 55

C Capture and measure impact of service dependencies on quality assets of provided services **58**
C.1 Control instructions service provided to Public telecom system 58
C.1.1 Detailed threat diagrams 58
C.1.2 Relevant indicators for risk monitoring 65
C.1.3 Design and deployment of indicators for risk monitoring 67
C.2 Electricity service provided to Distribution line 2 72
C.2.1 Detailed threat diagrams 72
C.2.2 Relevant indicators for risk monitoring 80
C.2.3 Design and deployment of indicators for risk monitoring 80
C.3 Electricity service provided to Distribution line 3 86
C.3.1 Detailed threat diagrams 86
C.3.2 Relevant indicators for risk monitoring 87
C.3.3 Design and deployment of indicators for risk monitoring 87
C.4 Electricity service provided to Transmission line 88
C.4.1 Detailed threat diagrams 88
C.4.2 Relevant indicators for risk monitoring 98
C.4.3 Design and deployment of indicators for risk monitoring 100

D Monitor risk values based on identified indicators **104**
D.1 Likelihood calculation rules 104
D.2 Sensor data service provided to Public telecom system 107
D.3 Control instructions service provided to Public telecom system 110
D.4 Electricity services provided to Distribution line 2 and Distribution line 3 . . . 114
D.5 Electricity service provided to Transmission line 117

Using Indicators to Monitor Risk in Interconnected Systems: How to Capture and Measure the Impact of Service Dependencies on the Quality of Provided Services

Olav Skjelkvåle Ligaarden[1,2], Atle Refsdal[1], and Ketil Stølen[1,2]

[1] Department for Networked Systems and Services, SINTEF ICT, Norway
[2] Department of Informatics, University of Oslo, Norway

Abstract

Interconnected systems are collections of systems that interact through the use of services. Their often complex service dependencies and very dynamic nature make them hard to analyze and predict with respect to quality attributes. In this report we put forward a method for the capture and monitoring of impact of service dependencies on the quality of provided services. The method is divided into four main steps focusing on documenting the interconnected systems and the service dependencies, establishing the impact of service dependencies on risk to quality of provided services, identifying measurable indicators for dynamic monitoring, and specifying their design and deployment, respectively. We illustrate the method in an example-driven fashion based on a case study from the domain of power supply.

1 Introduction

In today's business environment, businesses/organizations co-operate with each other by providing and/or requiring different kinds of services. The systems facilitating such co-operation are often so-called system of systems (SoS). An SoS may be thought of as a kind of "super system" comprising a set of interconnected systems that work together towards some common goal.

An SoS is challenging from a quality perspective. Firstly, the provided services may require other services in order to function. Such requirements result in so-called service dependencies. Change in the quality attributes of one service may easily cause the quality attributes of its dependent services to change as well. Secondly, the different systems may be under different managerial control and within different jurisdictions. For the systems that are outside our control, we have limited knowledge of their risks, structure, and behavior. Thirdly, such a large number of systems, controlled and operated by different parties, evolve rapidly in a manner that may be difficult to predict.

To cope with this situation we propose the use of detailed dependency models to capture the impact of services dependencies, trust relations as a basis for analysis in the case of insufficient documentation, and monitoring to cope with evolution. Our main result is a method facilitating the set-up of such monitoring. The method is divided into four steps. Service dependencies and

trust relations are identified and documented in the first step. In the second step we conduct a risk analysis to capture the impact of service dependencies on risk to quality of a set of provided services. These services will not be provided according to their quality requirements if services that they depend on are not delivered according to their quality requirements. The focus of the risk analysis is therefore on assessing how service dependencies may result in risks, and how these risks may result in the provided services not being delivered according to their quality requirements. During this step, the identified trust relations are used when analyzing service dependencies involving systems of which we have insufficient documentation. In the third step we identify the risks to be monitored, as well as measurable indicators for monitoring their risk values. In the fourth and final step we specify how these indicators should be designed, i.e., how they should be calculated, and deployed in the interconnected systems, i.e., how data needed in the calculations should be extracted and transmitted within the interconnected systems in question. The result of applying the method is a risk picture parameterized by indicators, each defined by design and deployment specifications.

The rest of the report is organized as follows: in Section 2 we introduce basic terminology and definitions. Section 3 presents the methodological approach, while the four steps of the approach are demonstrated on an example case from the domain of power supply in Sections 4–7. In Section 8 we present related work, while we conclude and indicate further research in Section 9. For the sake of simplicity, the approach is only demonstrated for one provided service in Sections 5–7. In Appendices A–C we demonstrate the approach on the remaining provided services. In Appendix D we show how to monitor risk values for the different provided services based on indicators.

2 Basic terminology and definitions

In this section we provide basic terminology, definitions, and conceptual models for system of systems, risk, and related concepts.

2.1 System of systems and related concepts

As already explained, an SoS is basically a set of interconnected systems that work together towards some common goal. Our definition of SoS is based on the definitions of [1] and [2]. We define SoS as follows: *"A system of systems (SoS) is a set or arrangement of systems that are related or connected to fulfill common goals. The different systems may be controlled, operated, and maintained by different parties and within different jurisdictions. The loss of any system may seriously impact the other systems and the process of fulfilling the common goals."*

An SoS may arise naturally from the interconnection of individual systems, or it may be built specifically for the purpose of achieving goals that the individual systems cannot achieve alone. An example of the former is the interconnection of critical infrastructures, while a sensor network, constructed for the purpose of gathering low-level data to be aggregated, is an example of the latter.

We focus on SoS where the systems interact through the use of services. In Figure 1 is a conceptual model, in the form of a UML [3] class diagram, relating system, system of systems, and other concepts. The associations between the different concepts have cardinalities that specify how many instances of one concept that may be associated to an instance of another concept. The filled diamond specifies composition, while the hollow diamond specifies aggregation.

As shown in Figure 1, a *System of Systems* consists of at least two *Systems*. In this report, we divide a SoS into two parts; a *Target* and a *Environment*. The target consists of one or more *Target Systems*, and it is the fragment of the SoS which is controlled by the client enterprise

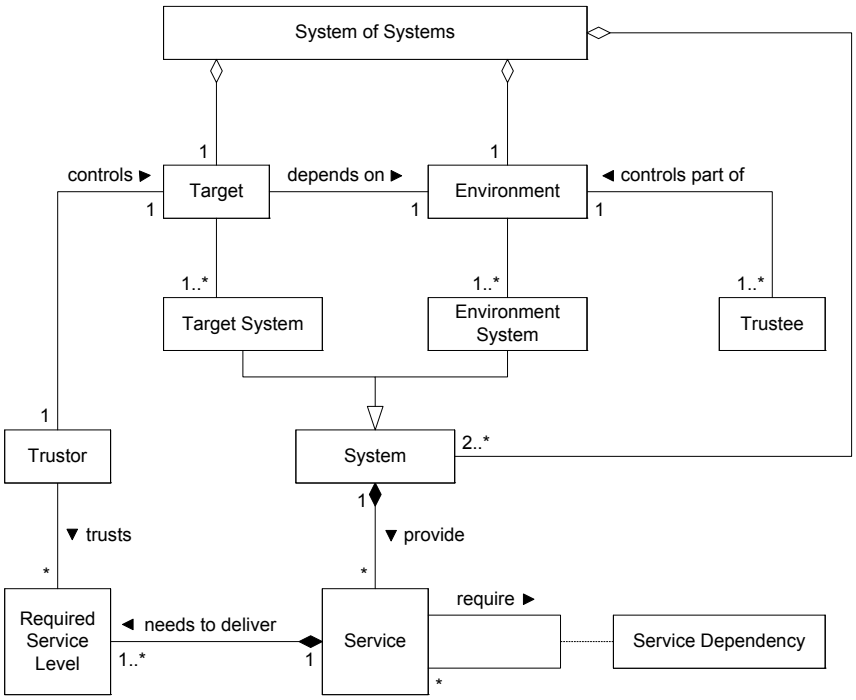


Figure 1: Conceptual model relating system, system of systems, and other concepts

on whose behalf our method is applied. We refer to this client as the *Trustor*. The target depends on the rest of the SoS that is controlled by other enterprises that may be thought of as *Trustees* of our client enterprise. We refer to the rest of the SoS as the environment of the target. The environment consists of a number of *Environment Systems*; each controlled by one of the trustees.

In this report, we only consider services where each service is provided by one system and required by another. Each service represents the exchange of some commodity (electricity, information, etc.). A *Service Dependency* describes a relationship between a service provided by a system and services required by the system. A service depends on other services if it requires the other services in order to be provided according to its requirements. In Figure 1, *Service Dependencies* are shown by the use of an association class. Service dependencies help us to better understand the importance of the individual services that are provided and required by the different systems in the SoS.

Typically, a service will have one or more *Required service levels*. Each required service level describes a requirement to one area of service scope. Availability, integrity, etc., are all examples of areas of service scope. The different required service levels may for instance be specified in a service-level agreement. Thus, one or more *Required Service Levels* are associated with each service. For each required service level, the *Trustor* may have a certain amount of trust in that the service delivers the required level of service. Inspired by [4, 5], Lysemose et al. [6] defines trust as *"the subjective probability by which an actor (the trustor) expects that another entity (the trustee) performs a given transition on which its welfare depends."* The level of trust may vary from 0 (complete distrust) to 1 (complete trust). In our case, trust assessment is only of relevance for required service levels associated with services provided by trustees' environment systems to the trustor's target systems. Trust is discussed in more detail in Section 3.1.3.

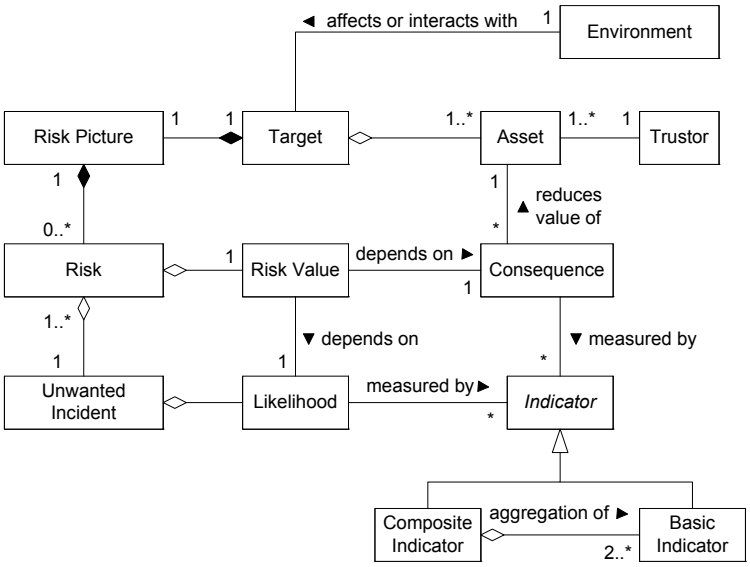


Figure 2: Conceptual model for risk and closely related concepts

2.2 Risk and related concepts

Figure 2 shows a conceptual model for risk and closely related concepts. A *Risk* involves an *Unwanted Incident*, such as "System operator is unable to control and operate the power plant." The unwanted incident may occur with a certain *Likelihood*. When the incident occurs, an *Asset* will be damaged (and its value reduced). This is the *Consequence* of the risk. An asset is owned by a *Trustor* and it is something of value that the trustor seeks to protect. It can be a physical thing, e.g., "Power plant," or conceptual, e.g., "Reputation of trustor." Since the consequence of an incident depends on the particular asset in question, the same incident may have different consequences for different assets.

By conducting a risk analysis we obtain a *Risk Picture*, consisting of zero or more risks, for the *Target* of analysis, i.e., the subject of the risk analysis. The *Target* in Figure 2 is the same as the *Target* in Figure 1. This is also true for the *Environment*. In [7], the environment of the target is defined as *"the surrounding things of relevance that may affect or interact with the target; in the most general case, the rest of the world."* In our case, the environment of the target is limited to those systems of the trustees that are of relevance to the risk analysis.

In order to choose and prioritize between treatments, we assign a *Risk Value* to each risk. A risk function calculates the risk value by taking the likelihood of the unwanted incident and its consequence for the asset in question as input. Typically, likelihood is measured in terms of frequency or probability, while the measure of consequence depends on the asset in question.

Zero or more *Indicators* may be used to measure likelihood and consequence values. Hammond et al. [8] defines indicator as *"something that provides a clue to a matter of larger significance or makes perceptible a trend or phenomenon that is not immediately detectable."* For example, an unexpected rise in the traffic load of a web server may signal a denial of service attack in progress. Thus, the significance of an indicator extends beyond what is actually measured to a larger phenomenon of interest. Moreover, an indicator is either basic or composite. Thus, an abstract class (name in italic) is used to represent *Indicator* in the conceptual model. By *Basic Indicator* we mean a measure such as the number of times a specific event generated by the ICT infrastructure has been observed within a given time interval, the average time between each generation of a specific event, the load on the network at a particular point in time, or similar. A *Composite Indicator* is the aggregation of two or more basic indicators.

Step 1 − Document interconnected systems
- 1.1 − Model interconnected systems
- 1.2 − Capture service dependencies
- 1.3 − Capture trust relations

Step 2 − Analyze the impact of service dependencies on risk to quality of provided services
- 2.1 − Identify quality assets
- 2.2 − Construct high-level threat diagrams of the impact of service dependencies on identified quality assets
- 2.3 − Construct detailed threat diagrams of the impact of service dependencies on identified quality assets

Step 3 − Identify indicators for interconnected systems
- 3.1 − Identify risks to be monitored
- 3.2 − Identify relevant indicators for the risks to be monitored

Step 4 − Specify design and deployment of identified indicators for interconnected systems
- 4.1 − Specify design of indicators for risk monitoring
- 4.2 − Specify deployment of indicators for risk monitoring

Figure 3: Overview of the methodological approach

3 Methodological approach

An overview of the methodological approach is presented in Figure 3. In the following we describe each of the four main steps as well as their sub-steps in terms of a detailed guideline. Throughout this section we exemplify different steps of the method. It should be noticed that the examples presented in this section are not used in the continuation of this report.

As already explained in Section 2, our intended client enterprise corresponds to the trustor in Figure 2. The trustor controls a fragment of the SoS which we refer to as the target. The target depends on the rest of the SoS that is controlled by other enterprises that may be thought of as trustees of our client enterprise. Our task is to establish a dynamic risk picture that captures the impact of service dependencies on risk to the quality of the services that the trustor provides to the trustees' systems.

The methodological approach presented in this section is closely related to the method ValidKI [9] (Valid Key Indicators). ValidKI is a method for designing indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of indicators. The ValidKI method is particularly relevant for further detailing of Step 3 and Step 4 as presented below. In Step 3, ValidKI supports the identification of indicators, while it supports the specification of the design and the deployment of indicators in Step 4.

3.1 Step 1: Document interconnected systems

3.1.1 Step 1.1: Model interconnected systems

Objective: Model the interconnected systems.

Rationale: To capture the impact of service dependencies on risk to quality of provided services, we need to document the services interactions between the different interconnected systems. In particular, it is essential to understand the dependencies between the target and the target's environment, i.e., the interconnected systems that are not controlled by the trustor. We also need to document the requirements to the different services. We are only concerned with the impact of services on risk when they are not delivered according to requirements.

How conducted: A target model is created by the analysis team based on input documentation provided by the trustor. The target model describes the systems of the target as well as the systems in the target's environment. It also captures the systems' service interactions and the required service levels of the different services. Each required service level is specified for one area of service scope. We can for instance specify the required level of availability, integrity, etc., for the same service.

Input documentation: The trustor provides information on the interconnected systems, their service interactions, and the requirements, in the form of required levels of service, for each service.

Output documentation: A target model documenting:

- the systems of the target and its environment;
- the service interactions between the systems; and
- the required service levels for each service.

Modeling guideline: The interconnected systems are modeled in the form of a graph, as illustrated by Figure 4. The system elements (vertices) in the graph represent systems, while service relations (edges) represent interactions in the form of services. The bold rectangular container with rounded corners separates the target from its environment. Each system element is annotated with the party controlling and operating the system represented by the element, while each service relation is annotated with the service in question and its required levels of service. In Figure 4 this has only been shown for two service relations, in order to save space. For one of the service relations, a required service level has been specified for one area of service scope, while required service levels have been specified for two areas of service scope for the other service. Here, *A* stands for availability, while *I* stands for integrity.

The source of a service relation represents the provider of the service, while the target of the relation represents the consumer of the service. A system may need to consume services in order to provide other services. If one system provides two or more services to another system, then the model is a multigraph, i.e., a graph which allows multiple edges, meaning edges with the same pair of source and target vertices.

3.1.2 Step 1.2: Capture service dependencies

Objective: Identify and document service dependencies within the interconnected systems.

Rationale: In Step 1.1 we documented the service interactions between the different systems. In this step we identify the service dependencies resulting from the interactions. This enables us to analyze the impact of service dependencies on risk to quality of provided services.

How conducted: The target model from Step 1.1 is annotated with service dependencies, based on input documentation provided by the trustor. The annotated model shows how provided services depend on required services.

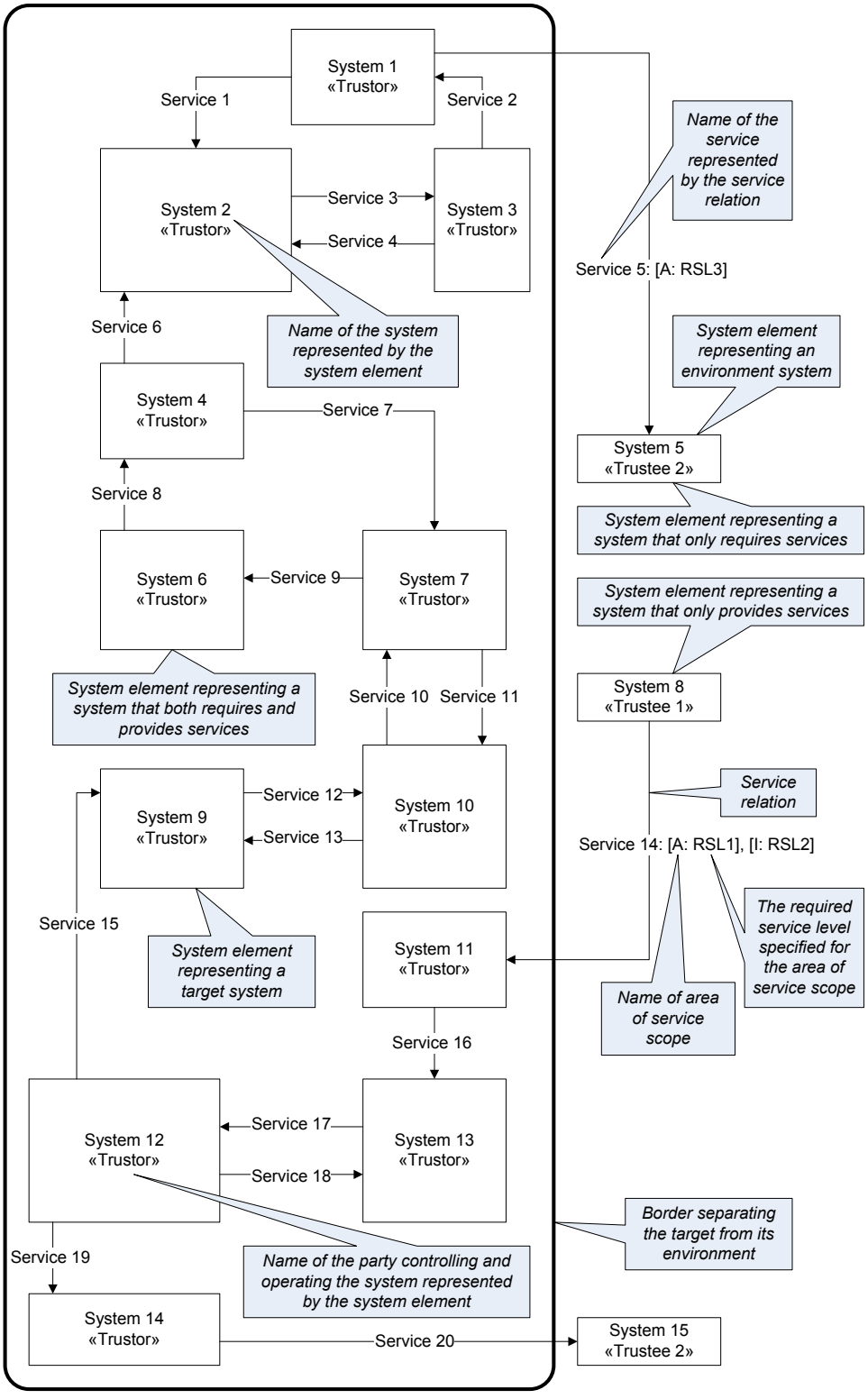


Figure 4: Target model

Input documentation:

- The target model from Step 1.1.
- The trustor provides information on the relations between required and provided services for the different systems documented in the target model.

Output documentation: The target model from Step 1.1 annotated with service dependencies.

Modeling guideline: Figure 5 shows the target model in Figure 4 annotated with service dependency constructs. The constructs describe dependencies between the provided and the required services of the systems. Dependencies between required and provided services are combined with "and" ($\wedge$) or "or" ($\vee$) operators. For an operator we refer to services that enter the operator as incoming, while we refer to services that leave the operator as outgoing. The meaning of the "and" operator is that all the incoming services are required to provide each of the outgoing services, while the meaning of the "or" operator is that only one of the incoming services is required to provide each of the outgoing services. Operators may be combined to express dependencies that cannot be expressed by a single operator alone. This has not been exemplified in Figure 5. For examples of this, we refer to Figure 11 on page 28.

Figure 5 also shows examples of service dependency constructs that do not rely on operators for expressing dependencies. If only one service is required to provide one or more services, then it is of course not necessary to use "and" or "or" operators to describe the dependencies.

3.1.3 Step 1.3: Capture trust relations

Objective: Document the trustor's trust in the required levels of services being delivered by its trustees.

Rationale: A trustor will normally not have detailed knowledge of the interior of systems owned by its trustees. Moreover, they may be changed and updated in a manner not controlled by the trustor. Hence, services provided by environment systems are difficult to analyze due to lack of documentation as well as control. To cope with this lack of knowledge we capture trust levels with respect to the failure of environment systems to provide their services with the required service levels. Each trust level states the degree to which the trustor trusts the required service level of a service to be delivered by the environment system of a trustee.

How conducted: The target model from Step 1.2 is annotated with trust relations. Each trust relation relates a trust level (in the interval $[0, 1]$) determined by the trustor to a required service level of a service provided by an environment system to a target system.

Input documentation: The target model from Step 1.2.

Output documentation: The target model from Step 1.2 annotated with trust relations.

Modeling guideline: Figure 6 shows the target model in Figure 5 annotated with trust relations. The trust relations are shown with dotted clouds. Each cloud is assigned to a required service level of a service provided by an environment system to a target system.

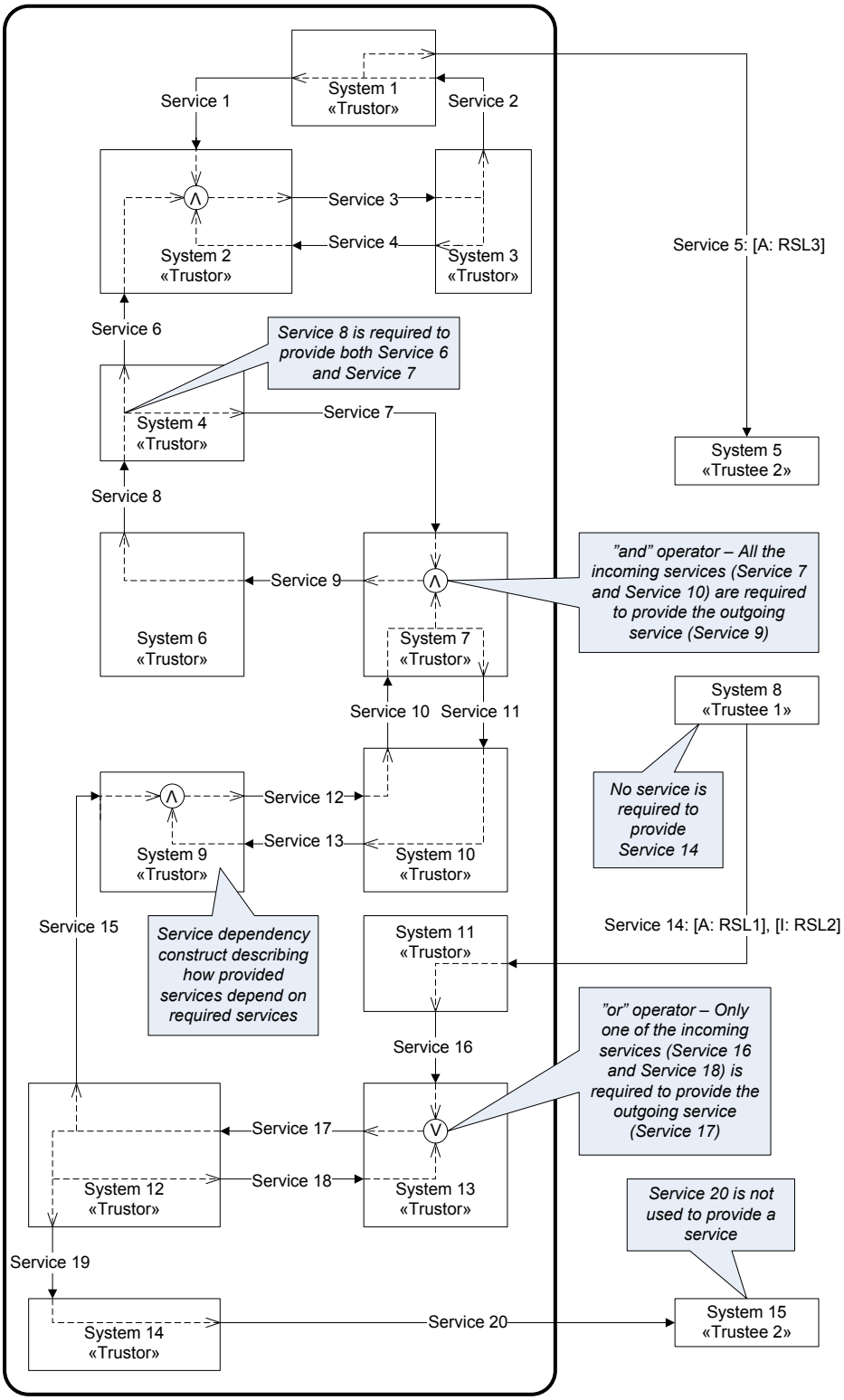


Figure 5: Target model annotated with service dependencies

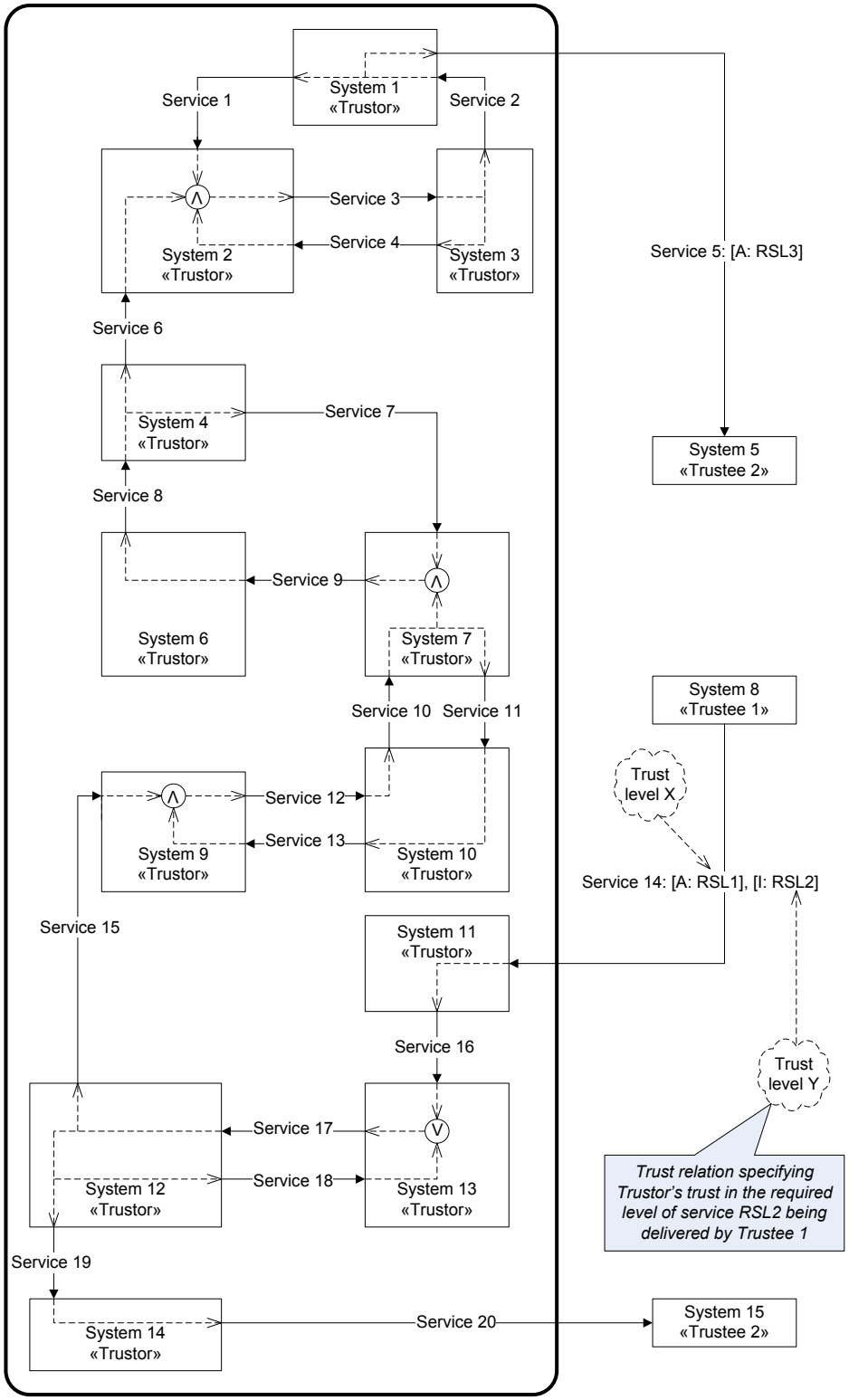


Figure 6: Target model annotated with trust relations

3.2 Step 2: Analyze the impact of service dependencies on risk to quality of provided services

3.2.1 Step 2.1: Identify quality assets to be analyzed

Objective: Identify the quality assets for which impact of service dependencies should be analyzed.

Rationale: The trustor wants to protect the quality of the services provided to its trustees, i.e., ensure that they are provided according to their required service levels. By identifying quality assets we restrict the identification of risks caused by service dependencies to only those risks that may harm the quality of the services provided by the trustor to its trustees. By doing so, we ensure that the available time and resources are spent identifying the most critical and important risks for the trustor in question.

How conducted: For each provided service, the trustor identifies the quality assets for which protection is required. A quality asset is identified for each area of service scope of a provided service for which a required service level has been defined. The value of a quality asset is reduced if the service level becomes less than the required service level.

Input documentation: Target model from Step 1.3.

Output documentation: A list of quality assets for each provided service.

3.2.2 Step 2.2: Construct high-level threat diagrams of the impact of service dependencies on identified quality assets

Objective: Achieve an initial high-level understanding of the impact of service dependencies on the identified quality assets by schematically constructing threat diagrams from the target model.

Rationale: In order to conduct a detailed analysis of the impact of service dependencies on risk to quality of provided services, we first establish an initial high-level understanding of how the failure of individual systems to deliver their services according to requirements may lead to the failure of other individual systems to deliver their services according to requirements. Moreover, we establish how this eventually may lead to unwanted incidents that harm the identified quality assets. Such an initial high-level understanding is achieved by schematically constructing a threat diagram for each provided service.

How conducted: Figure 7 presents a threat diagram that provides an initial overview of how the quality asset "Availability of Service 5 delivered to System 5" may be harmed if the different services represented by the referring threat scenarios are not delivered according to their required service levels. The threat diagram has been schematically constructed from the target model in Figure 6.

We use CORAS [7], which is a model-driven approach to asset-oriented risk analysis, for the modeling and analysis of risk. The threat diagram is expressed in the CORAS language. The referring threat scenarios, vulnerabilities, and the referring unwanted incident have been given names following the conventions "Service X, Z, and Y not delivered according to requirements," "Service X depends on Service Y," and "Incident with impact on the A," (where A is the name

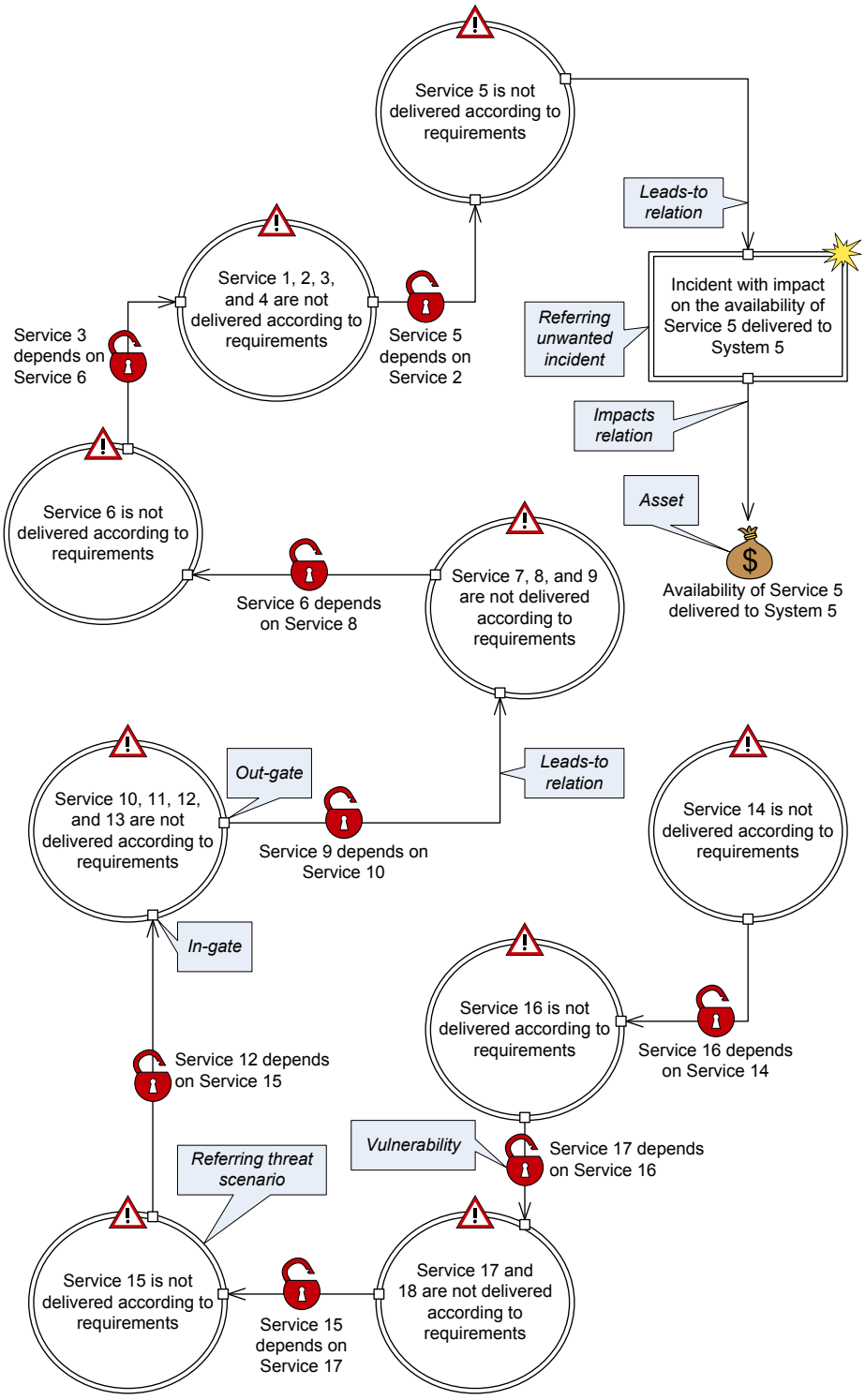


Figure 7: Threat diagram, constructed schematically from the target model in Figure 6, which provides a high-level outline of the impact of service dependencies on the quality asset "Availability of Service 5 delivered to System 5"

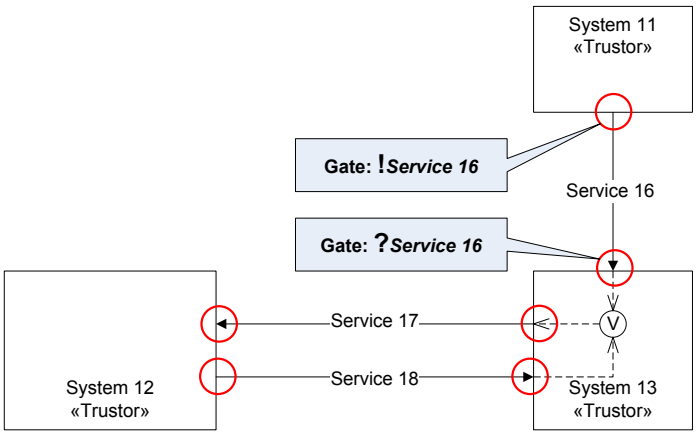


Figure 8: Excerpt of the target model in Figure 6, where dependency gates have been high-lighted

of the asset) respectively. It can also be seen that the vulnerability names only describe direct dependencies between services. Indirect dependencies may be identified by consulting the target model.

For all leads-to relations in the threat diagram, the source and target of the relation is an out-gate and in-gate, respectively. The gates are connected to referring threat scenarios and unwanted incidents. Moreover, the source of each impacts relation is an out-gate, where the out-gate is connected to a referring unwanted incident. In-gates and out-gates are explained in more detail in Step 2.3 of the demonstration of the methodological approach on the example case.

Before we present the schematic procedure used to construct the threat diagram in Figure 7 from the target model in Figure 6, we provide a number of definitions needed for this purpose.

A dependency gate is either the provider gate $!s$ or the consumer gate $?s$ of a service s. A dependency is a pair of dependency gates. This means that a dependency is either of the form $(!s, ?s)$ for some service s, or of the form $(?s, !t)$ where s and t are different services. A dependency path is a totally ordered finite set of dependencies

$$\{(g_1, h_1), (g_2, h_2), \ldots, (g_n, h_n)\}$$

such that for all $0 < j < n, h_j = g_{j+1}$. The gate g' is dependent on the gate g if there is a dependency path

$$\{(g_1, h_1), (g_2, h_2), \ldots, (g_n, h_n)\}$$

such that $g = g_1$ and $g' = h_n$. We then write $g \rightsquigarrow g'$.

In the following we illustrate the relations between dependency constructs, dependency gates, dependencies, and dependency paths. In Figure 8 is an excerpt of the target model in Figure 6, where dependency gates have been high-lighted. We use the short-hand notation s_X to refer to "Service X" in the following. The excerpt has the following dependency gates, dependencies, and dependency paths:

- Dependency gates: $!s_{16}$, $?s_{16}$, $!s_{17}$, $?s_{17}$, $!s_{18}$, and $?s_{18}$.
- Dependencies: $(!s_{16}, ?s_{16})$, $(!s_{17}, ?s_{17})$, $(!s_{18}, ?s_{18})$, $(?s_{16}, !s_{17})$, and $(?s_{18}, !s_{17})$.
- Dependency paths

- of length one: $\{(!s_{16}, ?s_{16})\}$, $\{(!s_{17}, ?s_{17})\}$, $\{(!s_{18}, ?s_{18})\}$, $\{(?s_{16}, !s_{17})\}$, and $\{(?s_{18}, !s_{17})\}$.
- of length two: $\{(!s_{16}, ?s_{16}), (?s_{16}, !s_{17})\}$, $\{(?s_{16}, !s_{17}), (!s_{17}, ?s_{17})\}$, $\{(!s_{18}, ?s_{18}), (?s_{18}, !s_{17})\}$, and $\{(?s_{18}, !s_{17}), (!s_{17}, ?s_{17})\}$.
- of length three: $\{(!s_{16}, ?s_{16}), (?s_{16}, !s_{17}), (!s_{17}, ?s_{17})\}$, and $\{(!s_{18}, ?s_{18}), (?s_{18}, !s_{17}), (!s_{17}, ?s_{17})\}$.

If we had replaced the "or" operator in the dependency construct in Figure 8 with an "and" operator, then we would have ended up with the same dependencies and dependencies paths. We do not distinguish between "and" and "or" operators when identifying dependencies and dependency paths. These operators are only of importance when capturing the impact of dependencies on risk to quality of provided services.

Two gates g_1 and g_2 are mutually dependent iff

$$g_1 \rightsquigarrow g_2 \ \wedge \ g_2 \rightsquigarrow g_1$$

or

$$g_1 = g_2$$

We then write $g_1 \leftrightsquigarrow g_2$. Moreover, we write $g_1 \overset{g}{\leftrightsquigarrow} g_2$ to state that $g_1 \leftrightsquigarrow g_2$ and $g_1 \rightsquigarrow g$ and $g_2 \rightsquigarrow g$. Since $\leftrightsquigarrow$ is a reflexive, symmetric, and transitive relation of the set of gates it follows that $\leftrightsquigarrow$ is an equivalence relation. The same holds for $\overset{g}{\leftrightsquigarrow}$. For any gate g, let $[g]$ be its equivalence class with respect to $\leftrightsquigarrow$. Moreover, we use $[g]_{g'}$ to denote its restriction to $\overset{g'}{\leftrightsquigarrow}$.

For each service s provided by a target system to an environment system, construct a high-level threat diagram from the target model as follows:

1. Introduce the quality assets identified in Step 2.1 for the provided service s.
2. For each of these quality assets, introduce a high-level unwanted incident and connect this to the asset by an impacts relation.
3. Let G_T be the set of all provider gates $!s'$ within the target such that $!s' \rightsquigarrow ?s$.
4. Introduce a high-level threat scenario for each equivalence class $[g]_{?s}$ where $g \in G_T$.
5. Only one of these equivalence classes contains $!s$. Connect its high-level threat scenarios to the high-level unwanted incidents introduced under 2 using leads-to relations.
6. For each pair of different equivalence classes $[g_1]_{?s}$ and $[g_2]_{?s}$ connect their high-level threat scenarios with a leads-to relation decorated by a vulnerability if there is a dependency path $\{(g_1, g), (g, g_2)\}$.
7. Let G_E be the set of all provider gates $!s'$ within the environment such that $\{(!s', g_1), (g_1, g_2)\}$, where $g_2 \in G_T$.
8. Introduce a high-level threat scenario for each $!s' \in G_E$, and connect the scenario to the high-level threat scenario representing the equivalence class $[g_2]_{?s}$ using a leads-to relation decorated by a vulnerability.

In the following we present the results of executing the different steps of the procedure presented above when constructing the high-level threat diagram in Figure 7 from the target model in Figure 6. We use the short-hand notation s_X to refer to "Service X" in Figure 6.

1. The quality asset "Availability of Service 5 delivered to System 5" is introduced.
2. The unwanted incident "Incident with impact on the availability of Service 5 delivered to System 5" is introduced, and connected to the quality asset by an impacts relation.
3. The set $G_T = \{!s_1, \ldots, !s_{13}, !s_{15}, \ldots, !s_{18}\}$ is identified.
4. The following equivalence classes and their respective high-level threat scenarios are identified and introduced, respectively:
   - $[!s_1]_{?s_5} = [!s_2]_{?s_5} = [!s_3]_{?s_5} = [!s_4]_{?s_5} = \{!s_1, !s_2, !s_3, !s_4\}$: "Service 1, 2, 3, and 4 are not delivered according to requirements"
   - $[!s_5]_{?s_5} = \{!s_5\}$: "Service 5 is not delivered according to requirements"
   - $[!s_6]_{?s_5} = \{!s_6\}$: "Service 6 is not delivered according to requirements"
   - $[!s_7]_{?s_5} = [!s_8]_{?s_5} = [!s_9]_{?s_5} = \{!s_7, !s_8, !s_9\}$: "Service 7, 8, and 9 are not delivered according to requirements"
   - $[!s_{10}]_{?s_5} = [!s_{11}]_{?s_5} = [!s_{12}]_{?s_5} = [!s_{13}]_{?s_5} = \{!s_{10}, !s_{11}, !s_{12}, !s_{13}\}$: "Service 10, 11, 12, and 13 are not delivered according to requirements"
   - $[!s_{15}]_{?s_5} = \{!s_{15}\}$: "Service 15 is not delivered according to requirements"
   - $[!s_{16}]_{?s_5} = \{!s_{16}\}$: "Service 16 is not delivered according to requirements"
   - $[!s_{17}]_{?s_5} = [!s_{18}]_{?s_5} = \{!s_{17}, !s_{18}\}$: "Service 17 and 18 are not delivered according to requirements"
5. The high-level threat scenario "Service 5 is not delivered according to requirements" is connected by a leads-to relation to the unwanted incident.
6. The high-level threat scenarios of the following pairs of equivalence classes are connected by leads-to relations decorated by vulnerabilities:
   - $[!s_{17}]_{?s_5}$ and $[!s_{15}]_{?s_5}$ as a result of $\{(!s_{17}, ?s_{17}), (?s_{17}, !s_{15})\}$
   - $[!s_{15}]_{?s_5}$ and $[!s_{12}]_{?s_5}$ as a result of $\{(!s_{15}, ?s_{15}), (?s_{15}, !s_{12})\}$
   - $[!s_{10}]_{?s_5}$ and $[!s_9]_{?s_5}$ as a result of $\{(!s_{10}, ?s_{10}), (?s_{10}, !s_9)\}$
   - $[!s_8]_{?s_5}$ and $[!s_6]_{?s_5}$ as a result of $\{(!s_8, ?s_8), (?s_8, !s_6)\}$
   - $[!s_6]_{?s_5}$ and $[!s_3]_{?s_5}$ as a result of $\{(!s_6, ?s_6), (?s_6, !s_3)\}$
   - $[!s_2]_{?s_5}$ and $[!s_5]_{?s_5}$ as a result of $\{(!s_2, ?s_2), (?s_2, !s_5)\}$
7. The set $G_E = \{!s_{14}\}$ is identified.
8. The high-level threat scenario "Service 14 is not delivered according to requirements" is introduced and connected to the high-level threat scenario "Service 16 is not delivered according to requirements" by a leads-to relation decorated by a vulnerability as a result of $\{(!s_{14}, ?s_{14}), (?s_{14}, !s_{16})\}$.

Input documentation:

- The target model from Step 1.3.
- The identified quality assets from Step 2.1.

Output documentation: One high-level threat diagram outlining the impact of service dependencies on the quality assets for each provided service.

3.2.3 Step 2.3: Construct detailed threat diagrams of the impact of service dependencies on identified quality assets

Objective: Achieve a detailed understanding of the impact of service dependencies on the identified quality assets.

Rationale: The threat diagrams from Step 2.2 provide only a high-level outline of the impact of service dependencies on the identified quality assets. To establish a risk picture that can be monitored, we need to detail those diagrams.

How conducted: In Figure 9 is a threat diagram (where some of the details have been suppressed) that shows part of the result of detailing the high-level threat diagram in Figure 7.

We detail the high-level constructs, one by one, by following the instructions given in [7]. We only deviate from these instructions when detailing leads-to relations. A leads-to relation between two high-level constructs is detailed by decomposing it. If vulnerabilities are assigned to the leads-to relation being detailed, then the detailing also involves the decomposition of those vulnerabilities. It should be noticed that if the vulnerability represents the dependency of target services on an environment service, then the vulnerability is decomposed into as many vulnerabilities as there are required service levels associated with the environment service. For example, the vulnerability "Service 16 depends on Service 14" in Figure 7 has been decomposed into the two vulnerabilities "Service 16 depends on availability of Service 14" and "Service 16 depends on integrity of Service 14"; one for each of the required service levels associated with "Service 14."

As a result of the decomposition of the high-level vulnerabilities, the referring threat scenarios, and the referring unwanted incident in Figure 7, the high-level in-gates and out-gates and the impacts relation in Figure 7 have been decomposed, and likelihood values and consequences values have been assigned to the gates and impacts relations, respectively. For each out-gate being the source of a leads-to relation associated with a vulnerability representing the dependence of target services on a particular area of service scope of an environment service, we estimate the likelihood of the required service level not being delivered. This is done by first calculating the worst-case service level of the particular area of service scope. The worst-case service level specifies our minimum expectation to the particular area of service scope. It is calculated based on the required service level and the trust level calculated in Step 1.3. The likelihood is then estimated based on the difference between the required service level and the worst case service level.

As part of this step, we also specify scales for measuring likelihood and consequence, and functions for calculating risk values. The risk functions are used after we have created the detailed threat diagrams to determine the risk values of the different risks to quality of provided services. A risk value is determined based on the likelihood of an unwanted incident and its consequence with respect to a quality asset.

Input documentation:

- The high-level threat diagrams from Step 2.2.
- Target model from Step 1.3.

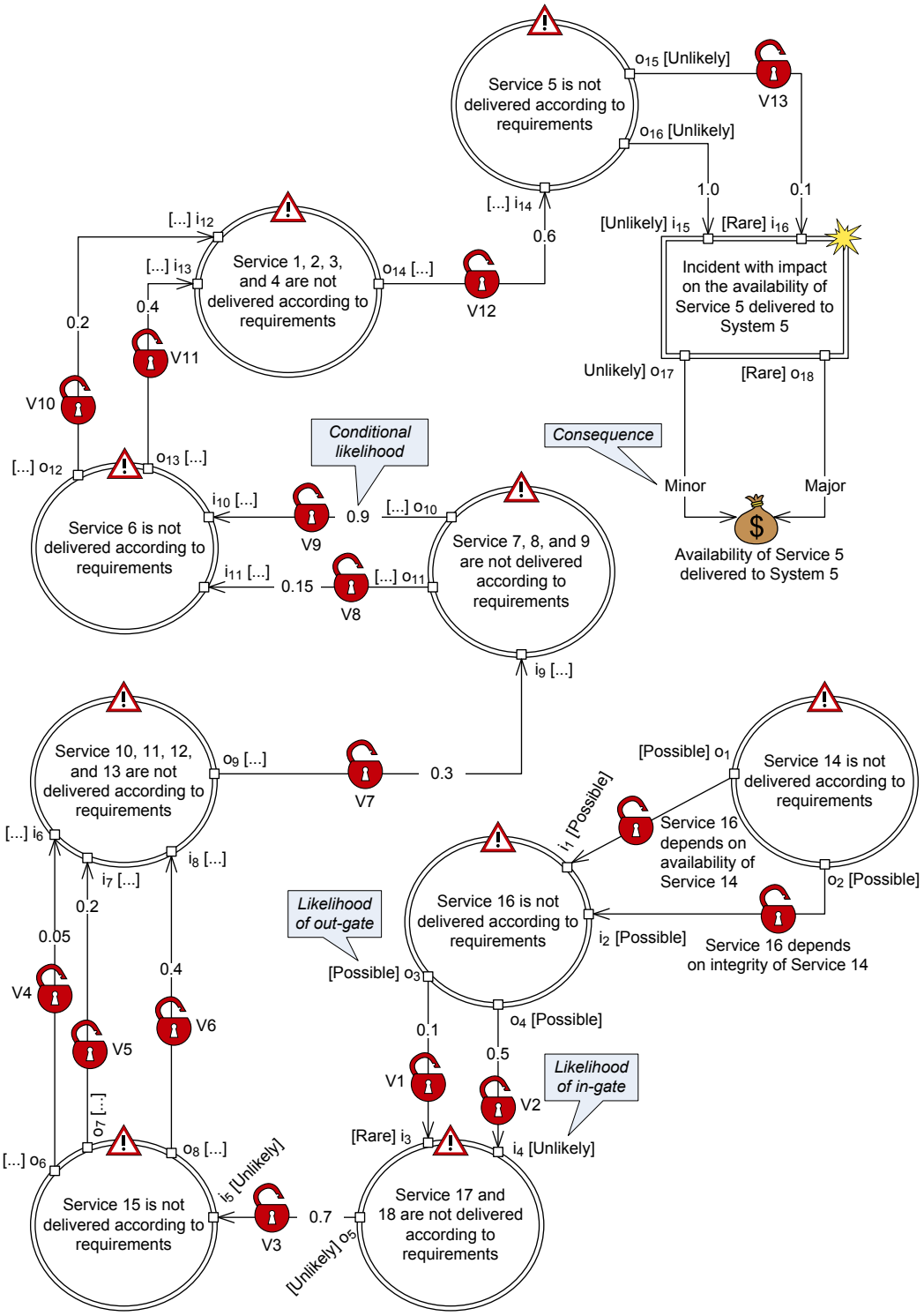


Figure 9: Threat diagram that shows part of the result of detailing the threat diagram in Figure 7

Output documentation:

- Detailed threat diagrams documenting the impact of service dependencies on the quality assets.
- Worst-case service levels.
- Scales for measuring likelihood and consequence.
- Risk functions for calculating risk values.
- A list of risks to quality of provided services.

3.3 Step 3: Identify indicators for interconnected systems

3.3.1 Step 3.1: Identify risks to be monitored

Objective: Identify the risks to quality of provided services that should be monitored.

Rationale: A risk analysis will often result in a number of identified risks to quality of provided services. We need to identify the risks that should be monitored, since it is often not in the trustor's interest to monitor all the risks. Moreover, there may be risks for which monitoring is not feasible.

How conducted: For each risk resulting from Step 2.3, we must decide whether it should be monitored. Typically, a risk to quality of provided services is selected for monitoring if it is believed that the likelihood and/or consequence value determining its risk value is likely to change in a manner that will considerably harm the trustor. A risk may also be selected for monitoring if we are uncertain about the risk value.

Input documentation:

- The detailed threat diagrams from Step 2.3.
- The list of risks to quality of provided services from Step 2.3.

Output documentation: A list of risks to quality of provided services to be monitored.

3.3.2 Step 3.2: Identify relevant indicators for the risks to be monitored

Objective: Identify relevant indicators for monitoring the risk values of the risks to be monitored.

Rationale: To monitor changes in risk values we need to identify indicators. The indicators are calculated from measurable properties of the interconnected systems.

How conducted: For the risks identified to be monitored in Step 3.1, we identify relevant indicators. Indicators for monitoring consequence are related to impacts relations between unwanted incidents and quality assets. On the other hand, indicators for monitoring likelihood may not only be related to unwanted incidents, but also to vulnerabilities and threat scenarios leading up to an incident, since the likelihoods of vulnerabilities being exploited and threat scenarios occurring will affect the likelihood of the unwanted incident occurring.

Basic indicators are identified for the different likelihood and consequence values to be monitored. If more than one basic indicator is needed for monitoring a consequence or likelihood value, then a composite indicator, aggregating the basic indicators, is also identified.

Input documentation:

- The list of risks to quality of provided services to be monitored from Step 3.1.
- The detailed threat diagrams from Step 2.3.

Output documentation: A set of relevant basic and composite indicators for monitoring likelihood and consequence.

3.4 Step 4: Specify design and deployment of identified indicators for interconnected systems

3.4.1 Step 4.1: Specify design of indicators for risk monitoring

Objective: Specify how basic and composite indicators for monitoring likelihood and consequence values should be designed.

Rationale: We need to specify how the identified basic and composite indicators from Step 3.2 should be designed, i.e., how they should be calculated, in order to be useful for monitoring.

How conducted: A design specification, in the form of an algorithm, is provided for each indicator identified in Step 3.2. It specifies the data needed for calculating the indicator, how the indicator should be calculated, and the output from the calculation. Assuming the likelihood and consequence intervals obtained in Step 2.3 are correct, the algorithm should yield likelihoods and consequences in these intervals when applied to the basic indicator values at the time these intervals were determined.

Input documentation:

- The list of risks to quality of provided services to be monitored from Step 3.1.
- The relevant indicators identified in Step 3.2.
- The detailed threat diagrams from Step 2.3.
- Basic indicator values from the time when the detailed threat diagrams were constructed.

Output documentation: A design specification for each indicator identified in Step 3.2.

3.4.2 Step 4.2: Specify deployment of indicators for risk monitoring

Objective: Specify how basic and composite indicators for monitoring likelihood and consequence values should be deployed in the interconnected systems.

Rationale: We need to specify how the identified basic and composite indicators from Step 3.2 should be deployed in the interconnected systems, i.e., how the data needed to calculate the different indicators should be extracted and transmitted within the interconnected systems, in order to be useful for monitoring.

How conducted: A deployment specification is provided for each indicator identified in Step 3.2. It specifies how the data needed to calculate the indicator should be extracted and transmitted within the interconnected systems.

Input documentation: The design specifications from Step 4.1.

Output documentation: A deployment specification for each indicator.

4 Demonstration of Step 1: Document interconnected systems

We consider an SoS consisting of an electrical power production infrastructure (EPP), a public telecom infrastructure (PTI), and an electrical power grid (EPG). In the following we assume that we as analysts have been hired by the company in charge of the electrical power production infrastructure, Client EPP, to help capture and monitor the impact of service dependencies on the quality of the services that Client EPP provides to the parties in charge of the public telecom infrastructure and the electrical power grid.

4.1 Step 1.1: Model interconnected systems

Figure 10 documents the electrical power production infrastructure and its environment. The different systems provide and/or require electricity (*elec*), control instructions (*cinstr*), and sensor data (*sdata*). All the services with the exception of the electricity services are data services. For each electricity service, we provide a required service level for availability. Each required service level is a conjunction of availability with respect to time and availability with respect to the amount of electricity (in megawatt hours (MWh)) that needs to be delivered. Both these availability requirements are for the period of one year. The required service levels for electricity services take into account that service disruptions may occur. For instance, consider the electricity service provided by "Distribution line 3" to "Private telecom system." The "Private telecom system" will not experience any disruptions of the service if the availability with respect to time is 100% (available 8760 hours per year) and if the availability with respect to electricity delivered is 22 MWh. The latter is an estimate for the amount of electricity that "Private telecom system" needs during the period of one year.

For the data services, the required service levels (also for the period of one year) are specified in terms of percentages of all sensor data/control instructions messages that are sent. We can for instance specify the percentages of all sent data messages that need to be delivered (availability), be delivered with integrity, and comply with the data confidentiality policy of Client EPP. In Section 5.2 we explain what it means to comply with the data confidentiality policy. An integrity requirement cannot be higher than the availability requirement for the same service, since each integrity requirement specifies the percentage of all sent data messages that needs

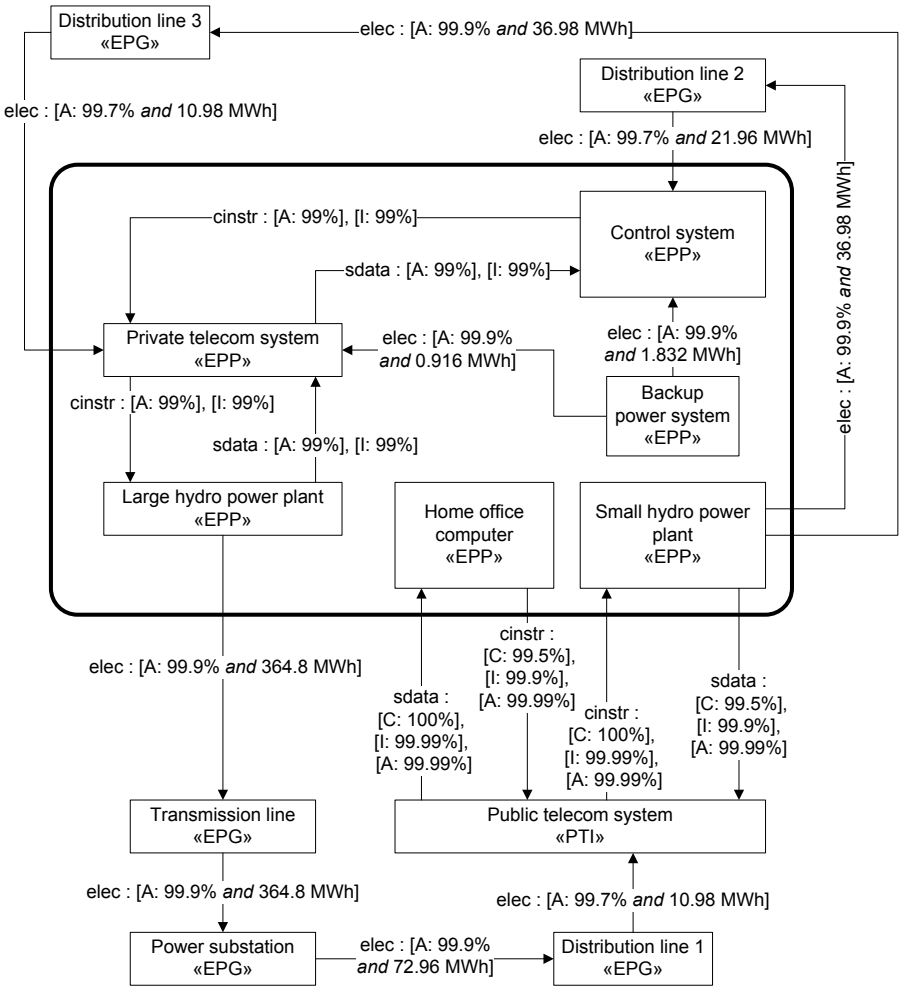


Figure 10: Target model for the electrical power production infrastructure and its environment

to be delivered with integrity. Thus, the integrity requirement is equal to or less than the availability requirement for each data service in Figure 10. For Client EPP, the integrity of a data message is only important if it is delivered. On the other hand, confidentiality is important for both data messages that are delivered and data messages that are lost during transmission. A data message can for instance be intercepted by an outsider before it is lost during transmission. Thus, the confidentiality requirement may be higher than the availability requirement for the same service.

In the electrical power production infrastructure there is a "Large hydro power plant." The electrical power produced by this plant is transmitted on a high-voltage "Transmission line" to a "Power substation." Here, the power is transformed to low-voltage power by a transformer, before being distributed to its end-users by distribution lines. "Distribution line 1" provides electrical power to the "Public telecom system." The infrastructure also consists of a "Small hydro power plant." This power plant distributes power directly to its end-users by the use of "Distribution line 2" and "Distribution line 3." "Private telecom system" and "Control system," both located within the electrical power production infrastructure, are two of the end-users that receive electrical power from these two distribution lines. These two systems share a "Backup power system," which is used when the electrical power grid fails to provide electricity to one or both systems.

The "Control system" is used to operate the "Large hydro power plant." By the use of the "Private telecom system" it sends control instructions to the plant, while sensors at the plant send data to the "Control system" through the same telecom system. The "Control system" responds to errors arising at the plant. If it cannot resolve the errors, it will shut down the plant to protect equipment. If the connection to the "Control system" is lost, the plant will automatically shut down if it cannot resolve errors by itself. The required service level with respect to availability is 99% for all the data services exchanged between the "Control system" and the "Large hydro power plant," since the plant has some ability of operating independently of the "Control system." Moreover, the required service level with respect to integrity is 99% for all the data services.

Due to its size, the "Small hydro power plant" is operated by a system operator from his "Home office computer." The operator uses a computer that is dedicated to this task. He sends encrypted control instructions to the plant through the "Public telecom system," while the sensors at the plant sends encrypted data to the operator through the same telecom system. The encrypted communication is achieved through the use of symmetric-key cryptography. The system operator responds to errors arising at the plant. If he cannot resolve the errors, he will shut down the plant to protect equipment. If the connection to the "Public telecom system" is lost, the plant will automatically shut down to protect equipment. This is done as a precautionary step, since the plant is not able to resolve errors by itself. Since the availability of the data services exchanged between the "Small hydro power plant" and the "Home office computer" are crucial for the operation of the "Small hydro power plant," the required service level for all the data services with respect to availability is 99.99%. It should be noticed that the integrity and confidentiality requirements for data services provided by "Public telecom system" to "Home office computer" and "Small hydro power plant" do not specify explicit requirements that "Public telecom system" needs to fulfill when providing the data services. It is more correct to say that these requirements are to the data messages themselves. Client EPP requires that data messages' compliance with the data confidentiality policy and data messages' integrity should not be changed while at "Public telecom system" or during transmission to its destinations. Notice that only the confidentiality requirements have been set to 100% in Figure 10. The integrity requirements would have been set to 100% too, but this is not possible since the availability requirements equal 99.99% in both cases.

4.2 Step 1.2: Capture service dependencies

In Figure 11, the target model in Figure 10 is annotated with the service dependencies. Most of the service dependencies are self-explanatory, but note especially that "Small hydro power plant" depends on the availability of control instructions, provided by "Home office computer," to produce electricity. The "Large hydro power plant" is less dependent on control instructions than the "Small hydro power plant," but since it depends on control instructions in situations where it cannot resolve errors, there is a dependency between the required control instructions service and the electricity service provided to "Transmission line." It should also be noticed that both "Private telecom system" and "Control system" can require electricity from the "Backup power system" if the electrical power grid fails to provide electricity, and that incoming sensor data messages may affect the outgoing control instructions messages, and vice versa. The dependencies between incoming and outgoing messages are a result of control instructions messages often being created based on the incoming sensor data messages, and that control instructions messages affect the operation of "Small hydro power plant" and its data sensors, which again affect the outgoing sensor data messages.

4.3 Step 1.3: Capture trust relations

In Figure 12, the target model in Figure 11 is annotated with trust relations. As can be seen in the figure, trust levels have been assigned to the required service levels for those services that are provided by systems of the environment to systems of the target.

All the services for which trust levels should be assigned are considered very reliable by Client EPP. Thus, it is expected that they should achieve their required service levels. Even so, Client EPP is aware that the services can fail. After having considered both the high reliability of the services and the possibility of service failures, Client EPP assigns high trust levels to the different required service levels.

For the control instructions service provided by "Public telecom system" to "Small hydro power plant," Client EPP has a trust of:

- 0.97 in that the control service is delivered according to the confidentiality requirement;
- 0.95 in that the control service is delivered according to the integrity requirement; and
- 0.99 in that the control service is delivered according to the availability requirement.

5 Demonstration of Step 2: Analyze the impact of service dependencies on risk to quality of provided services

5.1 Step 2.1: Identify quality assets

For the sake of simplicity, we demonstrate the method by only identifying quality assets for one of the provided services. In Appendices A–C we demonstrate the method on the other provided services.

A concern of Client EPP is that services dependencies in the SoS may affect the ability of "Small hydro power plant" to provide the sensor data service according to the quality requirements associated with the service. If this service is affected, then the ability of "Home office computer" to control and operate the "Small hydro power plant" may be affected as well, which again may impact the electricity services provided to "Distribution line 2" and "Distribution line 3." Client EPP therefore seeks to protect the quality assets "Confidentiality of sensor data delivered to Public telecom system," "Integrity of sensor data delivered to Public telecom system,"

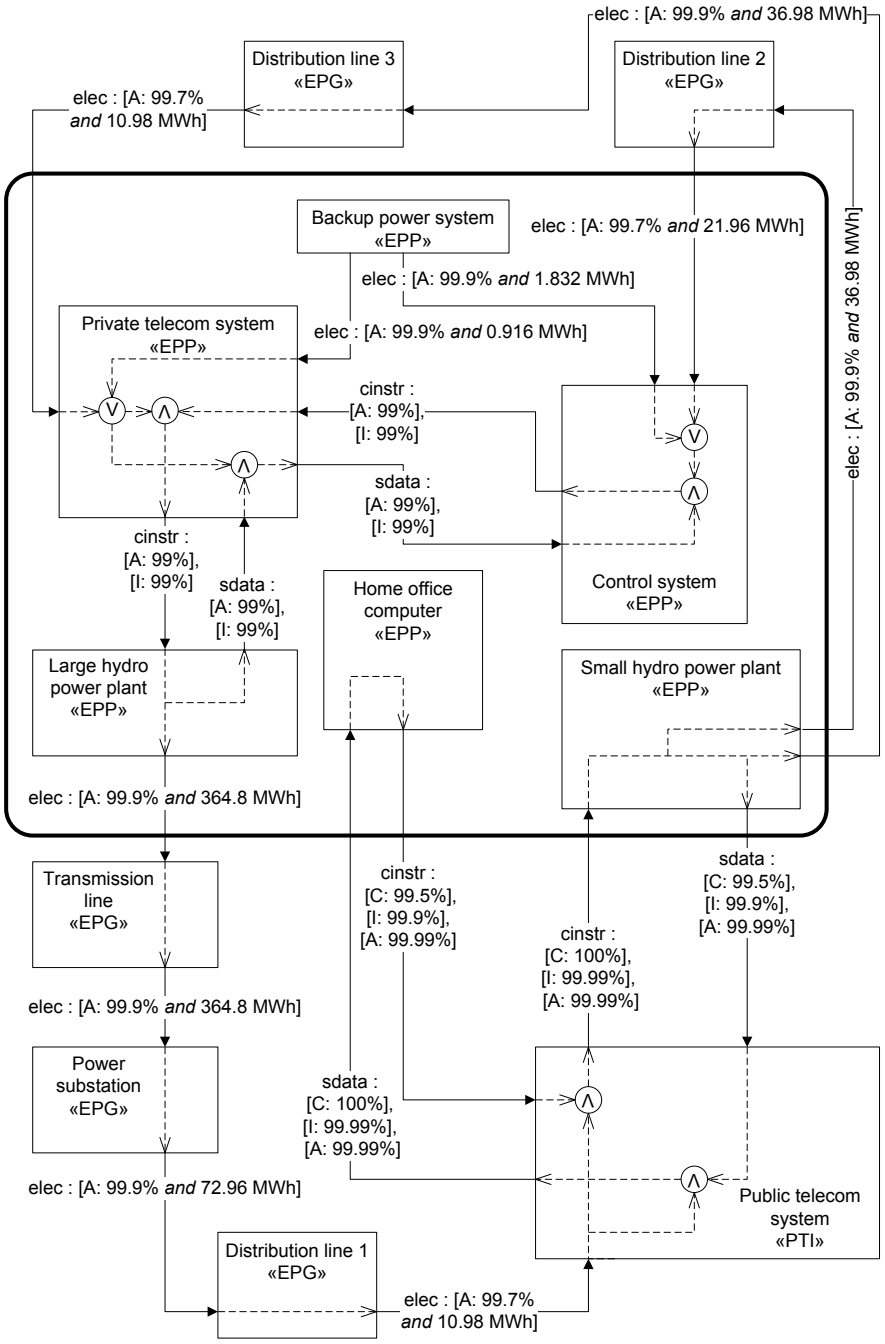


Figure 11: Target model annotated with service dependencies

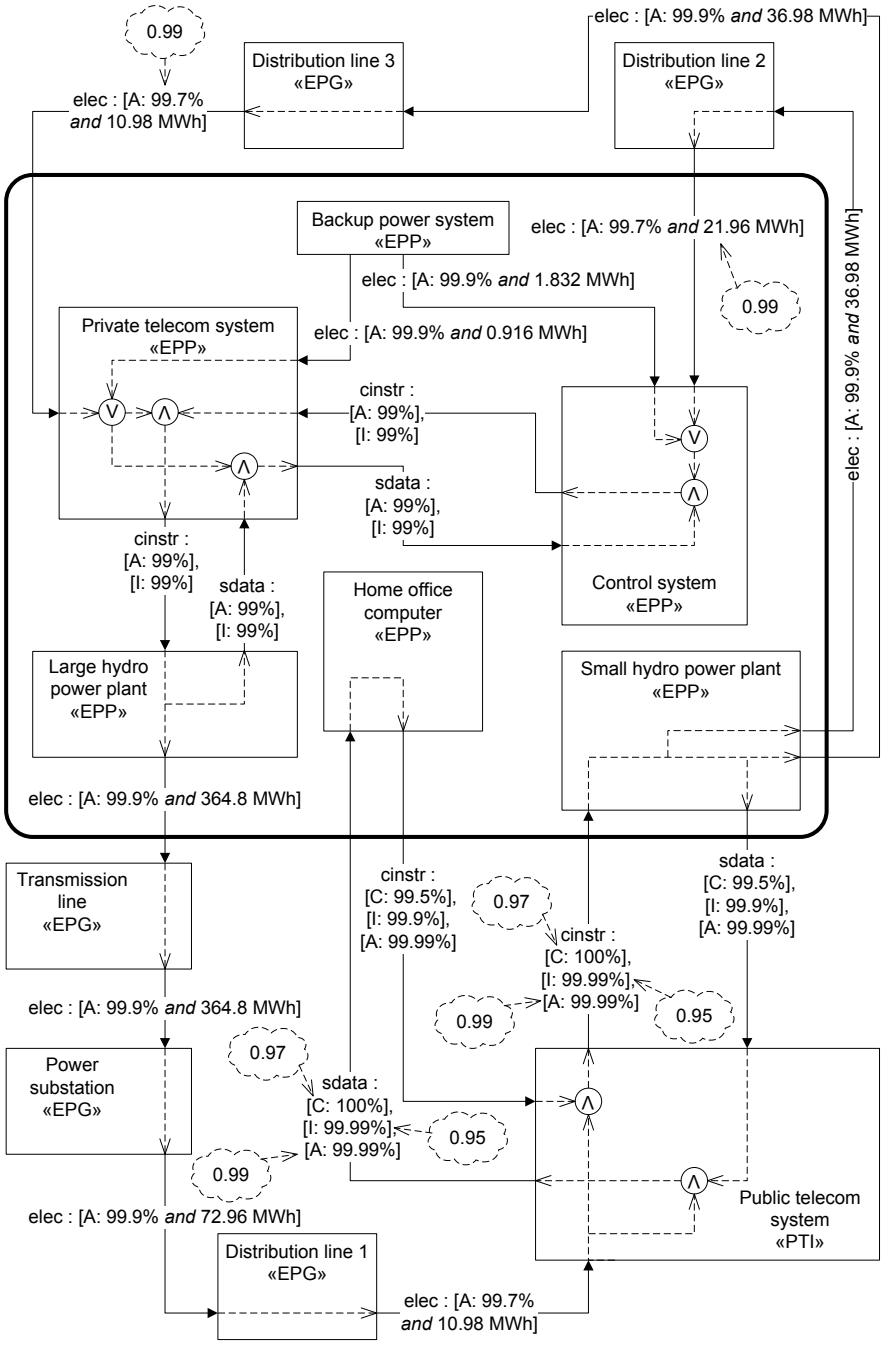


Figure 12: Target model annotated with trust relations

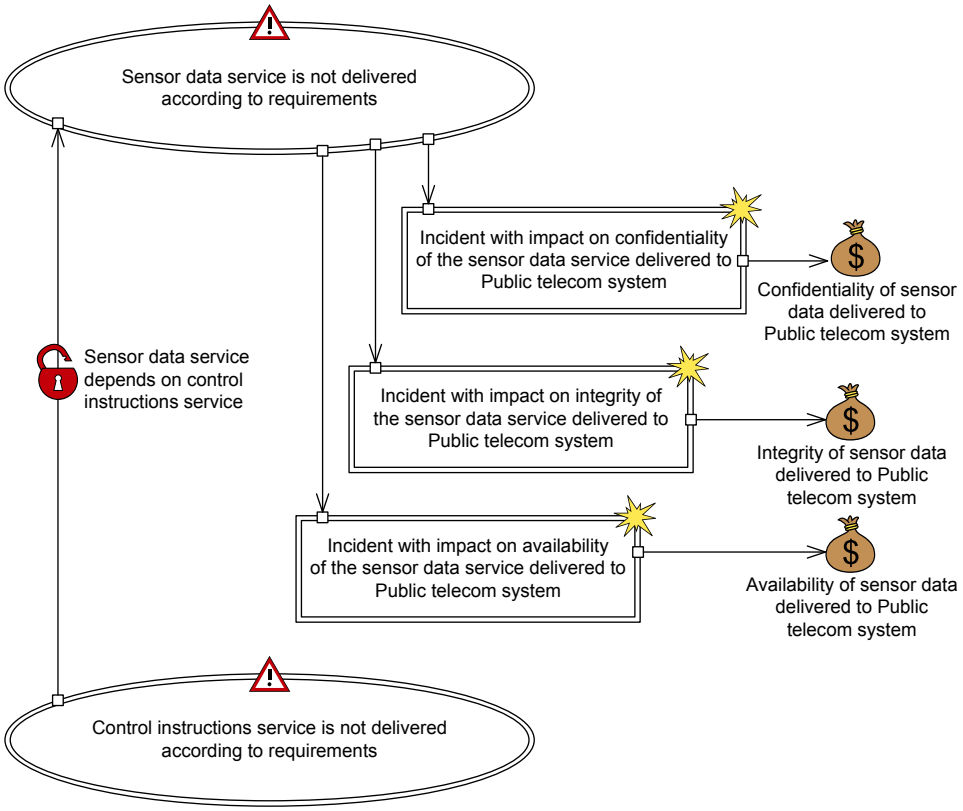


Figure 13: Threat diagram, constructed schematically from the target model in Figure 12, which provides a high-level outline of the impact of service dependencies on the quality of the sensor data service provided by "Small hydro power plant" to "Public telecom system"

and "Availability of sensor data delivered to Public telecom system," and wants to identify the service dependencies' impact on these quality assets.

5.2 Step 2.2: Construct high-level threat diagrams of the impact of service dependencies on identified quality assets

For the sensor data service provided to "Public telecom system," the high-level threat diagram in Figure 13 has been constructed schematically from the target model in Figure 12. The threat diagram provides a high-level description of the impact of service dependencies on the quality of the sensor data service provided to "Public telecom system." In the threat diagram we use the abbreviations "sensor data service" and "control instructions service" to refer to the sensor data service provided by "Small hydro power plant" to "Public telecom system" and the control instructions service provided by "Public telecom system" to "Small hydro power plant," respectively.

5.3 Step 2.3: Construct detailed threat diagrams of the impact of service dependencies on identified quality assets

Before we perform the detailed risk analysis of how target systems may fail to provide services according to requirements, we need to establish how to measure likelihood and consequence, as well as defining the risk function. Table 1 shows how likelihood is measured, while Table 2 shows how consequence is measured for the different quality assets.

Table 1: Likelihood scale

Likelihood	**Description**
Certain	Fifty times or more per year $[500, \infty\rangle : 10$ years
Very likely	Ten to fifty times per year $[100, 499] : 10$ years
Likely	Five times to ten times per year $[50, 99] : 10$ years
Possible	Two to five times per year $[20, 49] : 10$ years
Unlikely	Once a year $[6, 19] : 10$ years
Very unlikely	Less than once per year $[2, 5] : 10$ years
Rare	Less than once per ten years $[0, 1] : 10$ years

There is need to clarify what we mean with "lack of integrity" and "do not comply with the data confidentiality policy." ISO/IEC 27000 [10] defines confidentiality as the *"property that information is not made available or disclosed to unauthorized individuals, entities, or processes,"* while it defines integrity as the *"property of protecting the accuracy and completeness of assets."* In our case, asset refers to information. In the case of confidentiality, it may be extremely difficult to detect whether information contained in a sensor data message or control instructions message have been made available or been disclosed to unauthorized individuals, entities, or processes. Instead of focusing on whether the information has been disclosed, we focus on how the information is protected against disclosure. If a sensor data message or control instructions message comes with strong protection against disclosure of the information contained in the message, then it likely that the information will remain confidential during transmission. Client EPP has a data confidentiality policy that defines what it means for information in a sensor data message or in a control instructions message to be well-enough protected against disclosure. At Client EPP, all sent messages should comply with this policy. The information is, for instance, not well-enough protected if: the message is sent in clear text; the cryptographic algorithm used has flaws which makes it vulnerable to attacks; the cryptographic key used has been disclosed, has a long life-span, or has been incorrectly generated; etc.

In the case of "lack of integrity," we say that a sensor data message or a control instructions message has lack of integrity if: the information contained in the message has been changed deliberately or by accident during transmission, processing, or storage of the message; the message has not been created and sent by one of Client EPP's systems; or the message has been created based on data that is not correct with respect to the true state of the object represented by the data. With respect to the latter, a sensor data message may be created based on incorrect sensor data, while control instructions may be created based on sensor data that is not correct with respect to the true state of a power plant.

To calculate the number of sensor data messages that are not delivered, delivered with lack of integrity, or that do not comply with the data confidentiality policy, it is helpful to have an estimate of the number of sensor data messages sent from "Small hydro power plant" in the period of one year. Client EPP estimates this number to be 5000.

Table 2: How consequence is measured for the three quality assets

Availability of sensor data delivered to Public telecom system
Number of sensor data messages that are not delivered
Confidentiality of sensor data delivered to Public telecom system
Number of sensor data messages sent that do not comply with the data confidentiality policy
Integrity of sensor data delivered to Public telecom system
Number of sensor data messages that are delivered with lack of integrity

For all the risks, the risk is classified as acceptable or unacceptable as follows:

$$Expected\ service\ level = \frac{Maximum\ service\ level - (Likelihood \cdot Consequence)}{Maximum\ service\ level} \quad (1)$$

$$\textbf{if}\ Expected\ service\ level \geq \frac{Required\ service\ level}{Maximum\ service\ level}\ \textbf{then} \quad (2)$$
$$\quad Risk\ value = Acceptable$$
$$\textbf{else}$$
$$\quad Risk\ value = Unacceptable$$
$$\textbf{endif}$$

Here, the *Maximum service level* is the highest achievable service level for the area of service scope associated with the quality asset in question. For example, the highest achievable service level for the integrity of the sensor data service is 5000. This means that all the 5000 sensor data messages sent during the period of one year are delivered with integrity. A risk associated with a quality asset is *Unacceptable* if the *Expected service level* is less than $\frac{Required\ service\ level}{Maximum\ service\ level}$.

In Figure 14 is the detailed version of the high-level threat diagram in Figure 13. The referring elements in Figure 14 refer to the referenced threat scenarios provided in Figures 15 and 16, and the referenced unwanted incidents provided in Figure 20. Moreover, the referenced threat scenario in Figure 16 contains three referring threat scenarios, which refer to the referenced threat scenarios provided in Figures 17–19. Client EPP has estimated all the likelihood and consequence values in the different figures.

We refer to i_x and o_y of the referring threat scenarios and unwanted incidents as in-gate and out-gate, respectively. Relations to an element inside a referenced threat scenario must go through an in-gate, while relations to an element outside the referenced threat scenario must go through an out-gate. The likelihood value of an in-gate i_x documents the contribution of an element outside the referenced threat scenario via gate i_x to the likelihood of an element inside the referenced threat scenario, while the likelihood of the out-gate o_y documents the contribution of the likelihood of an element inside the referenced threat scenario via gate o_y to the likelihood of an element outside the referenced threat scenario.

Below we provide some examples of the semantics of elements and relations in the different figures. For more information on the semantics of the CORAS language, see [7].

- *Threat scenario*: Threat scenario "Control instructions message is not delivered" occurs with likelihood "Very likely" (Figure 17).
- *Leads-to relation (with conditional likelihood)*: "Invalid control instructions are used by the Small hydro power plant" leads to "Small hydro power plant starts to operate in an incorrect state" with conditional likelihood "0.1" (Figure 18).

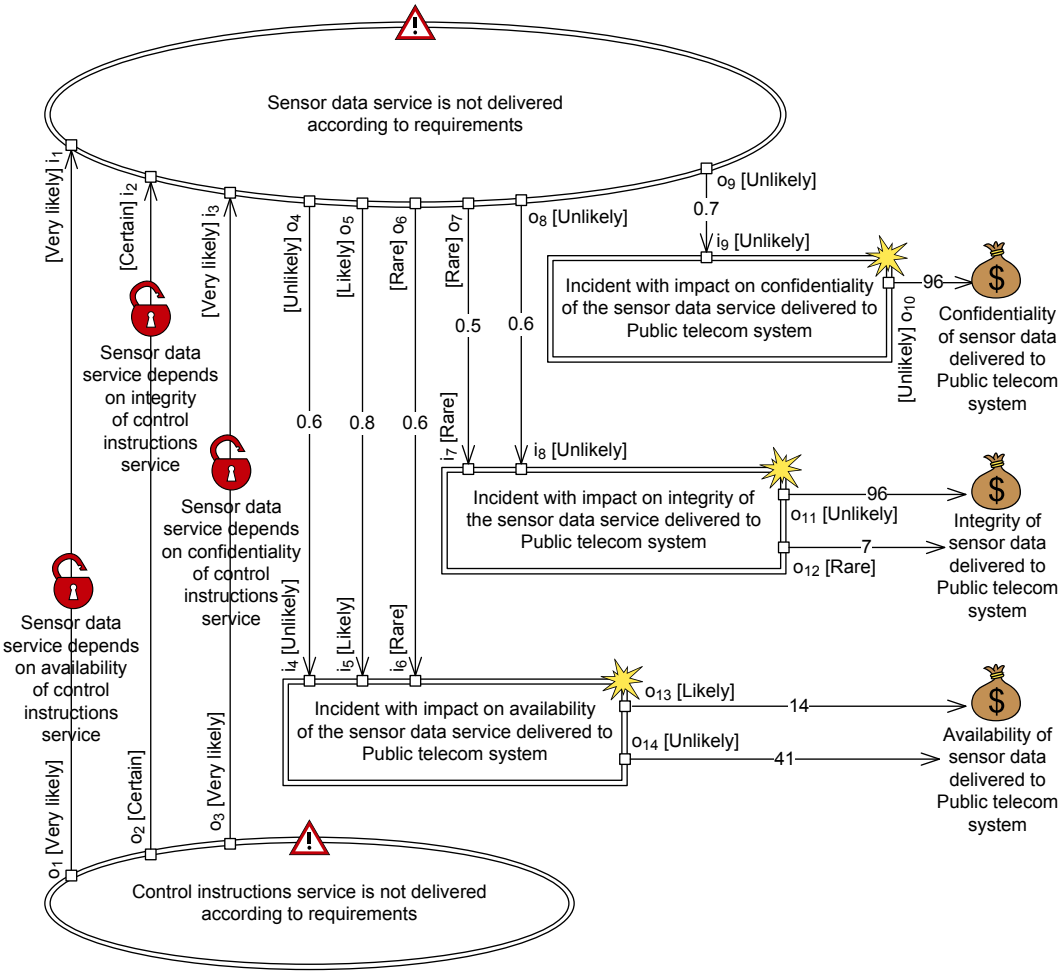


Figure 14: Detailed version of the high-level threat diagram in Figure 13

- *Leads-to relation (with vulnerability)*: "Control instructions message is delivered, where its integrity has been changed during transmission or while at Public telecom system" leads to "Re-transmission of control instructions message is not requested" with conditional likelihood "0.001," due to vulnerability "Possible that checksum algorithm fails to detect integrity violations" (Figure 18).

- *In-gate (with likelihood)*: i_1 is an in-gate with likelihood "Very likely" (Figure 14).

- *Out-gate (with likelihood)*: o_1 is an out-gate with likelihood "Very likely" (Figure 14).

- *Leads-to relations (between elements of referenced threat scenarios)*: "Control instructions service is not delivered by Public telecom system according to the availability requirement that Public telecom system is required to fulfill" leads to "Control instructions message is not delivered" via gates o_1, i_1, and i_{10}, due to vulnerability "Small hydro power plant depends on availability of control instructions" (Figures 14–17).

- *Unwanted incident*: Unwanted incident "Sensor data is sent in plain text from Small hydro power plant to an outsider" occurs with likelihood "Unlikely" (Figure 20).

- *Impacts relation (between element of referenced unwanted incident and asset)*: "Sensor data is sent in plain text from Small hydro power plant to an outsider" impacts "Confidentiality of sensor data delivered to Public telecom system" via gate o_{10} with consequence "96" (Figures 14 and 20).

As can be seen in Figure 14, the vulnerability "Sensor data service depends on control instructions service" in Figure 13 has been decomposed into three vulnerabilities. The referenced threat scenario in Figure 15 is a detailing of the referring threat scenario "Control instructions service is not delivered according to requirements" in Figure 13. Since "Public telecom system" is only required to deliver the control instructions service according to the availability requirement, the referenced threat scenario distinguish between the failure of not achieving the availability requirement, and the failures of not achieving the confidentiality and integrity requirements.

Client EPP estimates that 1000 control instructions messages are sent each year to "Small hydro power plant." Before we can estimate the likelihoods of the control instructions service not being delivered according to the confidentiality, integrity, and availability requirements, we need to calculate the worst-case service levels (required service level $\times$ trust level) of the control instructions service delivered by "Public telecom system." These are as follows:

- $100\% \cdot 0.97 = 97\%$ of the sent control instructions messages do comply with the data confidentiality policy;

- $99.99\% \cdot 0.95 = 94.99\%$ of the sent control instructions messages are delivered with integrity; and

- $99.99\% \cdot 0.99 = 98.99\%$ of the sent control instructions messages are delivered.

To estimate the likelihoods we use the estimated number of control instructions messages sent each year in combination with the required and worst-case service levels of the control instructions service delivered by "Public telecom system." The required service levels specify that:

- $1000 \cdot 100\% = 1000$ of the sent control instructions messages should comply with the data confidentiality policy;

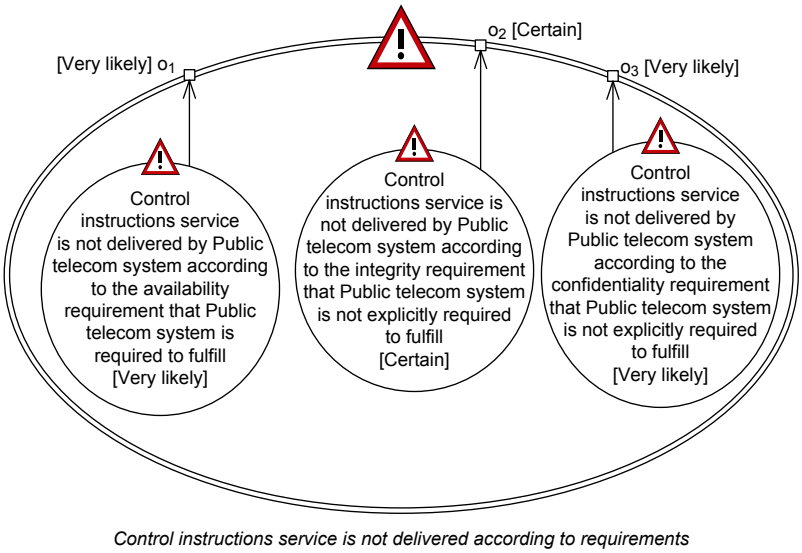


Figure 15: The referenced threat scenario "Control instructions service is not delivered according to requirements," referred to in Figure 14

- $1000 \cdot 99.99\% = 999.9$ of the sent control instructions messages should be delivered with integrity; and
- $1000 \cdot 99.99\% = 999.9$ of the sent control instructions messages should be delivered.

On the other hand, our expectations according to the worst-case service levels are that:

- $1000 \cdot 97\% = 970$ out of the required 1000 control instructions messages comply with the data confidentiality policy;
- $1000 \cdot 94.99\% = 949.9$ out of the required 999.9 control instructions messages are delivered with integrity; and
- $1000 \cdot 98.99\% = 989.9$ out of the required 999.9 control instructions messages are delivered.

Based on the calculations for required and worst-case service levels, we end up with the following likelihoods:

- The likelihood of the control instructions service not being delivered according to the confidentiality requirement is "Very likely" ($1000 - 970 = 30$ control instructions messages in the period of a year).
- The likelihood of the control instructions service not being delivered according to the integrity requirement is "Certain" ($999.9 - 949.9 = 50$ control instructions messages in the period of a year).
- The likelihood of the control instructions service not being delivered according to the availability requirement is "Very likely" ($999.9 - 989.9 = 10$ control instructions messages in the period of a year).

The referenced threat scenario "Sensor data service is not delivered according to requirements" is given in Figure 16. The internal threat behavior of "Small hydro power plant" is

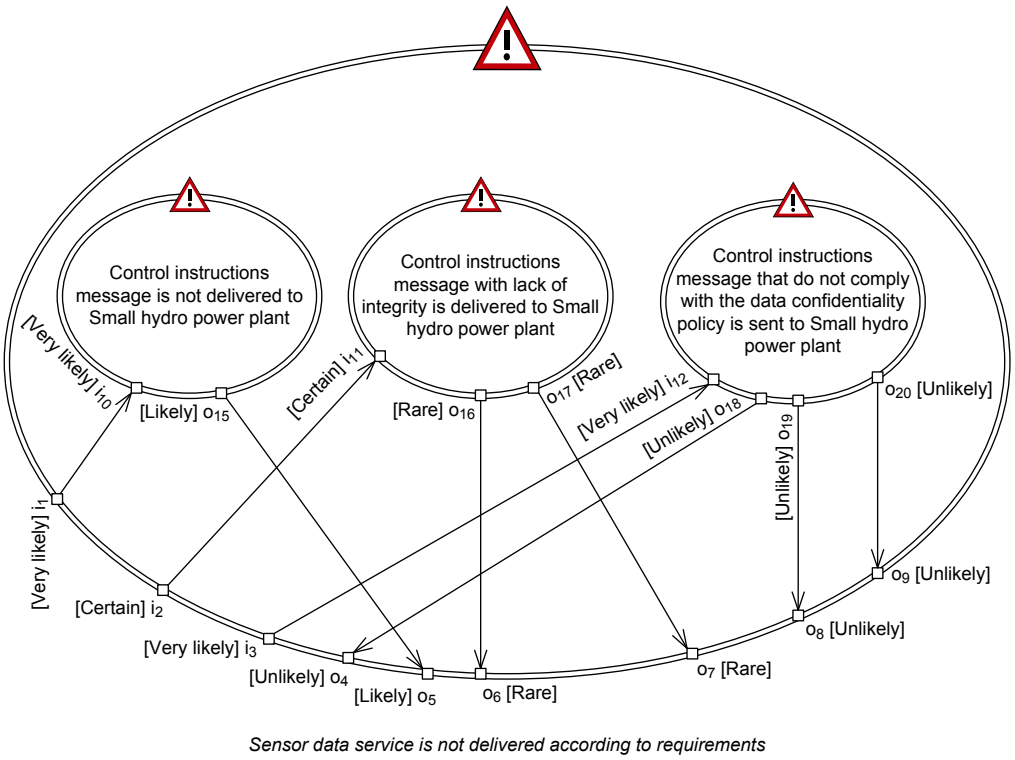


Figure 16: The referenced threat scenario "Sensor data service is not delivered according to requirements," referred to in Figure 14

described by the referenced threat scenarios in Figures 17–19. The different referenced threat scenarios describe how "Small hydro power plant" may fail to deliver the sensor data service according to requirements as a result of "Public telecom system" failing to deliver the control instructions service according to its requirements.

Figure 20 contains the referenced unwanted incidents referred to in Figure 14. For each of the unwanted incidents, Client EPP believes that more than one sensor data message is affected by the incident. For the incident "No sensor data messages are sent due to Small hydro power plant being unavailable due to lack of control instructions or use of invalid control instructions," Client EPP estimates a down time of one day, while a down time of 3 days is estimated for the incident "No sensor data messages are sent due to Small hydro power plant being unavailable due to malicious software." For the incident "Incorrect sensor data is sent to Public telecom system due to invalid control instructions being used by Small hydro power plant," Client EPP estimates that "Small hydro power plant" sends incorrect sensor data messages for a period of 12 hours as a result of using incorrect control instructions. For the incident "Sensor data is sent in plain text from Small hydro power plant to an outsider," Client EPP believes that this can go on undetected for at much as seven days. The same is believed for the incident "Incorrect sensor data is sent to Public telecom system due to sensors being infected with a computer virus." With an average number of 13.7 ($\frac{5000}{365}$) sensor data messages being sent each day, we get the consequence values documented in Figure 14.

The result of the detailed analysis is five risks, where each risk consists of an unwanted incident, its likelihood of occurring, and the consequence of the unwanted incident with respect to a quality asset. Based on the risk function, defined in Equations (1) and (2), the estimated number of sensor data messages sent each year (5000), and the required service levels for the sensor data service, we can calculate the risk values of the five risks.

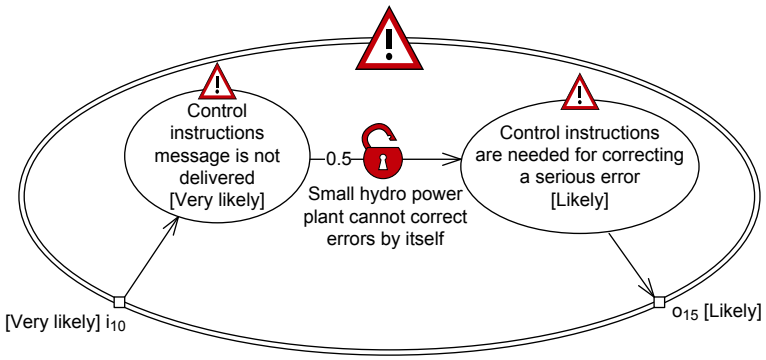


Figure 17: The referenced threat scenario "Control instructions message is not delivered to Small hydro power plant," referred to in Figure 16

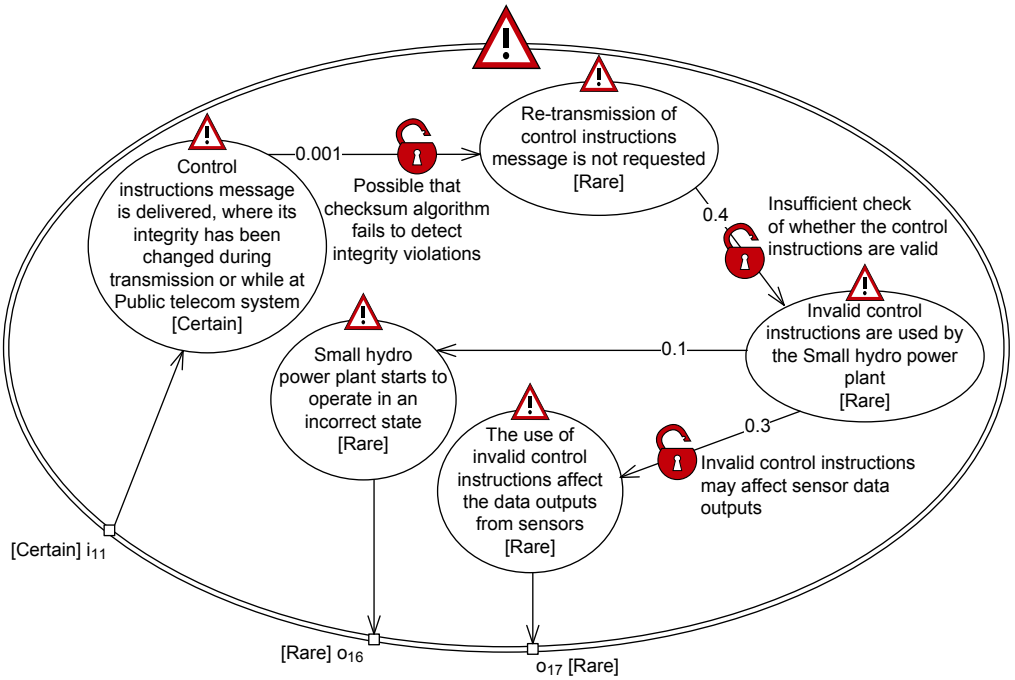


Figure 18: The referenced threat scenario "Control instructions message with lack of integrity is delivered to Small hydro power plant," referred to in Figure 16

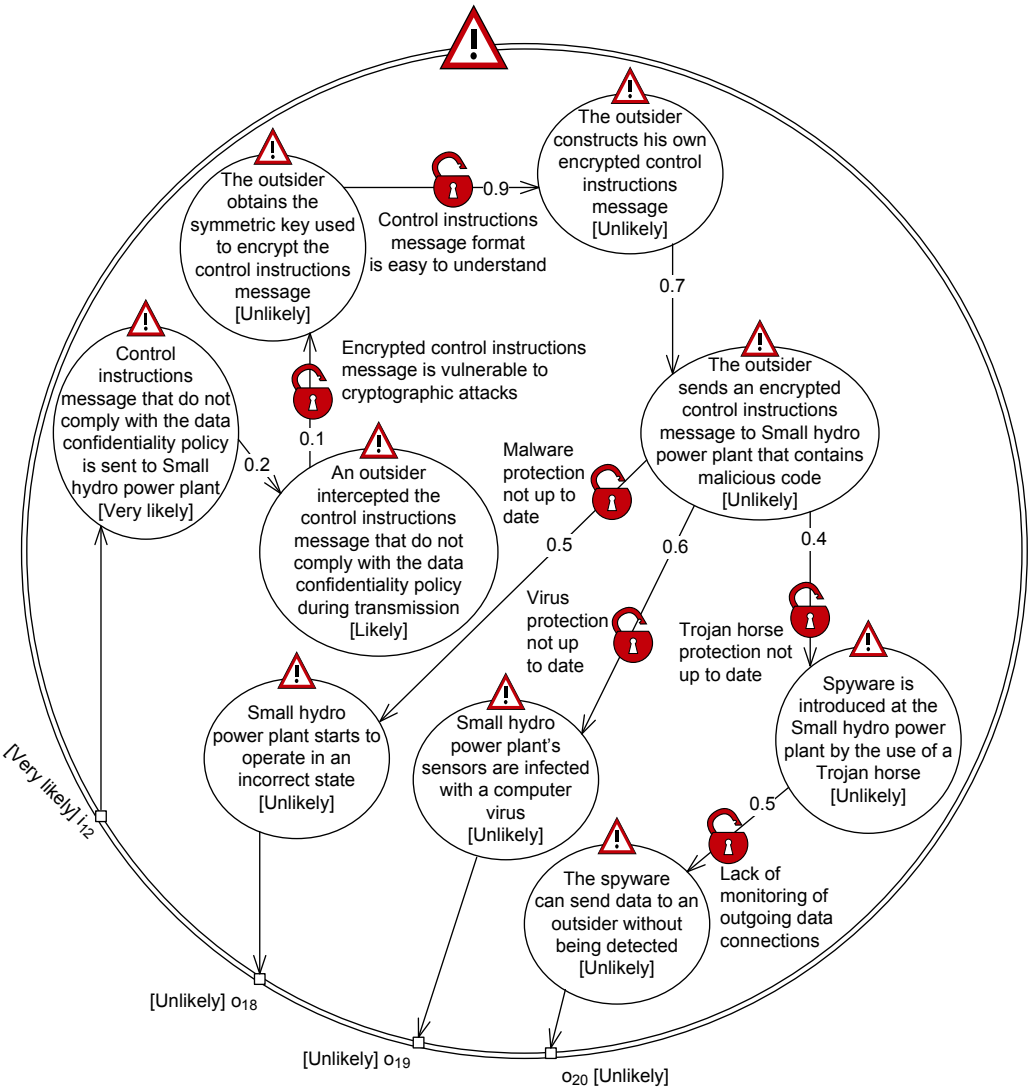


Figure 19: The referenced threat scenario "Control instructions message that do not comply with the data confidentiality policy is sent to Small hydro power plant," referred to in Figure 16

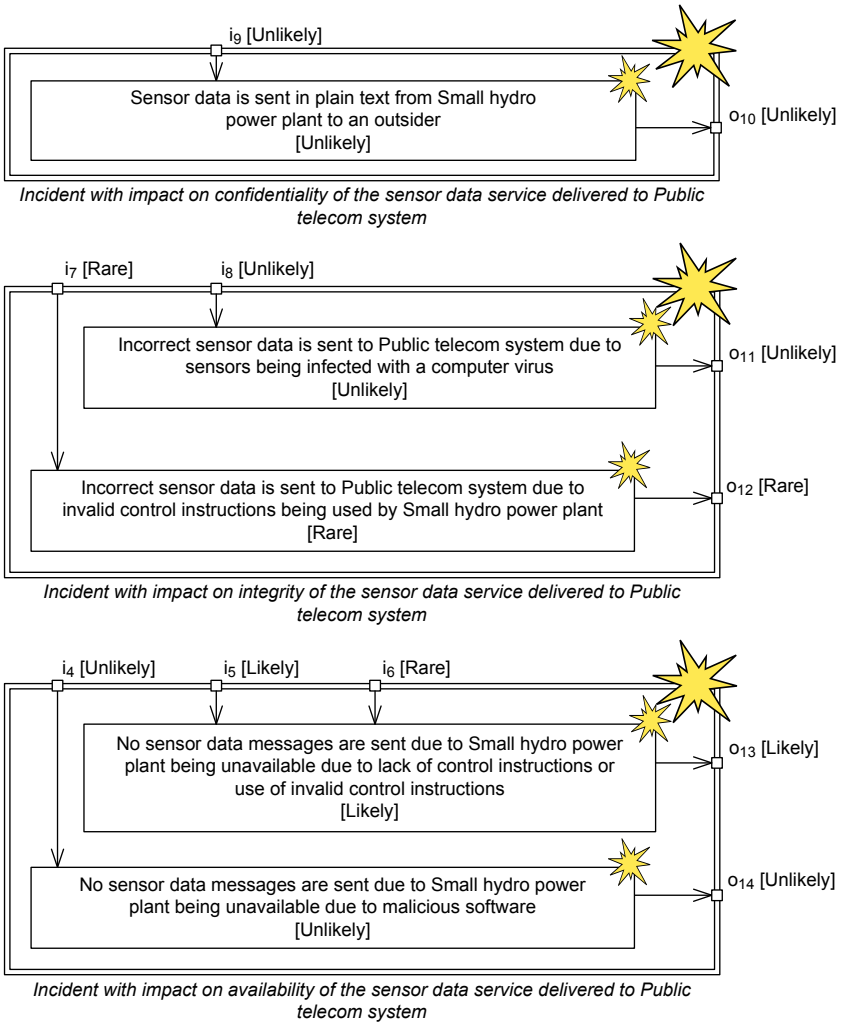


Figure 20: The referenced unwanted incidents “Incident with impact on confidentiality of the sensor data service delivered to Public telecom system,” “Incident with impact on integrity of the sensor data service delivered to Public telecom system,” and “Incident with impact on availability of the sensor data service delivered to Public telecom system,” referred to in Figure 14

Interval arithmetic needs to be used during the calculation of risk values, since likelihoods in the form of intervals are used in the calculations. For two intervals $[a, b]$ and $[c, d]$, where both are subsets of the positive real line $\mathbb{R}^+$, the basic operations of interval arithmetic are:

- **Addition:** $[a, b] + [c, d] = [a + c, b + d]$
- **Subtraction:** $[a, b] - [c, d] = [max(0, a - d), max(0, b - c)]$
- **Multiplication:** $[a, b] \cdot [c, d] = [a \cdot c, b \cdot d]$
- **Division:** $[a, b] \div [c, d] = [a \div d, b \div c]$ when 0 is not in $[c, d]$

In addition, a positive real number e may be written as the interval $[e, e]$. Notice that the application of all the basic operations result in intervals that are subsets of the positive real line. For instance, $[a, b] - [c, d]$ results in the interval $[0, 0]$ if $d > a$ and $c > b$. In our case, it does not make any sense to produce intervals that contains negative values.

A risk value is acceptable if *Expected service level* is greater than or equal to $\frac{Required\ service\ level}{Maximum\ service\ level}$, while it is unacceptable in the opposite case. We need some additional interval arithmetic rules to determine whether the risk value is acceptable or not. We let $[a, b]$ and $[c, d]$ represent *Expected service level* and $\frac{Required\ service\ level}{Maximum\ service\ level}$, respectively. Both intervals are subsets of the positive real line $\mathbb{R}^+$. The rules are as follows:

- Risk value is *Acceptable*: $[a, b] \geq [c, d]$ if $a \geq c$
- Risk value is *Unacceptable*: $[a, b] < [c, d]$ if $a < c$

In the following we calculate the risk values for the five risks. In all the equations for *Expected service level*, *Likelihood* is given for the period of one year, since both *Required service level* and *Maximum service level* are given for the period of one year.

The risk value of "Sensor data is sent in plain text from Small hydro power plant to an outsider" is *Unacceptable* since *Expected service level* is less than $\frac{Required\ service\ level}{Maximum\ service\ level}$. In this case, the calculations are as follows:

$$
\begin{aligned}
Expected\ service\ level &= \frac{Maximum\ service\ level - (Likelihood \cdot Consequence)}{Maximum\ service\ level} \\
&= \frac{5000 - ([0.6, 1.9] \cdot 96)}{5000} \\
&= \frac{[5000, 5000] - ([0.6, 1.9] \cdot [96, 96])}{[5000, 5000]} \\
&= \frac{[5000, 5000] - [57.6, 182.4]}{[5000, 5000]} \\
&= \frac{[4817.6, 4942.4]}{[5000, 5000]} \\
&= [0.9635, 0.9885]
\end{aligned}
$$

$$
\begin{aligned}
\frac{Required\ service\ level}{Maximum\ service\ level} &= \frac{5000 \cdot 0.995}{5000} \\
&= \frac{[5000, 5000] \cdot [0.999, 0.999]}{[5000, 5000]} \\
&= \frac{[4975, 4975]}{[5000, 5000]} \\
&= [0.995, 0.995]
\end{aligned}
$$

For the other risks, we end up with the following risk values:

- The risk value of "Incorrect sensor data is sent to Public telecom system due to sensors being infected with a computer virus" is *Unacceptable* since

  $$Expected\ service\ level = [0.9635, 0.9885]$$

  is less than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.999, 0.999]$$

- The risk value of "Incorrect sensor data is sent to Public telecom system due to invalid control instructions being used by Small hydro power plant" is *Acceptable* since

  $$Expected\ service\ level = [0.9999, 1]$$

  is greater than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.999, 0.999]$$

- The risk value of "No sensor data messages are sent due to Small hydro power plant being unavailable due to lack of control instructions or use of invalid control instructions" is *Unacceptable* since

  $$Expected\ service\ level = [0.9723, 0.986]$$

  is less than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.9999, 0.9999]$$

- The risk value of "No sensor data messages are sent due to Small hydro power plant being unavailable due to malicious software" is *Unacceptable* since

  $$Expected\ service\ level = [0.9844, 0.9951]$$

  is less than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.9999, 0.9999]$$

6 Demonstration of Step 3: Identify indicators for interconnected systems

6.1 Step 3.1: Identify risks to be monitored

Client EPP believes that the likelihood values used to calculate the risk values of the risks "Incorrect sensor data is sent to Public telecom system due to sensors being infected with a computer virus" and "Sensor data is sent in plain text from Small hydro power plant to an outsider" may be subject to change. We therefore decide to monitor these risks.

6.2 Step 3.2: Identify relevant indicators for the risks to be monitored

Indicators should be used to monitor likelihood values, since the likelihood values used to calculate the risk values of the two risks may be subject to change. Client EPP does not find it feasible to directly monitor the likelihoods of the unwanted incidents occurring, and has therefore decided to monitor the conditional likelihoods of two leads-to relations in the referenced threat scenario in Figure 19 that affect the likelihoods of the two unwanted incidents occurring. The relevant indicators for the two leads-to relations are presented in Figure 21. In Appendix D.2 we show how to use the conditional likelihoods we now address as well as other factors to monitor the resulting likelihoods of the risks identified for monitoring in Step 3.1.

One composite indicator c_1, which aggregates the two basic indicators b_1 and b_2, has been identified for one leads-to relation. c_1 makes a prediction about the percentage of computer viruses that "Small hydro power plant" is not protected against. For the other leads-to relation, we have identified the composite indicator c_2, which aggregates the two basic indicators b_3 and b_4. c_2 makes a prediction about the percentage of Trojan horses that "Small hydro power plant" is not protected against.

To calculate the indicators, Client EPP relies on data from the security vendor that delivers the security solutions and patches that are used in the control system of "Small hydro power plant." At the "Small hydro power plant" it may take some time between each upgrade of the security solutions and patching of the control system. This is due to that the updates and patches need to be inspected and tested before they can be introduced into the control system in order to ensure the stability of the control system of "Small hydro power plant." The consequence is that "Small hydro power plant" may be unprotected for some time against well-known computer viruses and Trojan horses.

7 Demonstration of Step 4: Specify design and deployment of identified indicators for interconnected systems

7.1 Step 4.1: Specify design of indicators for risk monitoring

In Figure 21 the composite indicators c_1 and c_2 are associated to one leads-to relation each. Conditional likelihoods were assigned to these leads-to relations during the detailed analysis described in Section 5. Values are therefore obtained for all the basic indicators from the time when the referenced threat scenario in Figure 19 was constructed. For b_1 and b_2 we obtain the values 750000 and 450000, respectively, while for b_3 and b_4 we obtain the values 500000 and 200000, respectively.

In Tables 3 and 4 are the design specifications for the different basic and composite indicators. All the specifications have been given in the form of algorithms. The four algorithms are to be used by a risk monitor within the electrical power production infrastructure. The indicators are updated every week. Afterwards, the risk picture is updated based on the updated composite indicators.

To calculate the two composite indicators, Client EPP uses data gathered in its infrastructure to update six lists. These lists are maintained by the risk monitor, and they are used to calculate the basic indicators. Client EPP takes into account that there may be computer viruses and Trojan horses that the security vendor is not aware of. Client EPP thinks it is reasonable to assume that the total number of computer viruses is $0.1 - 0.5\%$ higher than the sum $b_1 + b_2$, and that the total number of Trojan horses is $0.1 - 0.3\%$ higher than the sum $b_3 + b_4$. For both composite indicators we end up with an interval. By using the obtained values for the basic indicators as input to the algorithms of c_1 and c_2 in Tables 3 and 4, respectively, we get

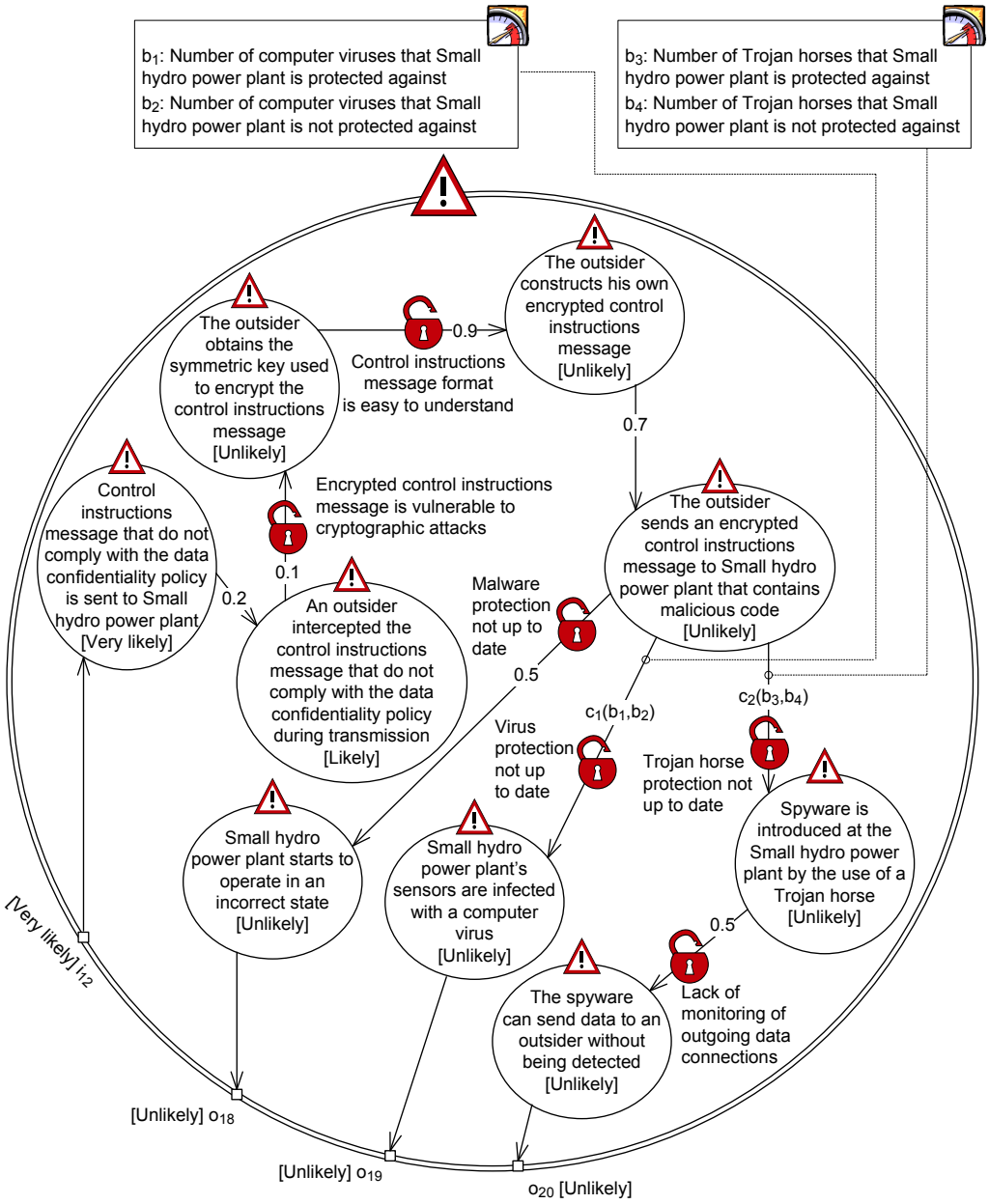


Figure 21: Relevant indicators, assigned to leads-to relations in the referenced threat scenario in Figure 19, for monitoring the risks "Incorrect sensor data is sent to Public telecom system due to sensors being infected with a computer virus" and "Sensor data is sent in plain text from Small hydro power plant to an outsider"

$[0.6006, 0.6032]$ for c_1, while we get $[0.4008, 0.4025]$ for c_2. These numbers are almost identical to the initial estimates of 0.6 and 0.4.

7.2 Step 4.2: Specify deployment of indicators for risk monitoring

In Table 5 is the deployment specification for the basic and composite indicators. The specification describes how data needed in the calculations of the indicators should be extracted and transmitted within the SoS.

8 Related work

The methodological approach presented in this report is a specialization of the approach presented in [11]. The approach in [11] is general in the sense that it only restricts the risk identification to the identified assets and nothing else. In our approach, the risk identification focuses entirely on risk to quality of provided services that have been caused by service dependencies. The approach in [11] can of course be used to identify indicators for the purpose of measuring the impact of service dependencies on risk to quality of provided services, because of its generality. Compared to our approach, however, it is inferior. The approach in [11] does not offer any support for dealing with interconnected systems or service dependencies. In addition, it focuses to a much lesser extent on the calculations of indicators, and it cannot be used to specify how the indicator calculations should be embedded in the systems to be monitored.

We are not aware of other approaches targeting the capture and measure of impact of service dependencies on risks to the quality of provided services. In [12], which is an approach for constructing formal models of services dependencies in information systems, the dependency models are used in security policy-based management. The dependency models are used to find enforcement points for security rules, which then support countermeasure deployment, and for computing the impact of attacks and countermeasures that propagate over the information system.

Service dependencies are also used in fault analysis [13] and dependability analysis [14], as well as in analyses targeting critical infrastructures. A number of the approaches that address service dependencies within critical infrastructures focus primarily on the consequences of infrastructure services not being provided. One such approach is [15]. This approach is used to create models of infrastructure systems and their interactions. The models are used in computer simulations where the main purpose is to investigate how the functionality of infrastructure systems and interconnections react to different attack scenarios ("what if" scenarios where one or two systems are removed), and how mechanisms for strengthening the underlying dependency graph can be used. Svendsen's approach differs, in particular, from our approach in that the likelihoods of incidents (systems failing to provide services according to requirements) are not considered.

Even though a lot of work has been done within the SoS field, there is still no single accepted definition of what an SoS is. Examples of different definitions may be found in [2]. With different understandings of what an SoS is, we also get different understandings of what should be addressed with respect to risk and security. For instance, some definitions state that an SoS only consists of systems that operate independently of each other, i.e., that the different systems do not rely on services from other systems in order in to function. This is quite different from our understanding of an SoS. In the literature, SoS has received relatively little coverage when it comes to risk and security analysis. Papers like [16], [17], [18], and [19], focus primarily on the challenges and relatively little on actual approaches.

Table 3: Design specifications, in the form of algorithms, for the basic indicators b_1 and b_2 and the composite indicator c_1

Algorithm for b_1 and b_2

Input: $data_1$: "Data on security updates/patches that have been applied in the control system at Small hydro power plant," $data_2$: "Data on the threat picture, the security updates and patches that are available from the security vendor of Client EPP, and malware that the security vendor is aware of but does not yet offer protection against"

Data maintained by the risk monitor: $list_1$: "List of names of computer viruses that the control system at Small hydro power plant is protected against," $list_2$: "List of names of all computer viruses that the security vendor of Client EPP offers protection against," $list_3$: "List of names of computer viruses that the security vendor of Client EPP is aware of but does not yet offer protection against"

Based on $data_1$, check whether the security updates/patches applied in the control system have resulted in protection against new computer viruses. Add the names of the new computer viruses to $list_1$, if applicable.

Based on $data_2$, check whether the security vendor offers protection against any new computer viruses. Add the names of the new computer viruses to $list_2$, if applicable. Remove names of computer viruses from $list_3$, if applicable.

Based on $data_2$, check whether there are any new computer viruses that the security vendor is aware of, but does not yet offer protection against. Add the names of the new computer viruses to $list_3$, if applicable.

b_1 := "The number of items in $list_1$"

b_2 := "The number of items in $list_2$, where each item is not in $list_1$" +
"The number of items in $list_3$"

Output: b_1, b_2

Algorithm for c_1

Input: b_1: "Number of computer viruses that Small hydro power plant is protected against," b_2: "Number of computer viruses that Small hydro power plant is not protected against"

$var_1 := b_2 + ((b_1 + b_2) \cdot [0.001, 0.005])$

$var_2 := b_1 + var_1$

$c_1 := \dfrac{var_1}{var_2}$

Output: c_1

Table 4: Design specifications, in the form of algorithms, for the basic indicators b_3 and b_4 and the composite indicator c_2

Algorithm for b_3 and b_4

Input: $data_1$: "Data on security updates/patches that have been applied in the control system at Small hydro power plant," $data_2$: "Data on the threat picture, the security updates and patches that are available from the security vendor of Client EPP, and malware that the vendor is aware of but does not yet offer protection against"

Data maintained by the risk monitor: $list_4$: "List of names of Trojan horses that Small hydro power plant is protected against," $list_5$: "List of names of all Trojan horses that the security vendor of Client EPP offers protection against," $list_6$: "List of names of Trojan horses that the security vendor of Client EPP is aware of but does not yet offer protection against"

Based on $data_1$, check whether the security updates/patches applied in the control system have resulted in protection against new Trojan horses. Add the names of the new Trojan horses to $list_4$, if applicable.

Based on $data_2$, check whether the security vendor offers protection against any new Trojan horses. Add the names of the new Trojan horses to $list_5$, if applicable. Remove names of Trojan horses from $list_6$, if applicable.

Based on $data_2$, check whether there are any new Trojan horses that the security vendor is aware of, but does not yet offer protection against. Add the names of the new Trojan horses to $list_6$, if applicable.

b_3 := "The number of items in $list_4$"

b_4 := "The number of items in $list_5$, where each item is not in $list_4$" +
"The number of items in $list_6$"

Output: b_3, b_4

Algorithm for c_2

Input: b_3: "Number of Trojan horses that Small hydro power plant is protected against," b_4: "Number of Trojan horses that Small hydro power plant is not protected against"

$var_3 := b_4 + ((b_3 + b_4) \cdot [0.001, 0.003])$

$var_4 := b_3 + var_3$

$c_2 := \dfrac{var_3}{var_4}$

Output: c_2

Table 5: Deployment specification for the basic indicators b_1, b_2, b_3, and b_4 and the composite indicators c_1 and c_2

Deployment specification for b_1, b_2, b_3, b_4, c_1, and c_2
Extraction and transmission of $data_1$: Client EPP maintains a security database that contains different kinds of information, including how the control system of "Small hydro power plant" is protected against malware. Each time the security solutions of the control system are updated or patches are installed, the information stored about the control system will be updated based on information that comes with the updates/patches. Every week, an automated ICT process extracts data for the control system that the database has been updated with in the period of one week backwards. It should be noticed that the process will extract all the available data for the control system the first time it is executed. We refer to the extracted data as $data_1$. The process transmits $data_1$ to the risk monitor by using the internal data network of the electrical power production infrastructure. **Extraction and transmission of $data_2$:** The security database of Client EPP also contains information that has been provided by the security vendor used by Client EPP. As part of delivering security solutions to Client EPP, the security vendor provides Client EPP with regular information updates on the threat picture, security updates and patches that are available from the vendor, and malware that the vendor is aware of but does not yet offer protection against. The security database is updated with this information. Every week, an automated ICT process extracts the information that the database has been updated with in the period of one week backwards. It should be noticed that the process will extract all the available information the first time it is executed. We refer to the extracted data as $data_2$. The process transmits $data_2$ to the risk monitor by using the internal data network of the electrical power production infrastructure.

Dependent CORAS [7] is an approach for modular risk modeling, which can be used to document and reason about risk in SoS. It extends the CORAS risk modeling language with facilities for documenting and reasoning about risk analysis assumptions. It was motivated by the need to deal with mutual dependencies in risk analysis of SoS. By employing dependent CORAS we may document risk separately for the individual systems in an SoS. In addition, we document the risk analysis assumptions for the different systems, i.e., how threat scenarios and unwanted incidents, documented for other systems, may lead to threat scenarios and unwanted incidents, documented for the system in question. These assumptions are due to some form of dependencies, not necessarily service dependencies, between the different systems. Thus, dependent CORAS deal with dependencies in a general way compared to our approach, which only focus on service dependencies. The different risk models may be combined in the end, if the dependencies between them are well-founded, i.e., not circular.

Many services need to fulfill quality requirements that are requirements to information security. There exist a number of approaches for measuring information security. One of those is the NIST Performance Measurement Guide for Information Security [20]. This approach aims to assist in the development, selection, and implementation of suitable measures. It also provides a number of candidate measures. Unlike our approach, it is not specialized towards using these measures for the purpose of calculating explicit likelihood and consequence values.

9 Conclusion

In this report we have addressed the issue of how to capture and measure the impact of service dependencies on risk to quality of provided services by the use of measurable indicators. To this end we have put forward a method consisting of four steps. To the best of our knowledge, there exists no similar approach. The applicability of the approach has been demonstrated on an example case within power supply.

In Step 1 of the approach, dependencies due to service interactions between the different interconnected systems are captured. Their impact on risk to quality of provided services is established in Step 2. In Step 3 we identify relevant indicators for monitoring the risks arising from service dependencies, while in Step 4 we specify how likelihood and consequence values associated with the risks should be calculated from sets of indicators and how these calculations should be embedded in the interconnected systems. The result of applying the method is a risk picture capturing the impact of service dependencies on quality of provided services that can be dynamically monitored via the specified indicators.

An interesting topic for further research is the use of leading indicators [21] to monitor the impact of service dependencies on risk to quality of provided services. Many indicators can be viewed as lagging indicators [21]. A lagging indicator that focuses on quality measures something that exists after a shift in quality, e.g. occurrence of unwanted incidents that affects quality assets. Leading indicators, on the other hand, measures something that exists before a shift in quality. In the case of service dependencies, the leading indicators may be used to predict their future impact on risk to quality of provided services. By employing leading indicators, countermeasures may be implemented prior to the risks occurring.

Acknowledgements

The research on which this report describes has been carried out within the DIGIT project (180052/S10), funded by the Research Council of Norway, and the MASTER and NESSoS projects, both funded from the European Community's Seventh Framework Programme

(FP7/2007-2013) under grant agreements FP7-216917 and FP7-256980, respectively.

References

[1] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. SoS and FoS FAQ. Retrieved February 9, 2012, from `http://www.acq.osd.mil/dpap/Docs/FAQs -- SoS & FoS.doc`, 2002.

[2] M. Jamshidi. System of Systems Engineering - New Challenges for the 21st Century. *IEEE Aerospace and Electronic Systems Magazine*, 23(5):4–19, 2008.

[3] Object Management Group. Unified Modeling Language Specification, Version 2.0, 2004.

[4] D. Gambetta. Can We Trust Trust? In D. Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, pages 213–237. Basil Blackwell, Oxford, 1988.

[5] A. Jøsang, C. Keser, and T. Dimitrakos. Can We Manage Trust? In *Proceedings of the Third International Conference on Trust Management (iTrust'05)*, pages 93–107, Berlin Heidelberg, 2005. Springer-Verlag.

[6] T. Lysemose, T. Mahler, B. Solhaug, J. Bing, D. Elgesem, and K. Stølen. ENFORCE Conceptual Framework. Technical Report SINTEF A1209, SINTEF, Oslo, 2007.

[7] M. S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis: The CORAS Approach*. Springer-Verlag, Berlin Heidelberg, 1st edition, 2010.

[8] A. Hammond, A. Adriaanse, E. Rodenburg, D. Bryant, and R. Woodward. *Environmental Indicators: A Systematic Approach to Measuring and Reporting on Environmental Policy Performance in the Context of Sustainable Development*. World Resources Institute, Washington, DC, 1995.

[9] O. S. Ligaarden, A. Refsdal, and K. Stølen. ValidKI: A Method for Designing Indicators to Monitor the Fulfillment of Business Objectives with Particular Focus on Quality and ICT-supported Monitoring of Indicators. Technical Report SINTEF A23413, SINTEF, Oslo, 2012.

[10] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27000:2009 Information Technology – Security Techniques – Code of Practice for Information Security Management – Overview and Vocabulary, 2009.

[11] A. Refsdal and K. Stølen. Employing Key Indicators to Provide a Dynamic Risk Picture with a Notion of Confidence. In *Proceedings of Third IFIP WG 11.11 International Conference (IFIPTM'09)*, pages 215–233, Berlin Heidelberg, 2009. Springer-Verlag.

[12] H. Debar, N. Kheir, N. Cuppens-Boulahia, and F. Cuppens. Service Dependencies in Information Systems Security. In *Proceedings of the 5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS'10)*, pages 1–20, Berlin Heidelberg, 2010. Springer-Verlag.

[13] B. Gruschke. Integrated Event Management: Event Correlation Using Dependency Graphs. In *Proceedings of Ninth Annual IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM'98)*, 1998.

[14] A. Rugina, K. Kanoun, and M. Kaâniche. A System Dependability Modeling Framework Using AADL and GSPNs. In R. de Lemos, C. Gacek, and A. Romanovsky, editors, *Architecting Dependable Systems IV*, pages 14–38. Springer-Verlag, Berlin Heidelberg, 2007.

[15] N. K. Svendsen. *Interdependencies in Critical Infrastructures – A Qualitative Approach to Model Physical, Logical, and Geographical Interdependencies*. PhD thesis, University of Oslo, Oslo, 2008. In series of dissertations submitted to the Faculty of Mathematics and Natural Sciences, University of Oslo, No. 748.

[16] A. Waller and R. Craddock. Managing Runtime Re-engineering of a System-of-Systems for Cyber Security. In *Proceedings of 6th International Conference on System of Systems Engineering (SoSE'11)*, pages 13–18, Piscataway, NJ, 2011. IEEE.

[17] S.J. Gandhi, A. Gorod, and B. Sauser. A Systemic Approach to Managing Risks of SoS. In *Proceedings of 2011 IEEE International Systems Conference (SysCon'11)*, pages 412–416, Piscataway, NJ, 2011. IEEE.

[18] D.J. Bodeau. System-of-Systems Security Engineering. In *Proceedings of 10th Annual Computer Security Applications Conference*, pages 228–235, Los Alamitos, CA, 1994. IEEE Computer Society.

[19] A.P. Sage. Conflict and Risk Management in Complex System of Systems Issues. In *Proceedings of 2003 IEEE International Conference on Systems, Man and Cybernetics*, pages 3296–3301, Piscataway, NJ, 2003. IEEE.

[20] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson. Performance Measurement Guide for Information Security. Technical report, National Institute of Standards and Technology, Gaithersburg, MD, 2008. NIST Special Publication 800-55 Revision 1.

[21] W. Jansen. *Directions in Security Metrics Research*. DIANE Publishing Company, Darby, PA, 2010.

A Assets to be analyzed for provided services

In this appendix and Appendices B and C we demonstrate the use of the methodological approach on the four provided services of Client EPP that the approach was not demonstrated on in Sections 5–7. This appendix focus on identifying quality assets for the four provided services, specifying scales for measuring likelihood and consequence, and specifying functions for calculating risk values.

On behalf of Client EPP we aim to capture and measure the impact of service dependencies on the quality of the following provided services:

- The control instructions service provided to "Public telecom system."
- The electricity service provided to "Distribution line 2."
- The electricity service provided to "Distribution line 3."
- The electricity service provided to "Transmission line."

The CORAS asset diagram in Figure 22 presents the relevant quality assets. The control instructions service provided to "Public telecom system" has been assigned three quality assets, while the different electricity services have for the sake of simplicity only been assigned one quality asset each.

Table 6 shows how consequence is measured for the different assets. The meaning of "lack of integrity" and "do not comply with the data confidentiality policy" was explained in Section 5.3. Client EPP has an estimate for the number of control instructions messages to be sent in the period of one year. We will present this estimate later. This estimate is used to calculate consequence values for the control instructions service.

Likelihood is measured as defined in Table 1 on page 31. For the control instructions service, we classify risks as acceptable or unacceptable by the use of Equations (1) and (2) on page 32. For the electricity services, we need to take into account that the required service level for availability is the conjunction of two availability requirements. We classify risks towards these services as follows:

$$Expected\ service\ level_T = \frac{Maximum\ service\ level_T - (Likelihood \cdot Consequence_T)}{Maximum\ service\ level_T} \quad (3)$$

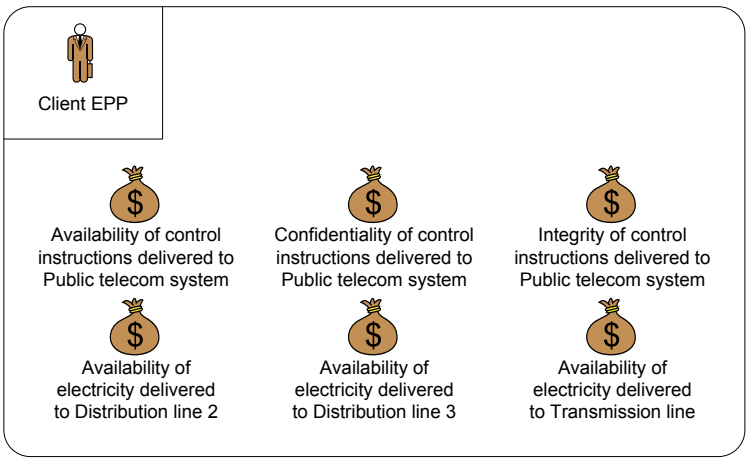


Figure 22: Asset diagram presenting the quality assets for which impact of service dependencies should be captured and measured

Table 6: How consequence is measured for the different quality assets

Availability of control instructions delivered to Public telecom system
Number of control instructions messages that are not delivered
Confidentiality of control instructions delivered to Public telecom system
Number of control instructions messages sent that do not comply with the data confidentiality policy
Integrity of control instructions delivered to Public telecom system
Number of control instructions messages that are delivered with lack of integrity
Availability of electricity delivered to Distribution line 2
Number of hours that the electricity service is unavailable and the amount of electricity (in kilowatt hours) that is not delivered
Availability of electricity delivered to Distribution line 3
Number of hours that the electricity service is unavailable and the amount of electricity (in kilowatt hours) that is not delivered
Availability of electricity delivered to Transmission line
Number of hours that the electricity service is unavailable and the amount of electricity (in kilowatt hours) that is not delivered

$$Expected\ service\ level_E = \frac{Maximum\ service\ level_E - (Likelihood \cdot Consequence_E)}{Maximum\ service\ level_E} \quad (4)$$

$$\begin{aligned} &\textbf{if } Expected\ service\ level_T \geq \frac{Required\ service\ level_T}{Maximum\ service\ level_T} \textbf{ and} \\ &\quad Expected\ service\ level_E \geq \frac{Required\ service\ level_E}{Maximum\ service\ level_E} \textbf{ then} \\ &\quad Risk\ value = Acceptable \\ &\textbf{else} \\ &\quad Risk\ value = Unacceptable \\ &\textbf{endif} \end{aligned} \quad (5)$$

In Equations (3)–(5), *T* refers to the requirement that focus on availability with respect to time, while *E* refers to the requirement that focus on availability with respect to the electricity delivered. In Appendix C.2.1, we provide an example of the use of the three equations given above.

B Schematic construction of threat diagrams for provided services

This appendix presents high-level threat diagrams for the four provided services of Client EPP that the approach was not demonstrated on in Sections 5–7.

B.1 Control instructions service provided to Public telecom system

For the control instructions service provided by "Home office computer" to "Public telecom system," the high-level threat diagram in Figure 23 has been schematically constructed from the target model in Figure 12 on page 29. The threat diagram provides a high-level description of the impact of service dependencies on the quality of the control instructions service provided to "Public telecom system." In the threat diagram we use the abbreviations "sensor data service" and "control instructions service" to refer to the sensor data service provided by "Public telecom system" to "Home office computer" and the control instructions service provided by "Home office computer" to "Public telecom system," respectively.

B.2 Electricity service provided to Distribution line 2

For the electricity service provided by "Small hydro power plant" to "Distribution line 2," the high-level threat diagram in Figure 24 has been schematically constructed from the target model

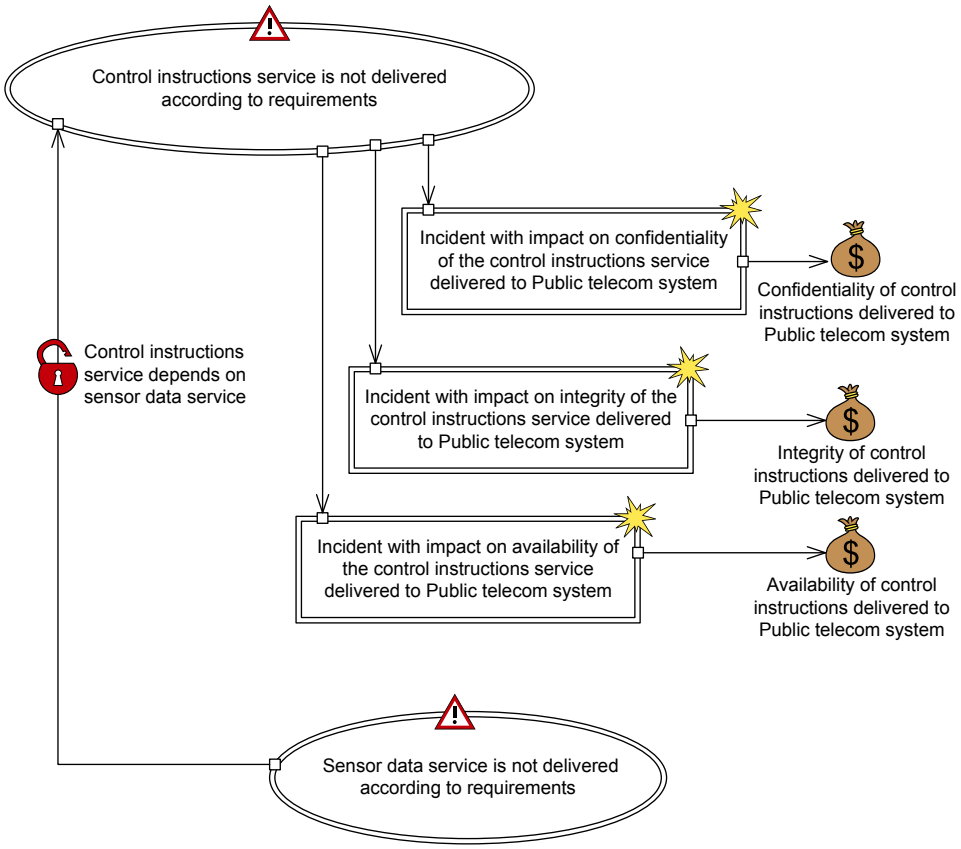


Figure 23: Threat diagram, which has been schematically constructed from the target model in Figure 12 on page 29, which provides a high-level outline of the impact of service dependencies on the quality of the control instructions service provided by "Home office computer" to "Public telecom system"

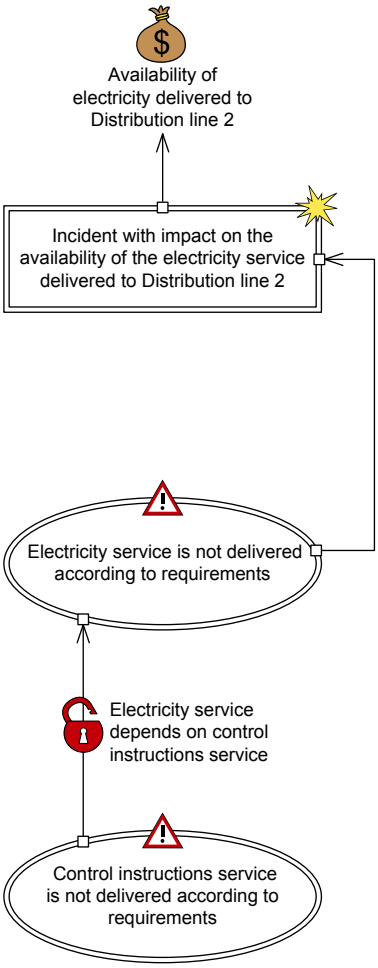


Figure 24: Threat diagram, which has been schematically constructed from the target model in Figure 12 on page 29, which provides a high-level outline of the impact of service dependencies on the quality of the electricity service provided by “Small hydro power plant” to “Distribution line 2”

in Figure 12 on page 29. The threat diagram provides a high-level description of the impact of service dependencies on the quality of the electricity service provided to “Distribution line 2.” In the threat diagram we use the abbreviations “control instructions service” and “electricity service” to refer to the control instructions service provided by “Public telecom system” to “Small hydro power plant” and the electricity service provided by “Small hydro power plant” to “Distribution line 2,” respectively.

B.3 Electricity service provided to Distribution line 3

For the electricity service provided by “Small hydro power plant” to “Distribution line 3,” the high-level threat diagram in Figure 25 has been schematically constructed from the target model in Figure 12 on page 29. The threat diagram provides a high-level description of the impact of service dependencies on the quality of the electricity service provided to “Distribution line 3.” In the threat diagram we use the abbreviations “control instructions service” and “electricity service” to refer to the control instructions service provided by “Public telecom system” to “Small hydro power plant” and the electricity service provided by “Small hydro power plant” to

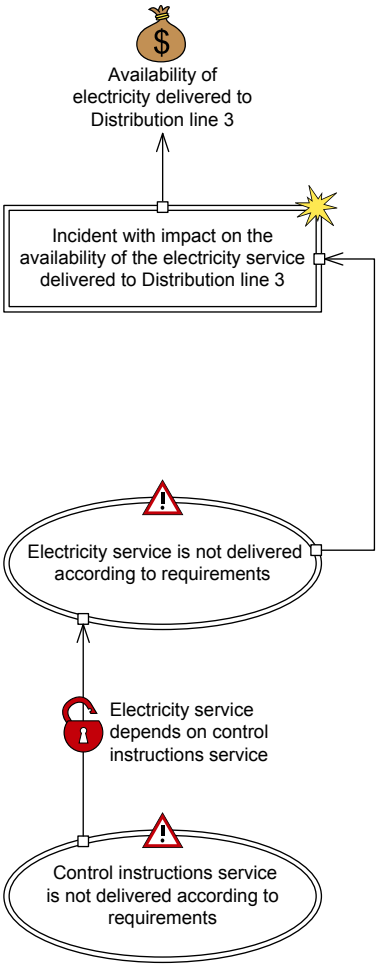


Figure 25: Threat diagram, which has been schematically constructed from the target model in Figure 12 on page 29, which provides a high-level outline of the impact of service dependencies on the quality of the electricity service provided by “Small hydro power plant” to “Distribution line 3”

“Distribution line 3,” respectively.

B.4 Electricity service provided to Transmission line

For the electricity service provided by “Large hydro power plant” to “Transmission line,” the high-level threat diagram in Figure 26 has been schematically constructed from the target model in Figure 12 on page 29. The threat diagram provides a high-level description of the impact of service dependencies on the quality of the electricity service provided to “Transmission line.” In the threat diagram we use the following abbreviations for the different services:

- “DL2-CS electricity service” refers to the electricity service provided by “Distribution line 2” to “Control system.”
- “PBS-CS electricity service” refers to the electricity service provided by “Backup power system” to “Control system.”
- “PBS-PTS electricity service” refers to the electricity service provided by “Backup power system” to “Private telecom system.”

- “DL3-PTS electricity service” refers to the electricity service provided by “Distribution line 3” to “Private telecom system.”
- “PTS-LHPP control instructions service” refers to the control instructions service provided by “Private telecom system” to “Large hydro power plant.”
- “LHPP-PTS sensor data service” refers to the sensor data service provided by “Large hydro power plant” to “Private telecom system.”
- “PTS-CS sensor data service” refers to the sensor data service provided by “Private telecom system” to “Control system.”
- “CS-PTS control instructions service” refers to the control instructions service provided by “Control system” to “Private telecom system.”
- “LHPP-TL electricity service” refers to the electricity service provided by “Large hydro power plant” to “Transmission line.”

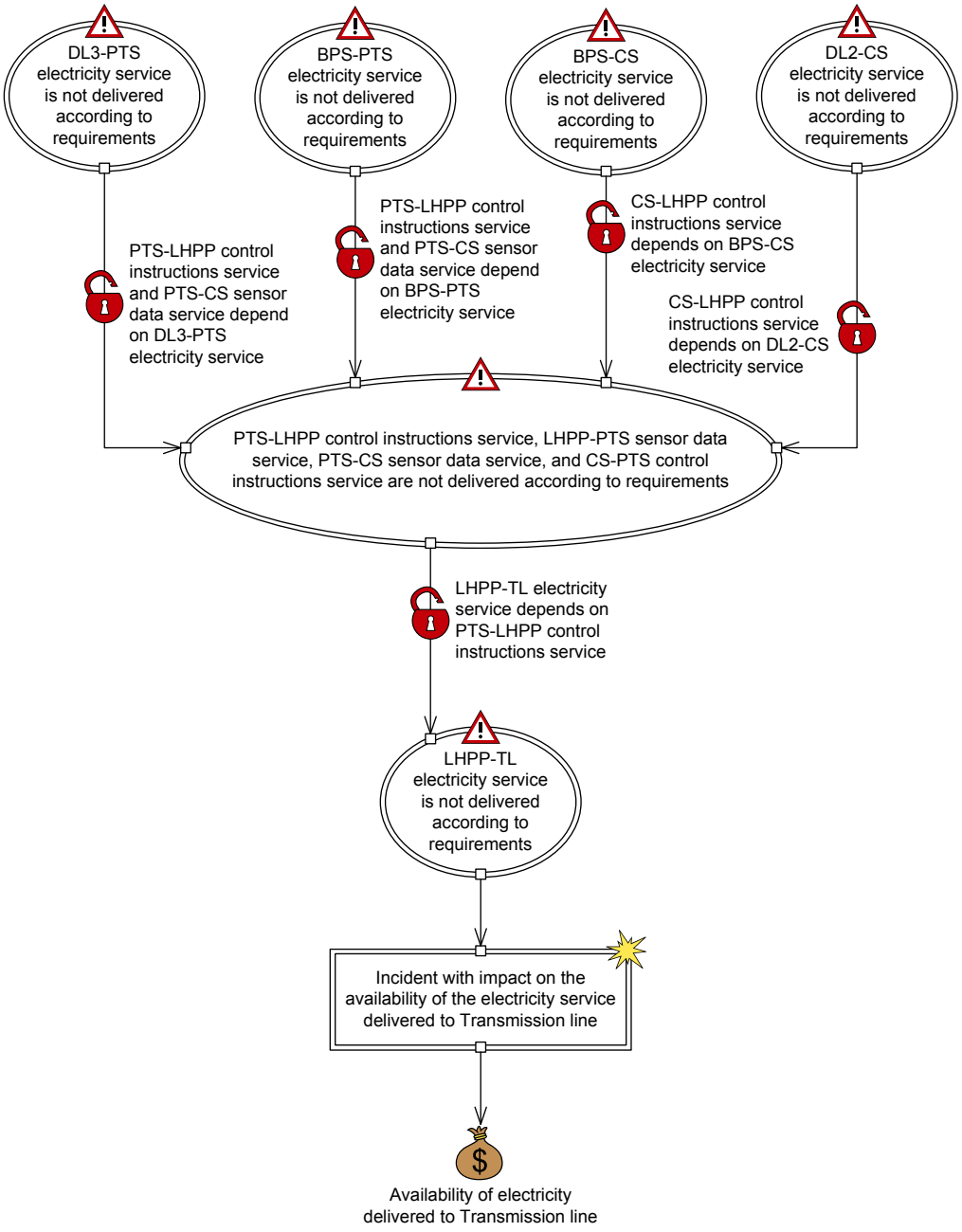


Figure 26: Threat diagram, which has been schematically constructed from the target model in Figure 12 on page 29, which provides a high-level outline of the impact of service dependencies on the quality of the electricity service provided by “Large hydro power plant” to “Transmission line”

C Capture and measure impact of service dependencies on quality assets of provided services

This appendix presents detailed threat diagrams for the four provided services of Client EPP that the approach was not demonstrated on in Sections 5–7. In addition, it presents relevant indicators for monitoring risk to the quality of the different provided services, and design and deployment specifications for these indicators.

C.1 Control instructions service provided to Public telecom system

C.1.1 Detailed threat diagrams

In Figure 27 is the detailed version of the high-level threat diagram in Figure 23. The referring elements in Figure 27 refer to the referenced threat scenarios provided in Figures 28 and 29, and the referenced unwanted incidents provided in Figure 33. Moreover, the referenced threat scenario in Figure 29 contains three referring threat scenarios, which refer to the referenced

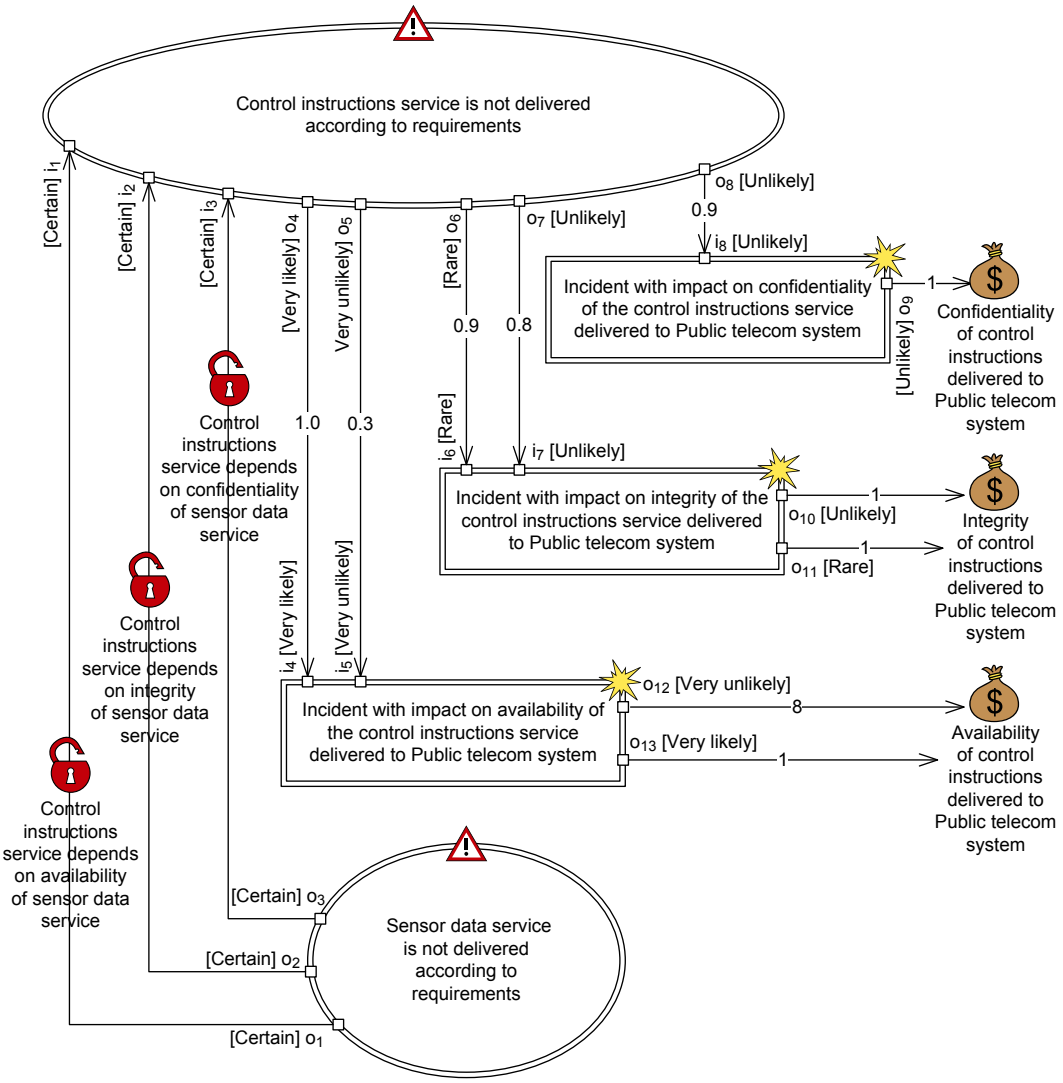


Figure 27: Detailed version of the high-level threat diagram in Figure 23

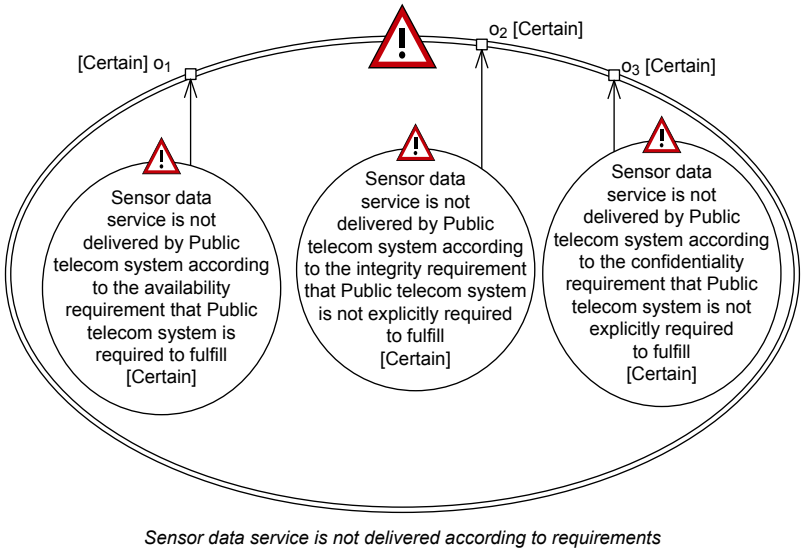


Figure 28: The referenced threat scenario "Sensor data service is not delivered according to requirements," referred to in Figure 27

threat scenarios provided in Figures 30–32. Client EPP has estimated all the likelihood and consequence values in the different figures.

As can be seen in Figure 27, the vulnerability "Control instructions service depends on sensor data service" in Figure 23 has been decomposed into three vulnerabilities. The referenced threat scenario in Figure 28 is a detailing of the referring threat scenario "Sensor data service is not delivered according to requirements" in Figure 23. Since "Public telecom system" is only required to deliver the sensor data service according to the availability requirement, the referenced threat scenario distinguish between the failure of not achieving the availability requirement, and the failures of not achieving the confidentiality and integrity requirements.

Client EPP estimates that 5000 sensor data messages are sent each year to "Home office computer." Moreover, Client EPP estimates the number of control instructions sent by "Home office computer" in the period of one year to be 1000. Before we can estimate the likelihoods of the sensor data service not being delivered according to the confidentiality, integrity, and availability requirements, we need to calculate the worst-case service levels of the sensor data service delivered by "Public telecom system." These are as follows:

- $100\% \cdot 0.97 = 97\%$ of the sent sensor messages do comply with the data confidentiality policy;
- $99.99\% \cdot 0.95 = 94.99\%$ of the sent sensor messages are delivered with integrity; and
- $99.99\% \cdot 0.99 = 98.99\%$ of the sent sensor data messages are delivered.

To estimate the likelihoods we use the estimated number of sensor data messages sent each year in combination with the required and worst-case service levels of the sensor data service delivered by "Public telecom system." The required service levels specify that:

- $5000 \cdot 100\% = 5000$ of the sent sensor data messages should comply with the data confidentiality policy;
- $5000 \cdot 99.99\% = 4999.5$ of the sent sensor data messages should be delivered with integrity; and

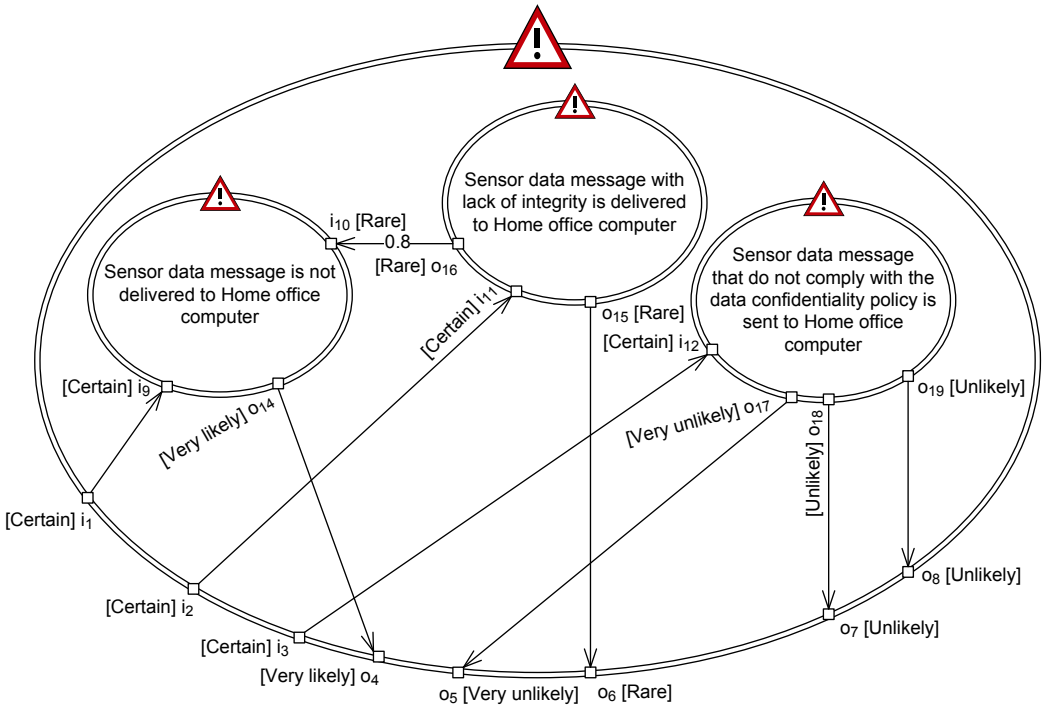


Figure 29: The referenced threat scenario "Control instructions service is not delivered according to requirements," referred to in Figure 27

- $5000 \cdot 99.99\% = 4999.5$ of the sent sensor data messages should be delivered.

On the other hand, our expectations according to the worst-case service levels are that:

- $5000 \cdot 97\% = 4850$ out of the 5000 required sensor data messages comply with the data confidentiality policy;
- $5000 \cdot 94.99\% = 4749.5$ out of the 4999.5 required sensor data messages are delivered with integrity; and
- $5000 \cdot 98.99\% = 4949.5$ out of the 4999.5 required sensor data messages are delivered.

Based on the calculations for required and worst-case service levels, we end up with the following likelihoods:

- The likelihood of the sensor data service not being delivered according to the confidentiality requirement is "Certain" ($5000 - 4850 = 150$ sensor data messages in the period of a year).
- The likelihood of the sensor data service not being delivered according to the integrity requirement is "Certain" ($4999.5 - 4749.5 = 250$ sensor data messages in the period of a year).
- The likelihood of the sensor data service not being delivered according to the availability requirement is "Certain" ($4999.5 - 4949.5 = 50$ sensor data messages in the period of a year).

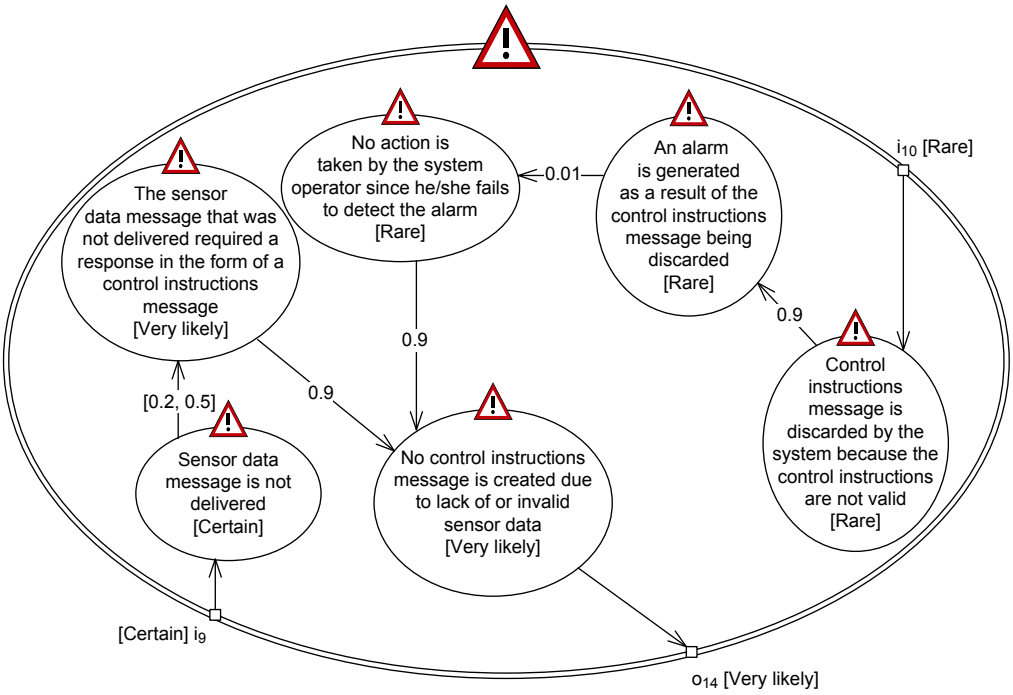


Figure 30: The referenced threat scenario "Sensor data message is not delivered to Home office computer," referred to in Figure 29

The referenced threat scenario "Control instructions service is not delivered according to requirements" is given in Figure 29. The internal threat behavior of "Home office computer" is described by the referenced threat scenarios in Figures 30–32. The different referenced threat scenarios describe how "Home office computer" may fail to deliver the control instructions service according to requirements as a result of "Public telecom system" failing to deliver the sensor data service according to its requirements.

Figure 33 contains the referenced unwanted incidents referred to in Figure 27. For each of the unwanted incidents, with the exception of "No control instructions messages are sent to Public telecom system due to Home office computer being unavailable," Client EPP assigns the consequence value 1, since each of these incidents only affects one control instructions message. In the case of the incident "No control instructions messages are sent to Public telecom system due to Home office computer being unavailable," Client EPP believes that the "Home office computer" may be unavailable for as long as 3 days. With an average number of 2.74 ($\frac{1000}{365}$) control instructions being sent each day, the consequence with respect to the quality asset is 8.

The result of the detailed analysis is five risks. Based on the risk function, defined in Equations (1) and (2) on page 32, the estimated number of control instructions sent each year (1000), and the required service levels for the control instructions service, we can calculate the risk values of the five risks. These are as follows:

- The risk value of "Outsider decrypts control instructions message sent to Public telecom system and discloses the control instructions contained in the message" is *Acceptable* since

  $$\textit{Expected service level} = [0.9981, 0.9994]$$

  is greater than

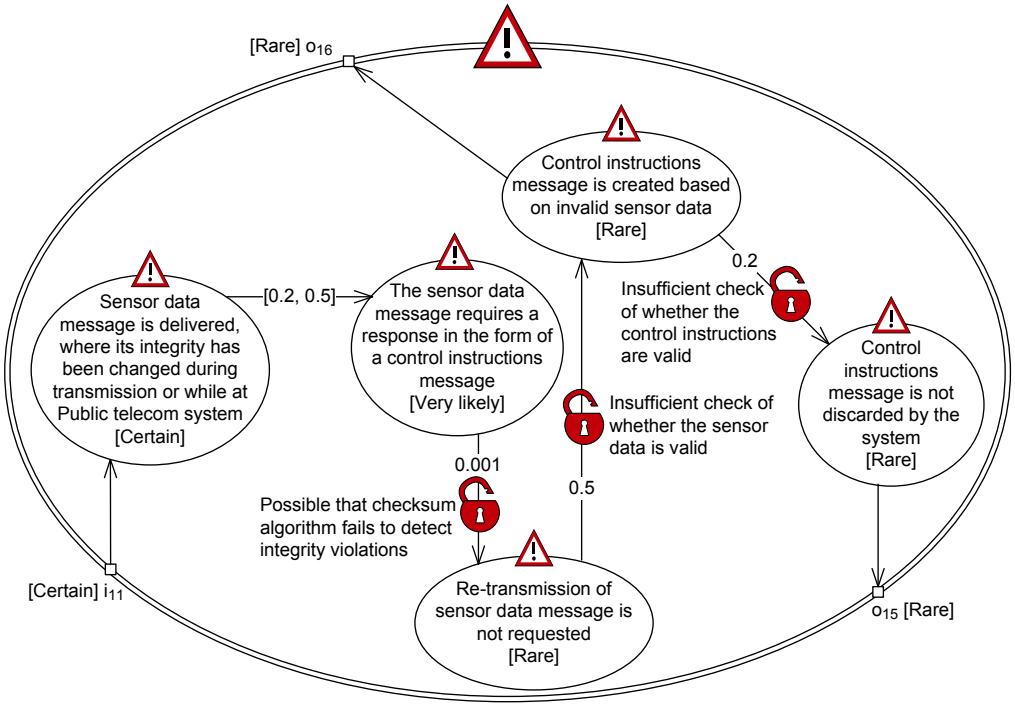


Figure 31: The referenced threat scenario "Sensor data message with lack of integrity is delivered to Home office computer," referred to in Figure 29

$$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.995, 0.995]$$

- The risk value of "Incorrect control instructions are sent to Public telecom system due to fake sensor data message sent by outsider to Home office computer" is *Unacceptable*

  $$Expected\ service\ level = [0.9981, 0.9994]$$

  is less than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.999, 0.999]$$

- The risk value of "Incorrect control instructions are sent to Public telecom system due to use of invalid sensor data" is *Acceptable*

  $$Expected\ service\ level = [0.9999, 1]$$

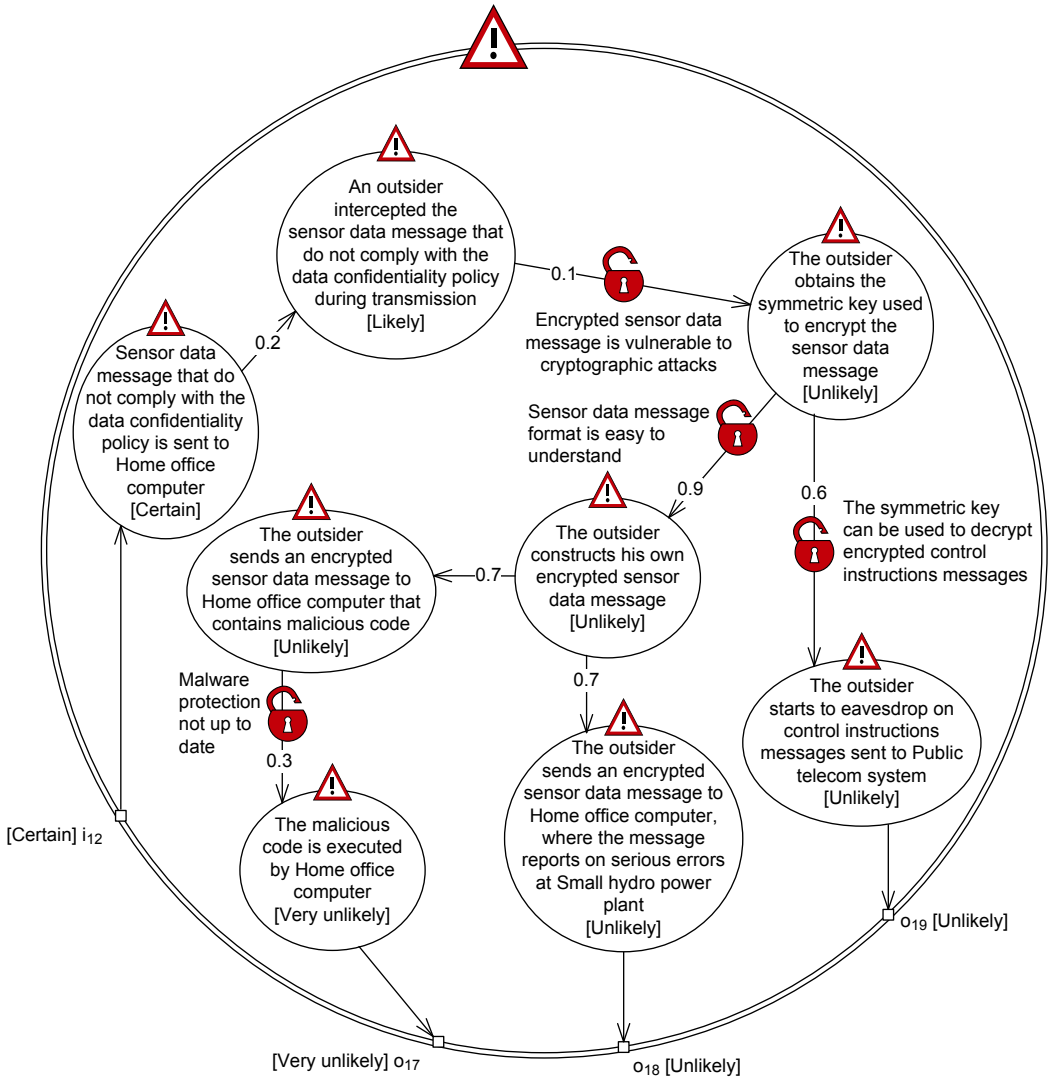
  is greater than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.999, 0.999]$$

- The risk value of "No control instructions messages are sent to Public telecom system due to Home office computer being unavailable" is *Unacceptable*

  $$Expected\ service\ level = [0.996, 0.9984]$$

  is less than



Sensor data message that do not comply with the data confidentiality policy is sent to Home office computer

Figure 32: The referenced threat scenario "Sensor data message that do not comply with the data confidentiality policy is sent to Home office computer," referred to in Figure 29

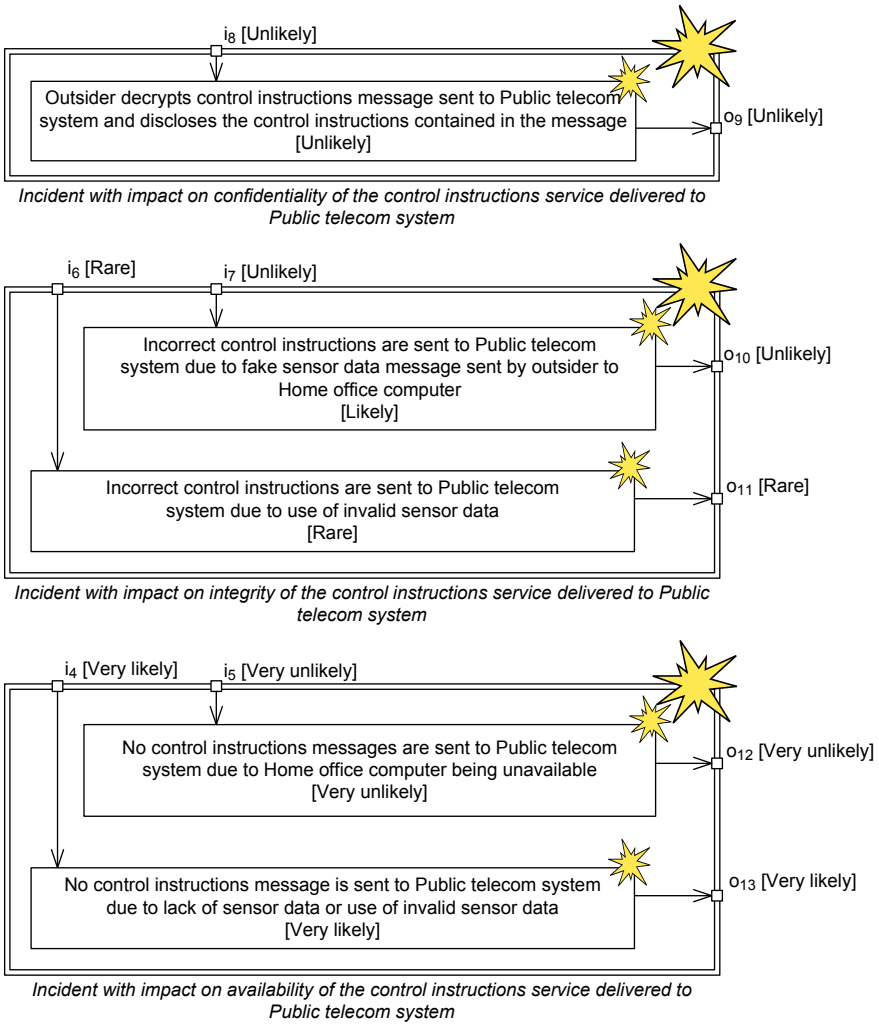


Figure 33: The referenced unwanted incidents "Incident with impact on confidentiality of the control instructions service delivered to Public telecom system," "Incident with impact on integrity of the control instructions service delivered to Public telecom system," and "Incident with impact on availability of the control instructions service delivered to Public telecom system," referred to in Figure 27

$$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.9999, 0.9999]$$

- The risk value of "No control instructions message is sent to Public telecom system due to lack of sensor data or use of invalid sensor data" is *Unacceptable*

  $$Expected\ service\ level = [0.9501, 0.99]$$

  is less than

  $$\frac{Required\ service\ level}{Maximum\ service\ level} = [0.9999, 0.9999]$$

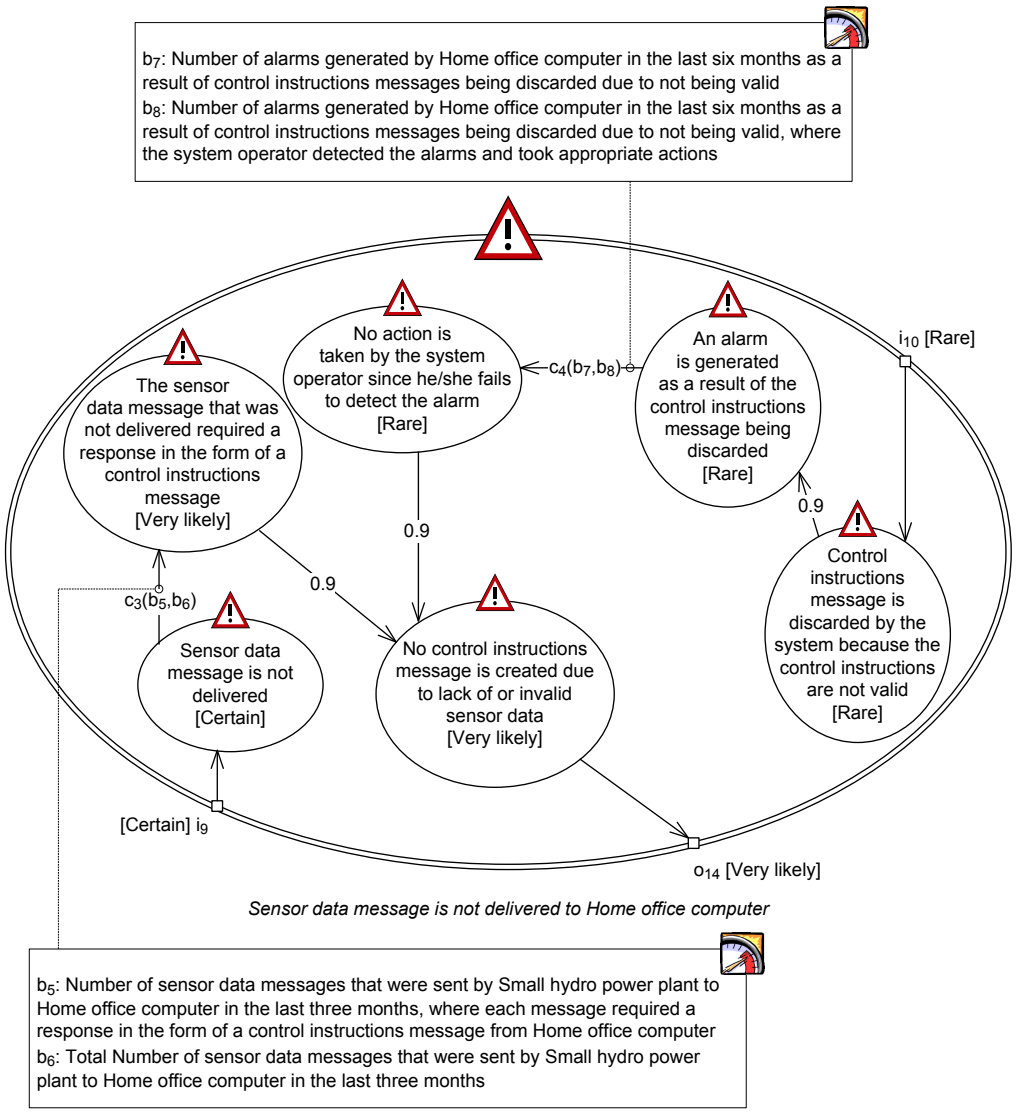


Figure 34: Relevant indicators, assigned to leads-to relations in the referenced threat scenario in Figure 30 for monitoring the risk "No control instructions message is sent to Public telecom system due to lack of sensor data or use of invalid sensor data"

C.1.2 Relevant indicators for risk monitoring

Client EPP believes that the likelihood value used to calculate the risk value of the risk "No control instructions message is sent to Public telecom system due to lack of sensor data or use of invalid sensor data" may be subject to change. We therefore decide to monitor this risk.

Indicators should be used to monitor likelihood values, since the likelihood value used to calculate the risk value of the risk may be subject to change. Client EPP does not find it feasible to directly monitor the likelihood of the unwanted incident occurring, and has therefore decided to monitor the conditional likelihoods of three leads-to relations in the referenced threat scenarios in Figures 30 and 31 that affect the likelihood of the unwanted incident occurring. The relevant indicators for the three leads-to relations are presented in Figures 34 and 35. In Appendix D.3 we show how to use the conditional likelihoods we now address as well as other factors to monitor the resulting likelihood of the risk identified for monitoring.

One composite indicator c_3, which aggregates the two basic indicators b_5 and b_6, has been

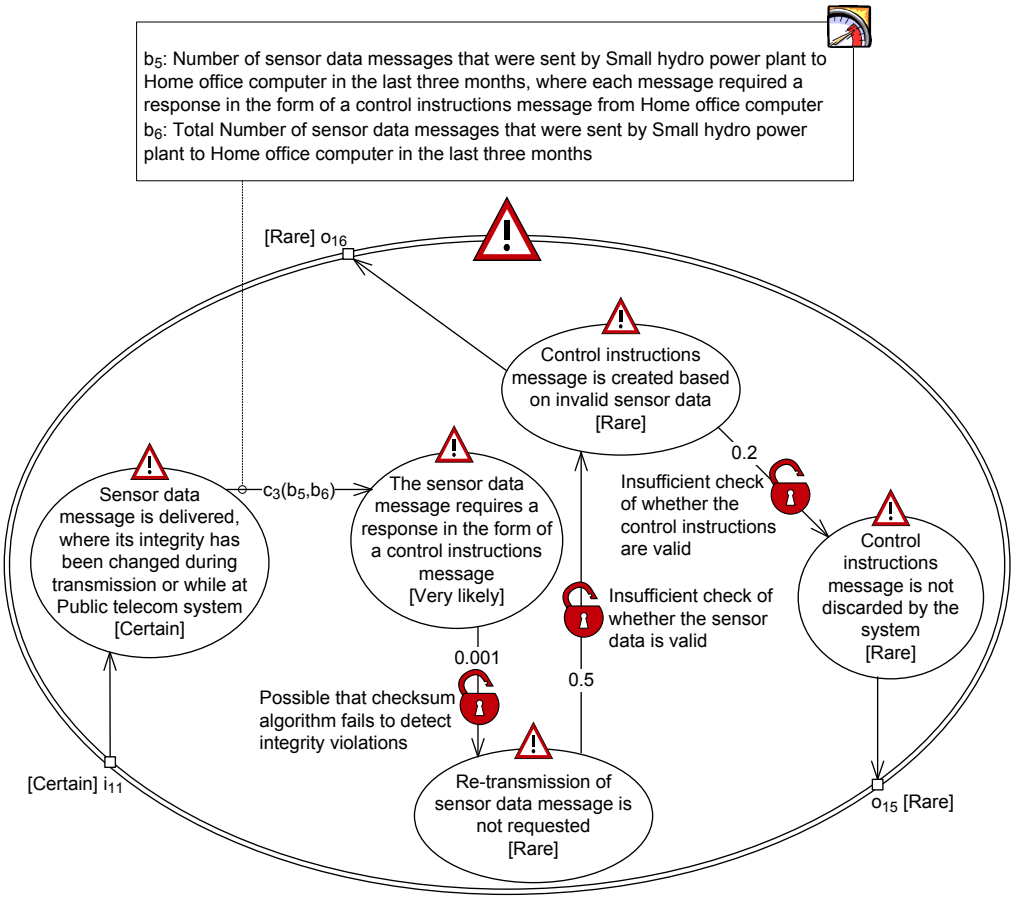


Figure 35: Relevant indicators, assigned to a leads-to relation in the referenced threat scenario in Figure 31, for monitoring the risk "No control instructions message is sent to Public telecom system due to lack of sensor data or use of invalid sensor data"

identified for two of the leads-to relations. c_3 calculates the ratio of sensor data messages that required responses in form of control instructions messages to all sensor data messages. For the third leads-to relation, we have identified the composite indicator c_4, which aggregates the two basic indicators b_7 and b_8. c_4 calculates the ratio of alarms where appropriate actions were taken by the system operator to all alarms generated.

C.1.3 Design and deployment of indicators for risk monitoring

In Figure 34, the composite indicators c_3 and c_4 are associated with one leads-to relation each. Moreover, c_3 is also associated with one leads-to relation in Figure 35. Conditional likelihoods were assigned to all of these leads-to relations during the detailed analysis described in Appendix C.1.1. Values are therefore obtained for all the basic indicators from the time when the referenced threat scenarios in Figures 30 and 31 were constructed constructed. For b_5 and b_6 we obtain the values 590 and 1255, respectively, while for b_7 and b_8 we obtain the value 20 for both.

In Tables 7–9 are the design specifications for the different basic and composite indicators. All the specifications have been given in the form of algorithms. The four algorithms are to be used by a risk monitor within the electrical power production infrastructure. The indicators are updated each month. Afterwards, the risk picture is updated based on the updated composite indicators.

The input $data_1$ is used by the algorithm for b_5 and b_6, while the inputs $data_2$ and $data_3$ are used by the algorithm for b_7 and b_8. It should be noticed that the first time the two algorithms are executed, the input $data_1$ consists of events that have been generated during the last three months, while the inputs $data_2$ and $data_3$ consist of events that have been generated during the last six months. This has been done in order to ensure correct calculation of the indicators. For all other executions of the two algorithms, the inputs will only consist of events that have been generated during the last month.

The composite indicator c_3 aggregates the two indicators b_5 and b_6. As can be seen in Figures 30 and 31, Client EPP has estimated that between 20% and 50% of the sensor data messages require responses in the form of control instructions messages. Thus, the probability interval $[0.2, 0.5]$. Client EPP finds it very likely that most values of c_3 should be contained in this interval, but is also aware of that some values may be lower than 0.2 or higher than 0.5. In Client EPP's opinion, the minimum value for c_3 should be 0.1. Thus, if the aggregation of b_5 and b_6 results in a value less than 0.1, then c_3 is assigned the value 0.1. It should be noticed that we do not perform any checks of whether b_6 is zero in the design specification in Table 7. This is due to that b_6 will never be zero. By using the obtained values for the basic indicators as input to the algorithm we get 0.47. This number is in accordance with the initial estimate of $[0.2, 0.5]$.

The composite indicator c_4 aggregates the two indicators b_7 and b_8. Client EPP is of the opinion that the system operator fails to notice at least 1% of the alarms. Thus, the minimum value for c_4 should be 0.01. If b_7 does not equal zero, then c_4 is 1 minus the ratio of b_8 to b_7. If the result of this calculation is less than 0.01, then c_4 is assigned the minimum value of 0.01. By using the obtained values for the basic indicators as input to the algorithm we get 0.01. This number is in accordance with the initial estimate of 0.01.

In Tables 10 and 11 are the deployment specifications for the basic and composite indicators.

Table 7: Design specifications, in the form of algorithms, for the basic indicators b_5 and b_6 and the composite indicator c_3

Algorithm for b_5 and b_6

Input: $data_1$: "Events generated by the control system at Small hydro power plant, where each event was generated as a result of sending a sensor data message"

Data maintained by the risk monitor: $event\ log_1$: "Events generated by the control system at Small hydro power plant during the last three months, where each event represents the sending of a sensor data message which required a response in the form of a control instructions message," $event\ log_2$: "Events generated by the control system at Small hydro power plant during the last three months, where each event represents the sending of a sensor data message"

Remove all events from $event\ log_1$ that were generated for more than three months ago.

Extract all events from $data_1$ that required a response in the form of a control instructions message. Add the extracted events to $event\ log_1$.

Remove all events from $event\ log_2$ that were generated for more than three months ago.

Extract all events from $data_1$. Add the extracted events to $event\ log_2$.

b_5 := "The number of events in $event\ log_1$"

b_6 := "The number of events in $event\ log_2$"

Output: b_5, b_6

Algorithm for c_3

Input: b_5: "Number of sensor data messages that were sent by Small hydro power plant to Home office computer in the last three months, where each message required a response in the form of a control instructions message from Home office computer," b_6: "Total number of sensor data messages that were sent by Small hydro power plant to Home office computer in the last three months"

$c_3 := \dfrac{b_5}{b_6}$

if $c_3 < 0.1$ **then**

  $c_3 := 0.1$

end if

Output: c_3

Table 8: Design specification, in the form of an algorithm, for the basic indicators b_7 and b_8

Algorithm for b_7 and b_8
Input: $data_2$: "Events generated by the Home office computer, where each event represents an alarm," $data_3$: "Events generated by the Home office computer, where each event represents the response to an alarm"
Data maintained by the risk monitor: $event\ log_3$: "Events generated by the Home office computer during the last six months, where each event represents an alarm that was generated as a result of a control instructions message being discarded due to not being valid," $event\ log_4$: "Events generated by the Home office computer during the last six months, where each event represents the system operator responding to an alarm generated as a result of a control instructions message being discarded due to not being valid"
Remove all events from $event\ log_3$ that were generated for more than six months ago.
Extract all events from $data_2$ where each event represents the generation of an alarm as a result of a control instructions message being discarded due to not being valid. Add the extracted events to $event\ log_3$.
Remove all events from $event\ log_4$ that were generated for more than six months ago.
Extract all events from $data_3$ where each event represents that the system operator responded to an alarm generated as a result of a control instructions message being discarded due to the control instructions not being valid. Add the extracted events to $event\ log_4$.
b_7 := "The number of events in $event\ log_3$"
b_8 := "The number of events in $event\ log_4$"
Output: b_7, b_8

Table 9: Design specification, in the form of an algorithm, for the composite indicator c_4

Algorithm for c_4

Input: b_7: "Number of alarms generated by Home office computer in the last six months as a result of control instructions messages being discarded due to not being valid," b_8: "Number of alarms generated by Home office computer in the last six months as a result of control instructions messages being discarded due to not being valid, where the system operator detected the alarms and took appropriate actions"
 	
if $b_7 \neq 0$ **then**
$c_4 := 1 - \frac{b_8}{b_7}$
else
$c_4 := 0.01$
end if
if $c_4 < 0.01$ **then**
$c_4 := 0.01$
end if
 	
Output: c_4

Table 10: Deployment specification for the basic indicators b_5 and b_6 and the composite indicator c_3

Deployment specification for b_5**,** b_6**, and** c_3
Extraction and transmission of $data_1$**:** The control system at the "Small hydro power plant" has an event log that contains different events generated by the control system. At the start of each month, an automated ICT process extracts all events from the event log that have been generated as a result of sending sensor data messages to "Home office computer" and where each event was generated during the last month. It should be noticed that the process will extract all events that have been generated during the last three months the first time it is executed. We refer to the extracted data as $data_1$. The process transmits $data_1$ to the risk monitor by using the internal data network of the electrical power production infrastructure.

Table 11: Deployment specification for the basic indicators b_7 and b_8 and the composite indicator c_4

Deployment specification for b_7, b_8, and c_4
Extraction and transmission of $data_2$: The "Home office computer" has an event log that contains different events generated by the computer. At the start of each month, an automated ICT process extracts all events from the event log that represent alarms and where each event was generated during the last month. It should be noticed that the process will extract all events that have been generated during the last six months the first time it is executed. We refer to the extracted data as $data_2$. The process transmits $data_2$ to the risk monitor by using the public telecom infrastructure. **Extraction and transmission of $data_3$:** At the start of each month, an automated ICT process extracts all events from the event log that represent responses to alarms and where each event was generated during the last month. It should be noticed that the process will extract all events that have been generated during the last six months the first time it is executed. We refer to the extracted data as $data_3$. The process transmits $data_3$ to the risk monitor by using the public telecom infrastructure.

C.2 Electricity service provided to Distribution line 2

C.2.1 Detailed threat diagrams

In Figure 36 is the detailed version of the high-level threat diagram in Figure 24 on page 54. The referring elements in Figure 36 refer to the referenced threat scenarios provided in Figures 37 and 38, and the referenced unwanted incident provided in Figure 42. Moreover, the referenced threat scenario in Figure 38 contains three referring threat scenarios, which refer to the referenced threat scenarios provided in Figures 39–41. Client EPP has estimated all the likelihood and consequence values in the different figures.

As can be seen in Figure 36, the vulnerability "Electricity service depends on control instructions service" in Figure 24 has been decomposed into three vulnerabilities. The referenced threat scenario in Figure 37 is a detailing of the referring threat scenario "Control instructions service is not delivered according to requirements" in Figure 24. Since "Public telecom sys-

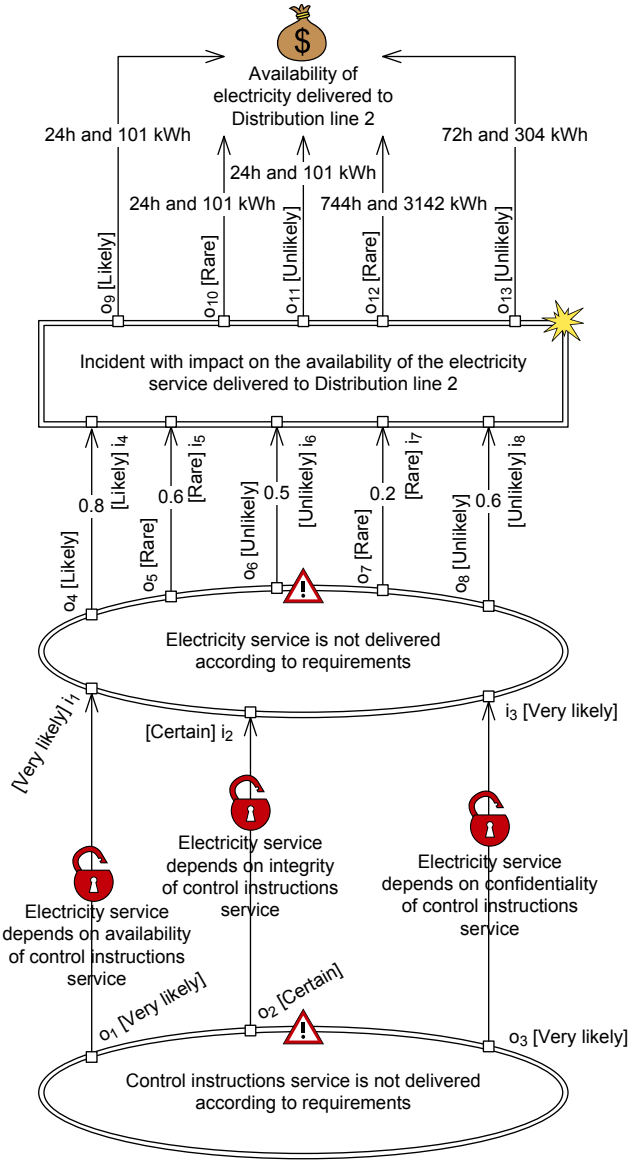


Figure 36: Detailed version of the high-level threat diagram in Figure 24 on page 54

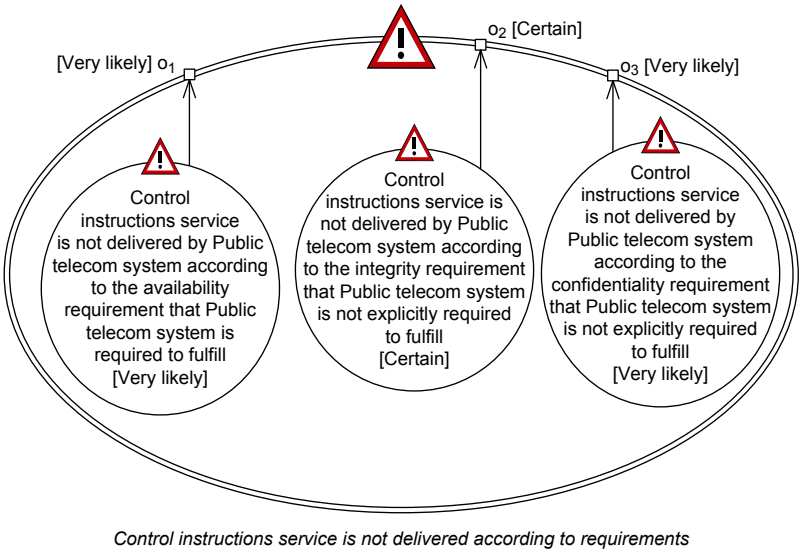


Figure 37: The referenced threat scenario "Control instructions service is not delivered according to requirements," referred to in Figure 36

tem" is only required to deliver the control instructions service according to the availability requirement, the referenced threat scenario distinguish between the failure of not achieving the availability requirement, and the failures of not achieving the confidentiality and integrity requirements.

Client EPP estimates that 1000 control instructions messages are sent each year to "Small hydro power plant." Moreover, Client EPP estimates the maximum amount of electricity delivered in the period of one year to each of "Distribution line 2" and "Distribution line 3" to be 37 MWh. The likelihoods of the control instructions service not being delivered according to the confidentiality, integrity, and availability requirements are identical to the ones calculated in Section 5.3. The likelihoods are as follows:

- The likelihood of the control instructions service not being delivered according to the confidentiality requirement is "Very likely."
- The likelihood of the control instructions service not being delivered according to the integrity requirement is "Certain."
- The likelihood of the control instructions service not being delivered according to the availability requirement is "Very likely."

The referenced threat scenario "Electricity service is not delivered according to requirements" is given in Figure 38. The internal threat behavior of "Small hydro power plant" is described by the referenced threat scenarios in Figures 39–41. The different referenced threat scenarios describe how "Small hydro power plant" may fail to deliver the electricity service according to requirements as a result of "Public telecom system" failing to deliver the control instructions service according to its requirements.

Figure 42 contains the referenced unwanted incident referred to in Figure 36. For most of the unwanted incidents, with the exceptions of "Small hydro power plant is shut down due to malicious software" and "Small hydro power plant is shut down due to damage to unstable power generator," Client EPP assign the consequence value of "24h and 101 kWh" (h is hours and kWh is kilowatt hours) with respect to the quality asset. Client EPP believes that the electricity

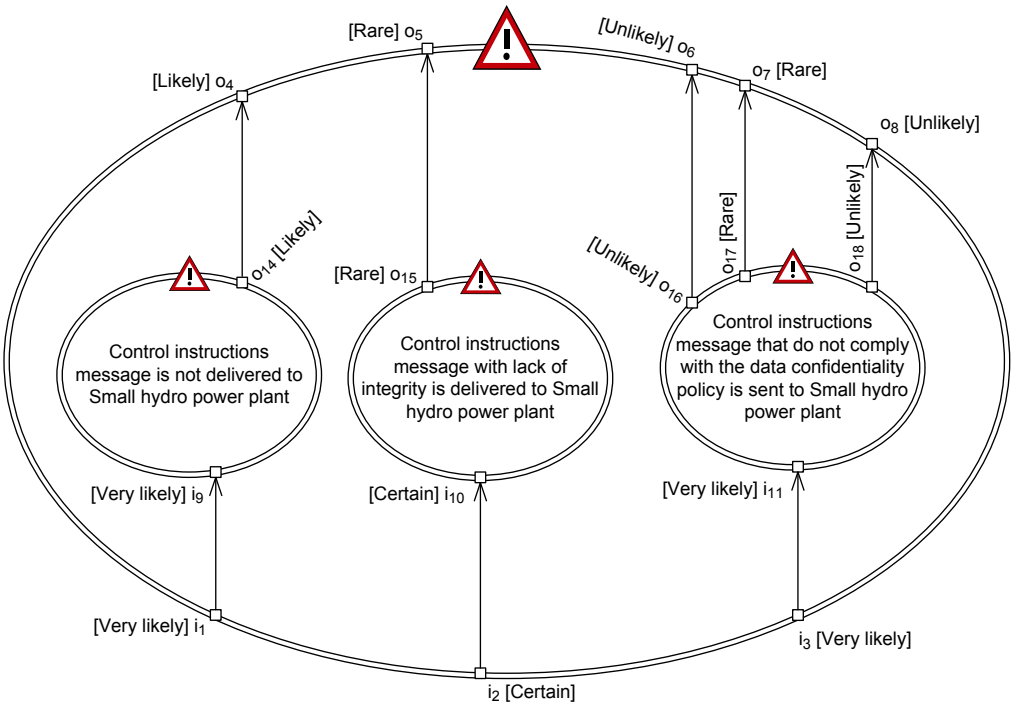


Figure 38: The referenced threat scenario "Electricity service is not delivered according to requirements," referred to in Figure 36

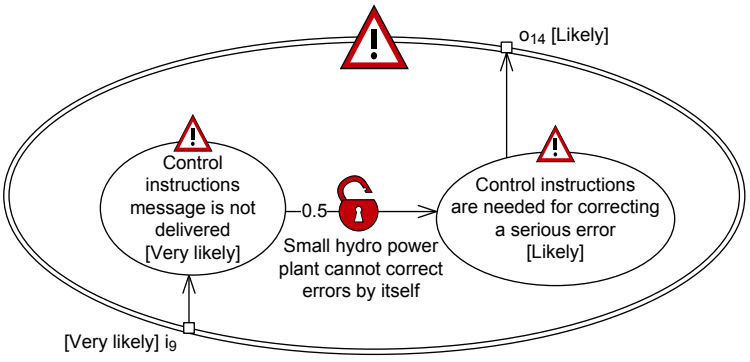


Figure 39: The referenced threat scenario "Control instructions message is not delivered to Small hydro power plant," referred to in Figure 38

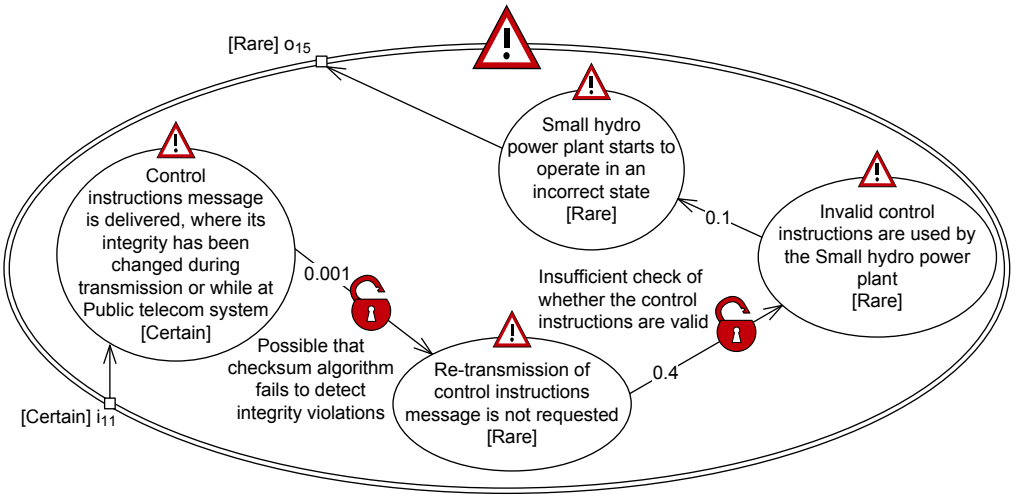


Figure 40: The referenced threat scenario "Control instructions message with lack of integrity is delivered to Small hydro power plant," referred to in Figure 38

service will not be provided for 24 hours. 101 kWh ($\frac{37000}{365}$) is the average amount of electricity produced for "Distribution line 2" in one day. For the incident "Small hydro power plant is shut down due to malicious software," Client EPP believes that "Small hydro power plant" will be shut down for three days (72 hours). Moreover, for the unwanted incident "Small hydro power plant is shut down due to damage to unstable power generator," Client EPP believes that such an incident may result in a down time of 31 days (744 hours), since it is very likely that the power generator needs to be replaced as a result of the incident.

The result of the detailed analysis is five risks. Based on the risk function, defined in Equations (3)–(5) on pages 51 and 52, the maximum service levels *Maximum service level*$_T$ (24 hours · 365 days = 8760 hours) and *Maximum service level*$_E$ (37 MWh per year), and the two availability requirements specified in the required service level of the electricity service, we can calculate the risk values of the five risks.

In the case of the risk "Small hydro power plant is shut down due to lack of control instructions for correcting errors," the *Expected service level*$_T$ is less than $\frac{Required\ service\ level_T}{Maximum\ service\ level_T}$, while the *Expected service level*$_E$ is less than $\frac{Required\ service\ level_E}{Maximum\ service\ level_E}$. This means that the risk value is *Unacceptable*. Below we present the calculations for this case. Notice that all the values are for

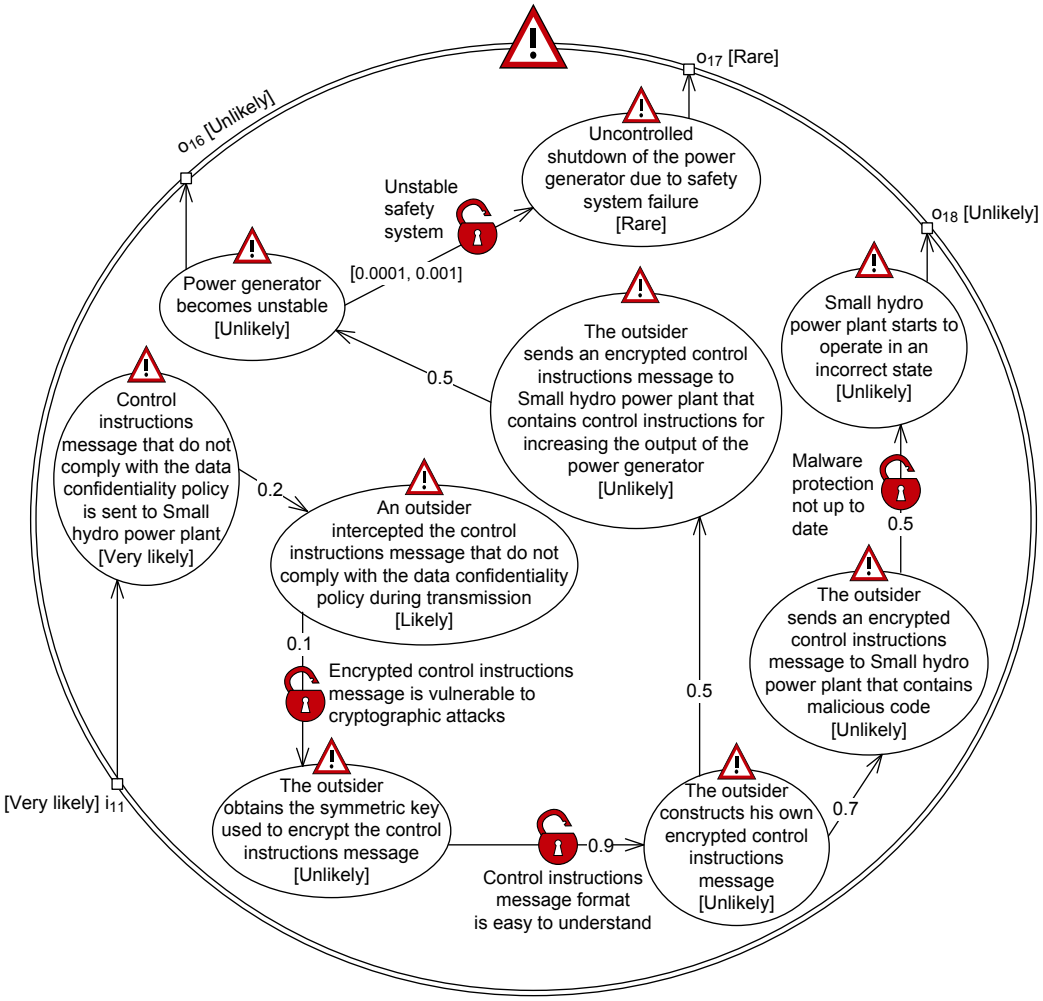


Figure 41: The referenced threat scenario "Control instructions message that do not comply with the data confidentiality policy is sent to Small hydro power plant," referred to in Figure 38

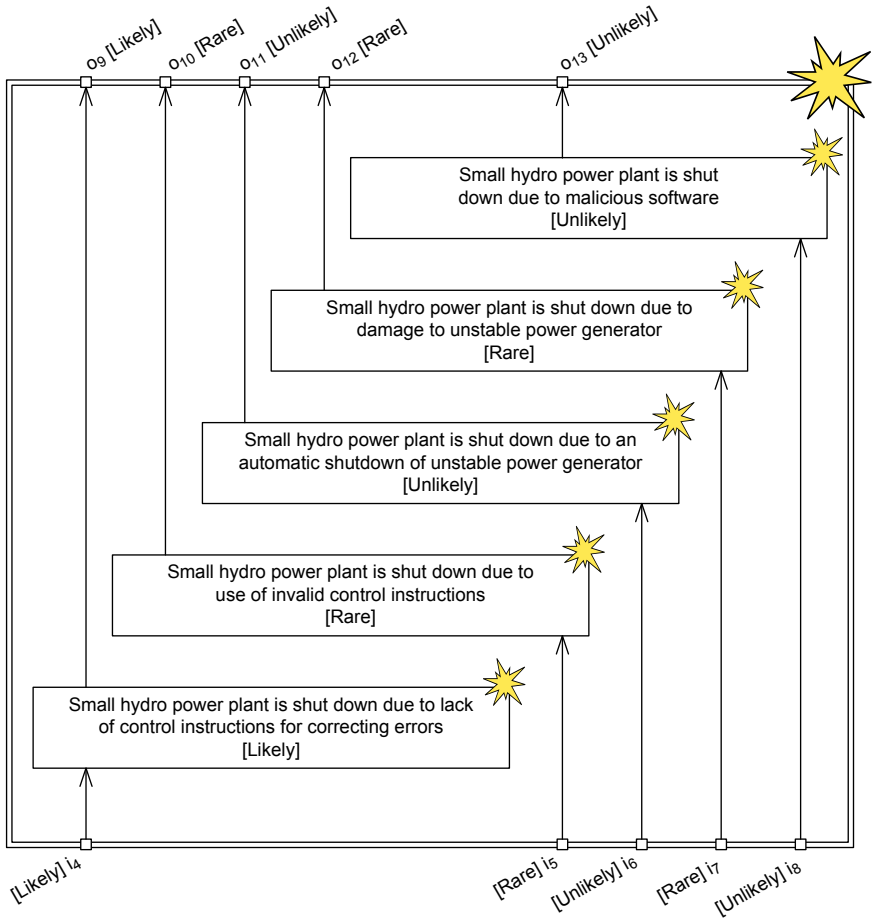


Figure 42: The referenced unwanted incident “Incident with impact on the availability of the electricity service delivered to Distribution line 2,” referred to in Figure 36

the period of one year.

$$
\begin{aligned}
\textit{Expected service level}_T &= \frac{\textit{Maximum service level}_T - (\textit{Likelihood} \cdot \textit{Consequence}_T)}{\textit{Maximum service level}_T} \\
&= \frac{8760 - ([5, 9.9] \cdot 24)}{8760} \\
&= \frac{[8760, 8760] - ([5, 9.9] \cdot [24, 24])}{[8760, 8760]} \\
&= \frac{[8760, 8760] - [120, 237.6]}{[8760, 8760]} \\
&= \frac{[8522.4, 8640]}{[8760, 8760]} \\
&= [0.9729, 0.9863]
\end{aligned}
$$

$$
\begin{aligned}
\frac{\textit{Required service level}_T}{\textit{Maximum service level}_T} &= \frac{8760 \cdot 0.995}{8760} \\
&= \frac{[8760, 8760] \cdot [0.999, 0.999]}{[8760, 8760]} \\
&= \frac{[8751.24, 8751.24]}{[8760, 8760]} \\
&= [0.999, 0.999]
\end{aligned}
$$

$$
\begin{aligned}
\textit{Expected service level}_E &= \frac{\textit{Maximum service level}_E - (\textit{Likelihood} \cdot \textit{Consequence}_E)}{\textit{Maximum service level}_E} \\
&= \frac{37000 - ([5, 9.9] \cdot 101)}{37000} \\
&= \frac{[37000, 37000] - ([5, 9.9] \cdot [101, 101])}{[37000, 37000]} \\
&= \frac{[37000, 37000] - [505, 999.9]}{[37000, 37000]} \\
&= \frac{[36000.1, 36495]}{[37000, 37000]} \\
&= [0.973, 0.9864]
\end{aligned}
$$

$$
\begin{aligned}
\frac{\textit{Required service level}_E}{\textit{Maximum service level}_E} &= \frac{36980}{37000} \\
&= 0.9995 \\
&= [0.9995, 0.9995]
\end{aligned}
$$

For the other risks, we end up with the following risk values:

- The risk value of "Small hydro power plant is shut down due to use of invalid control instructions" is *Acceptable* since

  $$\textit{Expected service level}_T = [0.9997, 1]$$

  is greater than

$$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

and since

$$Expected\ service\ level_E = [0.9997, 1]$$

is greater than

$$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

- The risk value of "Small hydro power plant is shut down due to an automatic shutdown of unstable power generator" is *Unacceptable* since

$$Expected\ service\ level_T = [0.9948, 0.9984]$$

is less than

$$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

and since

$$Expected\ service\ level_E = [0.9948, 0.9984]$$

is less than

$$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

- The risk value of "Small hydro power plant is shut down due to damage to unstable power generator" is *Unacceptable* since

$$Expected\ service\ level_T = [0.9915, 1]$$

is less than

$$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

and since

$$Expected\ service\ level_E = [0.9915, 1]$$

is less than

$$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

- The risk value of "Small hydro power plant is shut down due to malicious software" is *Unacceptable* since

$$Expected\ service\ level_T = [0.9844, 0.9951]$$

is less than

$$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

and since

$$Expected\ service\ level_E = [0.9844, 0.9951]$$

is less than

$$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

C.2.2 Relevant indicators for risk monitoring

Client EPP believes that both the likelihood value and the consequence value used to calculate the risk value of the risk "Small hydro power plant is shut down due to damage to unstable power generator" may be subject to change. We therefore decide to monitor this risk.

Client EPP does not find it feasible to directly monitor the likelihood of the unwanted incident occurring, and has therefore decided to monitor the conditional likelihood of a leads-to relation in the referenced threat scenario in Figure 41 that affects the likelihood of the unwanted incident occurring. In Figure 43 are relevant indicators for monitoring the conditional likelihood of the leads-to relation in Figure 41, while in Figure 44 are relevant indicators for monitoring the consequence of the impacts relation between the unwanted incident and the quality asset in the detailed high-level threat diagram in Figure 36. In Appendix D.4 we show how to use the conditional likelihood and the consequence we now address as well as other factors to monitor the risk value of the risk identified for monitoring.

One composite indicator c_5, which aggregates the two basic indicators b_9 and b_{10}, has been identified for the leads-to relation, while two composite indicators c_6 and c_7, where both aggregate the two basic indicators b_{11} and b_{12}, have been identified for the impacts relation. Client EPP relies on simulations to test the stability of the safety system. The software simulator uses data provided by sensors that monitors the state of the power generator and the safety system. In addition, the software simulator uses the ages of the power generator and the safety system as well as data on their previous failures as input. To monitor the basic indicators of the composite indicators c_6 and c_7, Client EPP relies on information from the vendor producing the power generators used by Client EPP, and information from the company maintaining and installing these generators.

C.2.3 Design and deployment of indicators for risk monitoring

In Figure 43 the composite indicator c_5 is associated with a leads-to relation, while in Figure 44 the composite indicators c_6 and c_7 are associated with an impacts relation. A conditional likelihood was assigned to the leads-to relation during the detailed analysis described in Appendix C.2.1, while a consequence value was assigned to the impacts relation associated with c_6 and c_7 during the same detailed analysis. Values are therefore obtained for all the basic indicators from the time when the detailed high-level threat diagram and the referenced threat scenario in Figures 36 and 41, respectively, were constructed. For b_9 and b_{10} we obtain the values 3 and 9997, respectively, while for b_{11} and b_{12} we obtain the values 28 and 3, respectively.

In Tables 12–14 are the design specifications for the different basic and composite indicators with the exception of the basic indicators b_{11} and b_{12}. These two basic indicators are so simple that no design specifications are needed. All the specifications have been given in the form of algorithms. The three algorithms are to be used by a risk monitor within the electrical power production infrastructure. The indicators b_9, b_{10}, and c_5 are updated each week, while the indicators b_{11}, b_{12}, c_6, and c_7 are updated every two weeks. The risk picture is updated after each composite indicator has been updated.

The algorithm for the two basic indicators b_9 and b_{10} is given in Table 12. It should be noticed that the two inputs $data_5$ and $data_6$ are only provided the first time the algorithm is

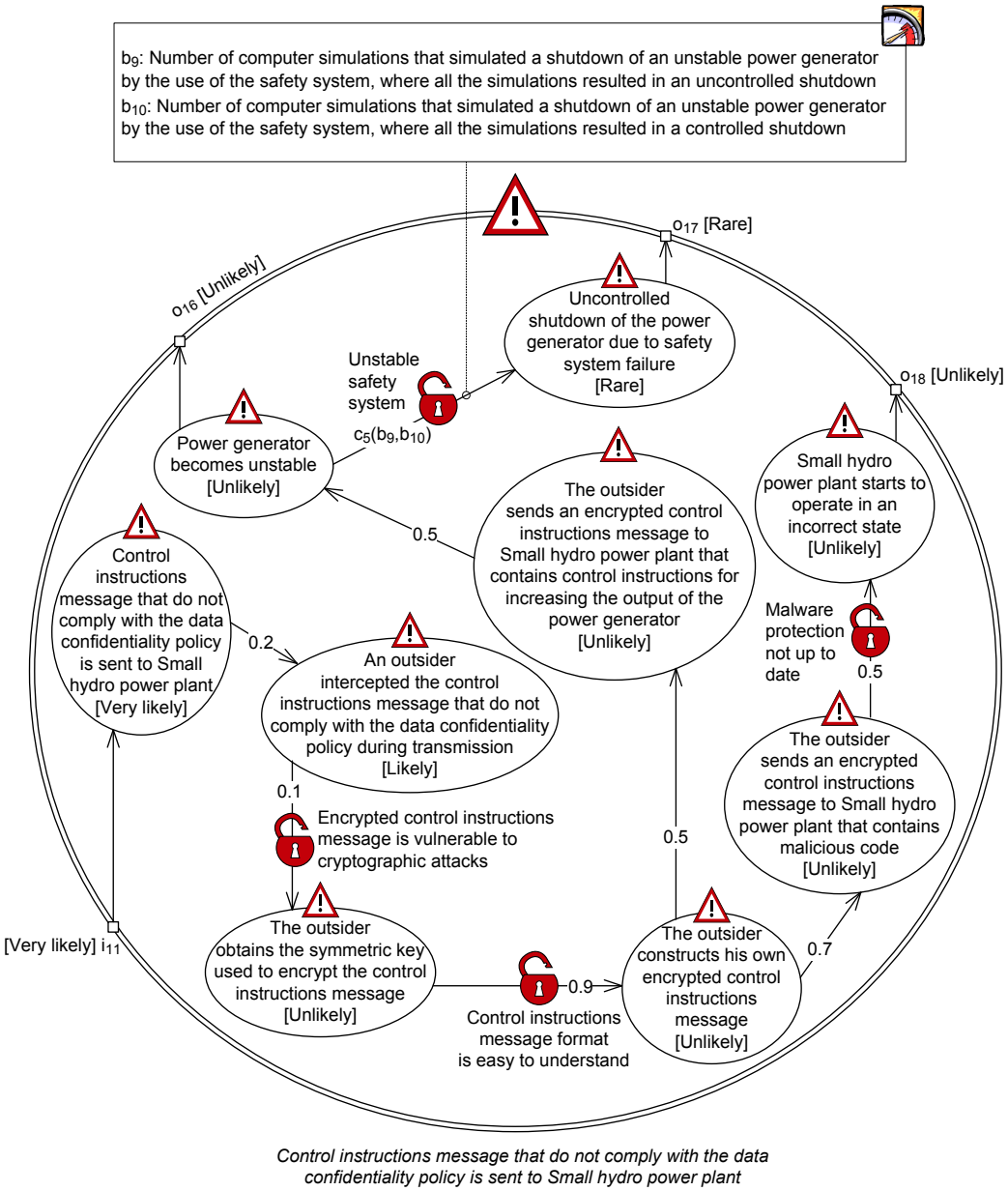


Figure 43: Relevant indicators, assigned to leads-to relations in the referenced threat scenario in Figure 41, for monitoring the risk "Small hydro power plant is shut down due to damage to unstable power generator"

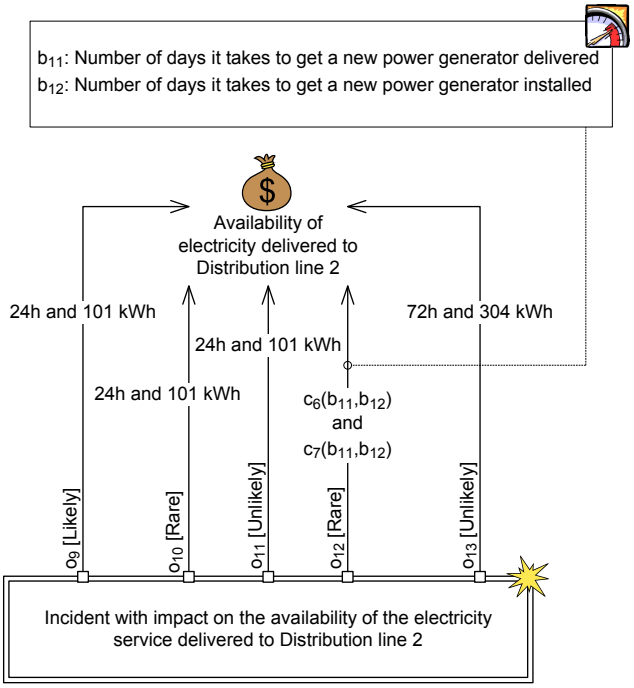


Figure 44: Relevant indicators, assigned to an impacts relation in an excerpt of the detailed high-level threat diagram in Figure 36, for monitoring the risk "Small hydro power plant is shut down due to damage to unstable power generator"

executed. The reason is that the two inputs will not change as long as the power generator and the safety system are not replaced. As can be seen in Table 12, the two inputs are used to initialize the two data items $time_1$ and $time_2$.

The composite indicator c_5 aggregates the two indicators b_9 and b_{10}. Client EPP understands that simulations cannot provide perfect predictions about the future, and decides therefore to come up with a minimum and a maximum value for c_5. Client EPP is of the opinion that the minimum value of c_5 should be 0.0001 (1 out of 10000 shutdowns of the unstable power generator results in an uncontrolled shutdown), and that the maximum value of c_5 should be 0.001 (10 out of 10000 shutdowns of the unstable power generator results in an uncontrolled shutdown). c_5 is calculated as the ratio of b_9 to $b_9 + b_{10}$. If c_5 is less than 0.0001 or greater than 0.001, then c_5 is assigned the value 0.0001 or the value 0.001, respectively. By using the obtained values for the basic indicators as input to the algorithm we get 0.0003, which is in accordance with the initial estimate of $[0.0001, 0.001]$.

The composite indicators c_6 and c_7 both aggregate the two indicators b_{11} and b_{12}. It should be noticed that neither of the indicators b_{11} and b_{12} can be equal to zero. The number 101.37 used to calculate c_7 is the average amount of electricity in kilowatt hours that is produced in one day by "Small hydro power plant" for "Distribution line 2." By using the obtained values for the basic indicators as input to the algorithm we get 744 for c_6, while we get 3142 for c_7. This is of course in accordance with the initial consequence estimate.

In Tables 15 and 16 are the deployment specifications for the basic and composite indicators.

Table 12: Design specifications, in the form of algorithms, for the basic indicators b_9 and b_{10}

Algorithm for b_9 and b_{10}

Input: $data_1$: "Sensor data for the period of one week backwards that describes the state of the power generator at Small hydro power plant," $data_2$: "Sensor data for the period of one week backwards that describes the state of the safety system at Small hydro power plant," $data_3$: "Data on previous failures for the power generator at Small hydro power plant," $data_4$: "Data on previous failures for the safety system at Small hydro power plant," $data_5$: "The installation time for the power generator at Small hydro power plant," $data_6$: "The installation time for the safety system at Small hydro power plant"

Data maintained by the risk monitor: $list_1$: "List containing data on all previous failures for the power generator at Small hydro power plant," $list_2$: "List containing data on all previous failures for the safety system at Small hydro power plant," $time_1$: "The installation time for the power generator at Small hydro power plant," $time_2$: "The installation time for the safety system at Small hydro power plant"

if First time the algorithm is executed **then**

$time_1$:= $data_5$, $time_2$:= $data_6$

end if

Based on $time_1$, calculate the age age_1 of the power generator

Based on $time_2$, calculate the age age_2 of the safety system

Update $list_1$ based on $data_3$

Update $list_2$ based on $data_4$

Initialize the software simulator with $data_1$, $data_2$, $list_1$, $list_2$, age_1, age_2

i := 0, b_9 := 0, b_{10} := 0

Start software simulator

while $i < 10000$ **do**

Simulate a shutdown of an unstable power generator by the use of the safety system

if Uncontrolled shutdown of the unstable power generator **then**

b_9 := b_9 + 1

else

b_{10} := b_{10} + 1

end if

i := i + 1

end while

Shutdown software simulator

Output: b_9, b_{10}

Table 13: Design specification, in the form of an algorithm, for the composite indicator c_5

Algorithm for c_5

Input: b_9: "Number of computer simulations that simulated a shutdown of an unstable power generator by the use of the safety system, where all the simulations resulted in an uncontrolled shutdown," b_{10}: "Number of computer simulations that simulated a shutdown of an unstable power generator by the use of the safety system, where all the simulations resulted in a controlled shutdown"
 	
$c_5 := \frac{b_9}{b_9 + b_{10}}$
if $c_5 < 0.0001$ **then**
$c_5 := 0.0001$
else
if $c_5 > 0.001$ **then**
$c_5 := 0.001$
end if
end if
 	
Output: c_5

Table 14: Design specification, in the form of an algorithm, for the composite indicators c_6 and c_7

Algorithm for c_6 **and** c_7
Input: b_{11}: "Number of days it takes to get a new power generator delivered," b_{12}: "Number of days it takes to get a new power generator installed" $c_6 := 24 \cdot (b_{11} + b_{12})$ $c_7 := 101.37 \cdot (b_{11} + b_{12})$ **Output:** c_6, c_7

Table 15: Deployment specification for the basic indicators b_9 and b_{10} and the composite indicator c_5

Deployment specification for b_9, b_{10}, and c_5
Extraction and transmission of $data_1$, $data_2$, $data_3$, $data_4$, $data_5$, and $data_6$: Client EPP has a maintenance database that contains information about different components and systems in the electrical power production infrastructure, including the power generator and the safety system at "Small hydro power plant." In the case of the power generator and the safety system, the database is updated at least on a daily basis by sensors that monitor the state of power generator and the safety system. Besides being updated by sensors, the database is also updated manually by humans. At the start of each week, an automated ICT process extracts all new sensor data that the database has been updated with in the period of one week backwards. We refer to the extracted sensor data for the power generator and the safety system as $data_1$ and $data_2$, respectively. If the power generator and/or the safety system experienced failures in the previous week, then the process extracts the data describing these failures. We refer to the extracted data describing previous failures for the power generator and the safety system as $data_3$ and $data_4$, respectively. The first time the automated ICT process is executed, it will extract all available data on previous failures for the power generator ($data_3$) and the safety system ($data_4$). It will also extract the installation time for the power generator and the safety system from the database. We refer to the former and the latter as $data_5$ and $data_6$, respectively. After having extracted the different data, the process transmits the data to the risk monitor by using the internal data network of the electrical power production infrastructure.

Table 16: Deployment specification for the basic indicators b_{11} and b_{12} and the composite indicators c_6 and c_7

Deployment specification for b_{11}, b_{12}, c_6, and c_7
Extraction and transmission of b_{11} and b_{12}: Every two weeks, an employee of Client EPP obtains the expected delivery time in days for a new power generator from the vendor producing the power generators used in the electrical power production infrastructure. The number obtained is the basic indicator b_{11}. The employee also obtains the expected installation time in days for a new power generator from the company that Client EPP uses for installing and maintaining power generators. The number obtained is the basic indicator b_{12}. The employee updates the maintenance database of Client EPP with these two numbers. After the database has been updated, an automated ICT process extracts b_{11} and b_{12}. The process transmits b_{11} and b_{12} to the risk monitor by using the internal data network of the electrical power production infrastructure.

C.3 Electricity service provided to Distribution line 3

C.3.1 Detailed threat diagrams

In Figure 45 is the detailed version of the high-level threat diagram in Figure 25 on page 55. With the only exceptions of the quality assets and the names of the referring unwanted incidents of Figures 36 and 45 being different, Figure 45 is identical to Figure 36.

The two electricity services provided to “Distribution line 2” and “Distribution line 3” share the referenced threat scenarios in Figures 37–41, since electricity cannot be provided by “Small hydro power plant” to “Distribution line 3” if it cannot be provided to “Distribution line 2” and vice versa. In Figure 46 is the referenced unwanted incident referred to in Figure 45. With the only exception of the names of the two referenced unwanted incidents in Figures 42 and 46 being different, Figure 46 is identical to Figure 42.

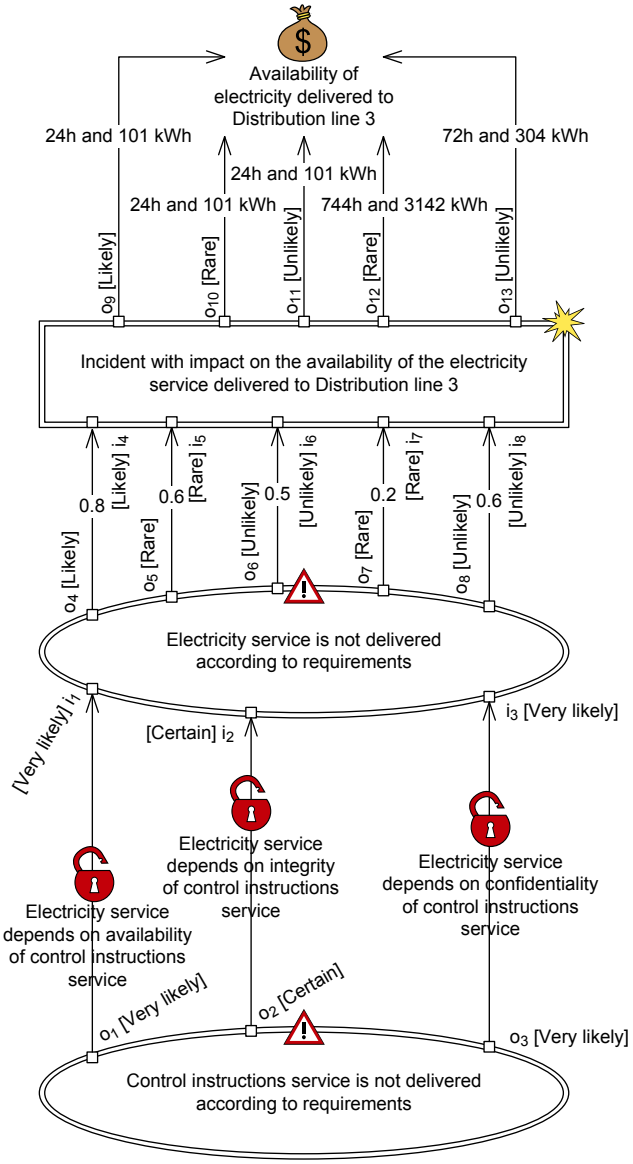


Figure 45: Detailed version of the high-level threat diagram in Figure 25 on page 55

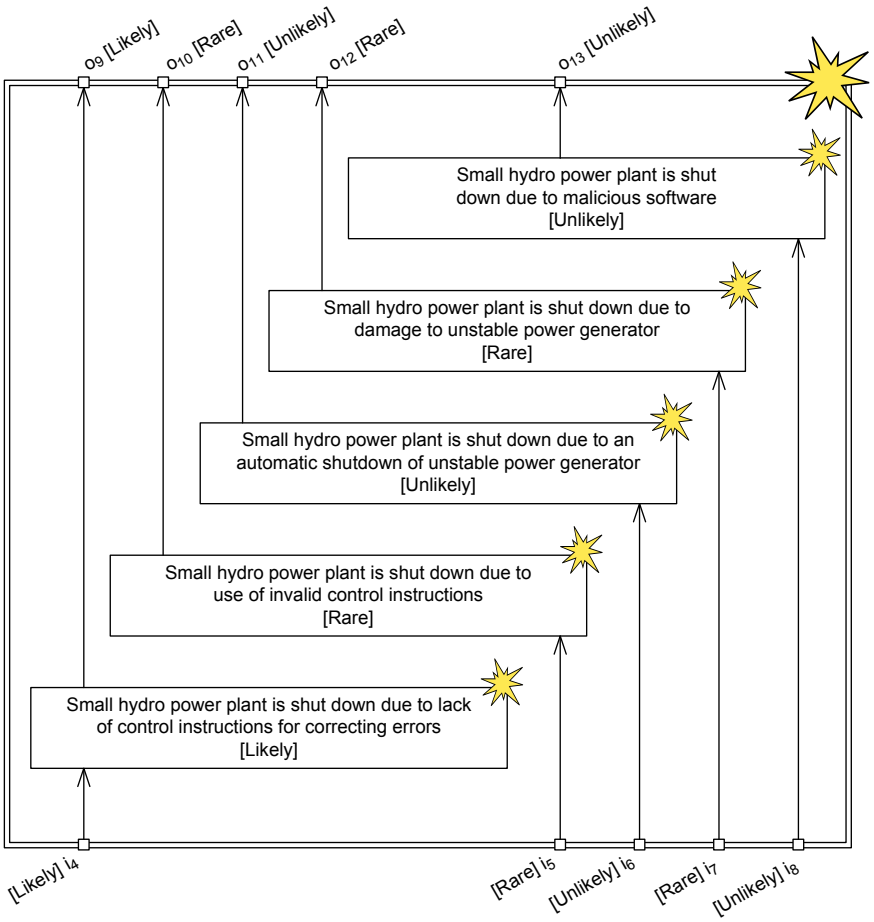


Figure 46: The referenced unwanted incident "Incident with impact on the availability of the electricity service delivered to Distribution line 3," referred to in Figure 45

C.3.2 Relevant indicators for risk monitoring

The relevant indicators for monitoring risk to quality of the electricity service provided to "Distribution line 3" are given in Appendix C.2.2.

C.3.3 Design and deployment of indicators for risk monitoring

Design and deployment specifications for the indicators for monitoring risk to quality of the electricity service provided to "Distribution line 3" are given in Appendix C.2.3.

C.4 Electricity service provided to Transmission line

C.4.1 Detailed threat diagrams

In Figure 47 is the detailed version of the high-level threat diagram in Figure 26 on page 57. The referring elements in Figure 47 refer to the referenced threat scenarios provided in Figures 48–52 and 57, and the referenced unwanted incident provided in Figure 58. Moreover, the referenced threat scenario in Figure 52 contains four referring threat scenarios, which refer to the referenced threat scenarios provided in Figures 53–56. Client EPP has estimated all the likelihood and consequence values in the different figures.

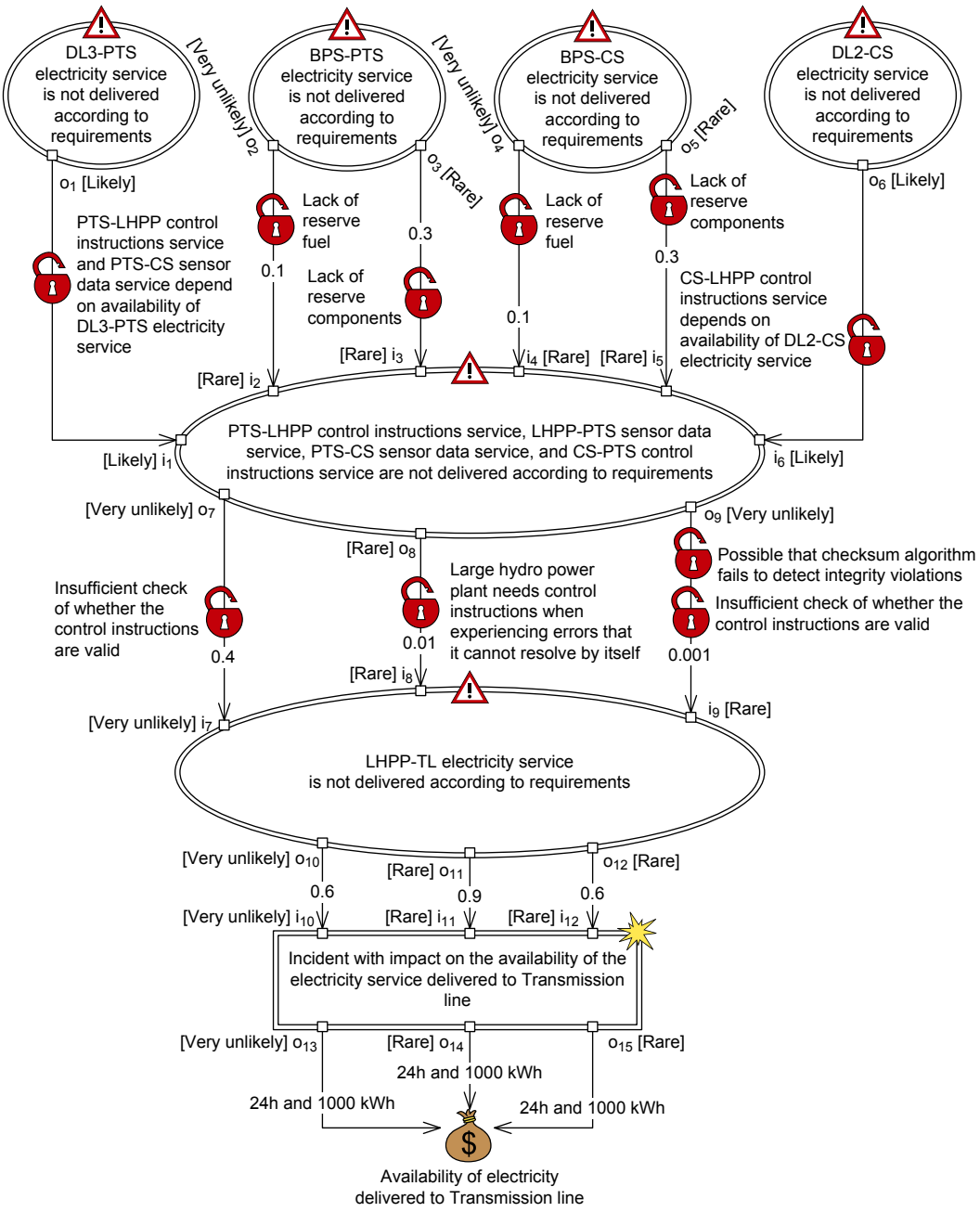


Figure 47: Detailed version of the high-level threat diagram in Figure 26 on page 57

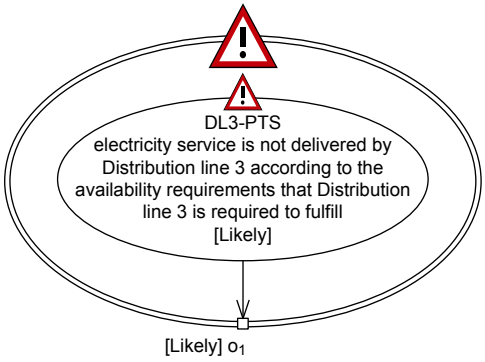


Figure 48: The referenced threat scenario "DL3-PTS electricity service is not delivered according to requirements," referred to in Figure 47

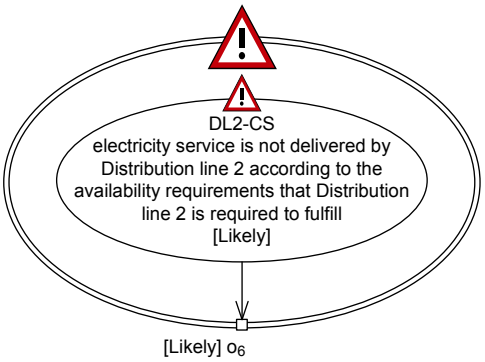


Figure 49: The referenced threat scenario "DL2-CS electricity service is not delivered according to requirements," referred to in Figure 47

As can be seen in Figure 47, the five vulnerabilities in Figure 26 have been decomposed into 10 vulnerabilities. The referenced threat scenarios in Figures 48 and 49 are the detailed versions of the referring threat scenarios "DL3-PTS electricity service is not delivered according to requirements" and "DL2-CS electricity service is not delivered according to requirements" in Figure 26, respectively. Both "Distribution line 3" and "Distribution line 2" need to fulfill the availability requirement when delivering electricity to "Private telecom system" and "Control system," respectively.

Client EPP estimates the maximum amount of electricity delivered in the period of one year to "Transmission line" to be 365 MWh. Before we can estimate the likelihoods of the DL3-PTS electricity service and the DL2-CS electricity service not being delivered according to their availability requirements, we need to calculate the worst-case service levels of the two services. These are as follows:

- DL3-PTS electricity service (availability with respect to time): $99.7\% \cdot 0.99 = 98.7\%$ – The service is available 98.7% of the time for "Private telecom system."
- DL3-PTS electricity service (availability with respect to electricity delivered): $10980 \cdot 0.99 = 10870.2$ kWh of electricity is delivered to "Private telecom system."
- DL2-CS electricity service (availability with respect to time): $99.7\% \cdot 0.99 = 98.7\%$ –

The service is available 98.7% of the time for "Control system."

- DL2-CS electricity service (availability with respect to electricity delivered): $21960 \cdot 0.99 = 21740.4$ kWh of electricity is delivered to "Control system."

The required service levels specify that:

- DL3-PTS electricity service (availability with respect to time): The service should be available 99.7% of the time for "Private telecom system."
- DL3-PTS electricity service (availability with respect to electricity delivered): 10980 kWh of electricity should be delivered to "Private telecom system."
- DL2-CS electricity service (availability with respect to time): The service should be available 99.7% of the time for "Control system."
- DL2-CS electricity service (availability with respect to electricity delivered): 21960 kWh of electricity should be delivered to "Control system."

To estimate likelihoods, we need to look at the differences between the required service levels and the worst-case service levels. The differences are as follows:

- DL3-PTS electricity service (availability with respect to time): $(8760 \cdot 0.997) - (8760 \cdot 0.987) = 87.6$ hours in the period of one year.
- DL3-PTS electricity service (availability with respect to electricity delivered): $10980 - 10870.2 = 109.8$ kWh of electricity in the period of one year.
- DL2-CS electricity service (availability with respect to time): $(8760 \cdot 0.997) - (8760 \cdot 0.987) = 87.6$ hours in the period of one year.
- DL2-CS electricity service (availability with respect to electricity delivered): $21960 - 21740.4 = 219.6$ kWh of electricity in the period of one year.

The "Private telecom system" uses an amount of about 30 kWh daily, while the "Control system" uses an amount of about 60 kWh daily. If electricity is not provided for three days to 'Private telecom system" and "Control system," then the amounts not delivered will be close to 109.8 kWh and 219.6 kWh. Moreover, the time the two services are not available will also be close to 87.6 hours. Client EPP does however not find it reasonable that electricity is not delivered for three full days to "Private telecom system" and "Control system." Thus, Client EPP believes that the likelihood for both services should be higher than three. Based on the differences between the required service levels and the worst-case service levels, Client EPP estimates the likelihood of the DL3-PTS electricity service not being delivered according to the availability requirements to be between 5 and 10 times per year ("Likely"). Moreover, Client makes the same estimate for the DL2-CS electricity service.

The referenced threat scenarios in Figures 50 and 51 are the detailed versions of the referring threat scenarios "BPS-PTS electricity service is not delivered according to requirements" and "BPS-CS electricity service is not delivered according to requirements" in Figure 26, respectively, while the referenced threat scenario in Figure 52 is the detailed version of the referring threat scenario "PTS-LHPP control instructions service, LHPP-PTS sensor data service, PTS-CS sensor data service, and CS-PTS control instructions service are not delivered according to requirements" in Figure 26. The referenced threat scenario consists of four referring threat scenarios that refer to the referenced threat scenarios in Figures 53–56. Moreover, the referenced threat scenario in Figure 57 is the detailed version of the referring threat scenario "LHPP-TL electricity service is not delivered according to requirements" in Figure 26.

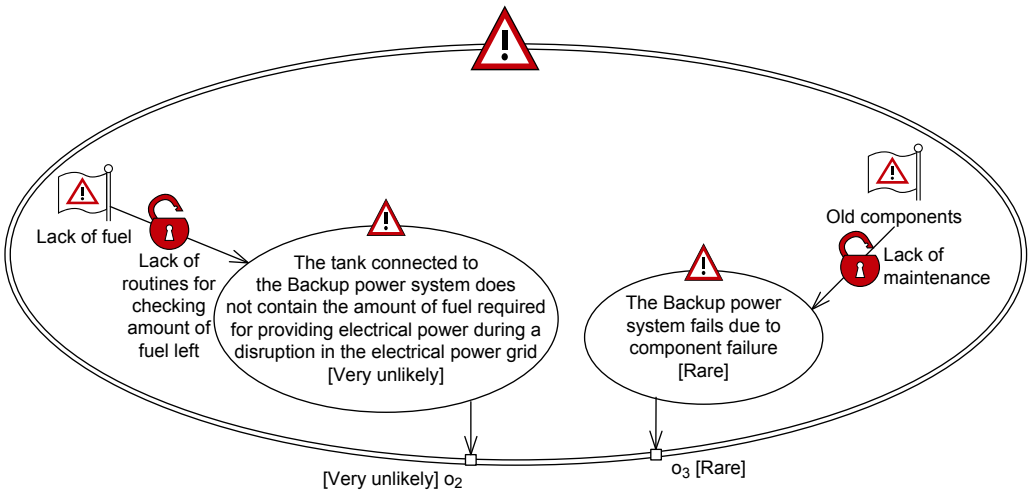


Figure 50: The referenced threat scenario "BPS-PTS electricity service is not delivered according to requirements," referred to in Figure 47

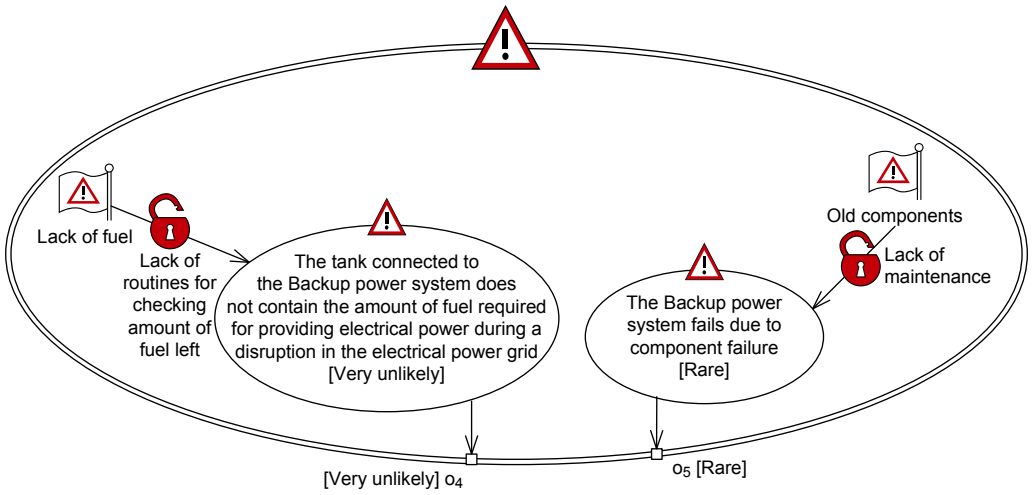
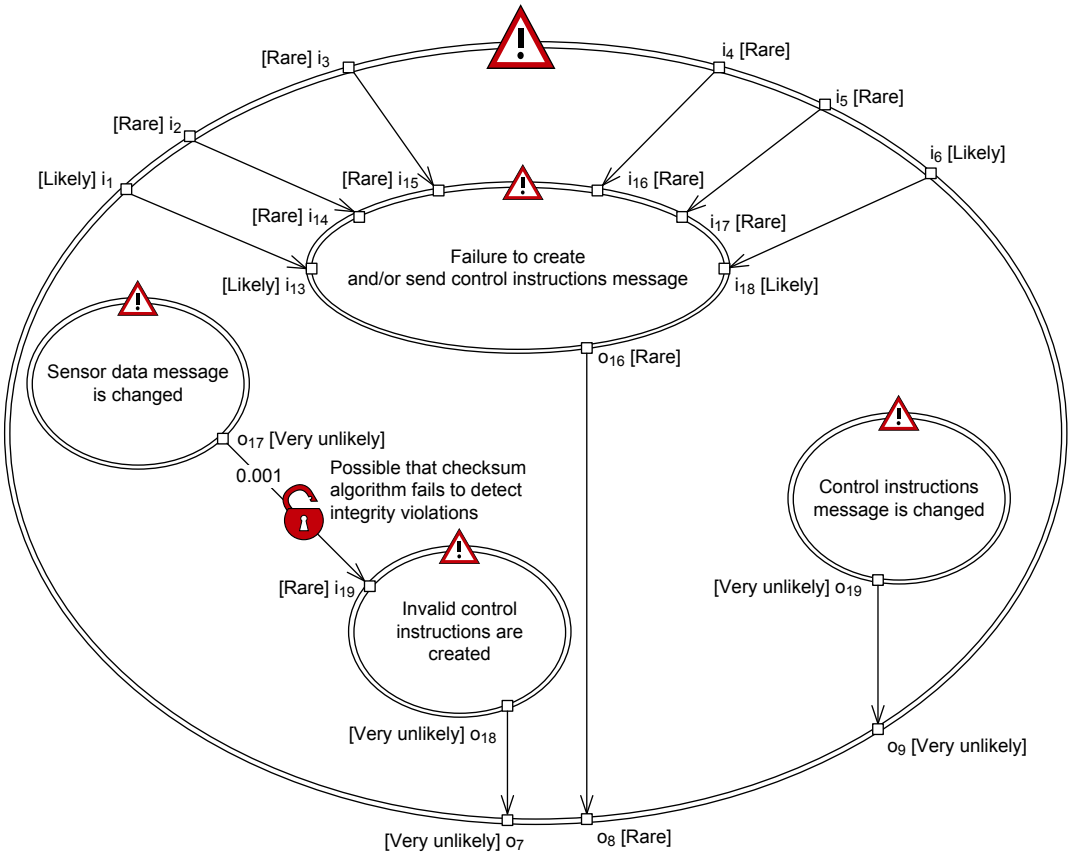


Figure 51: The referenced threat scenario "BPS-CS electricity service is not delivered according to requirements," referred to in Figure 47



PTS-LHPP control instructions service, LHPP-PTS sensor data service, PTS-CS sensor data service, and CS-PTS control instructions service are not delivered according to requirements

Figure 52: The referenced threat scenario "PTS-LHPP control instructions service, LHPP-PTS sensor data service, PTS-CS sensor data service, and CS-PTS control instructions service are not delivered according to requirements," referred to in Figure 47

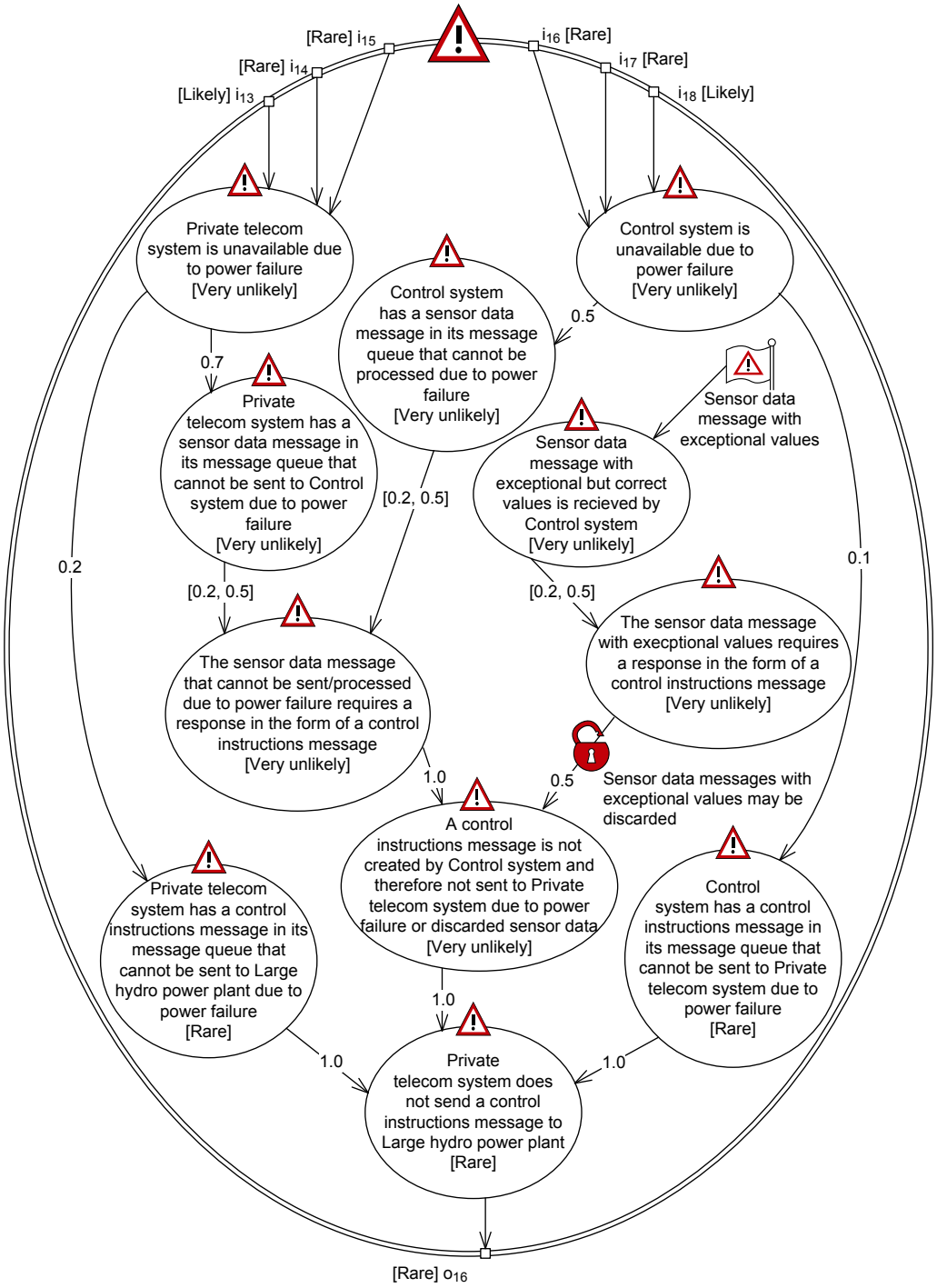


Figure 53: The referenced threat scenario "Failure to create and/or send control instructions message," referred to in Figure 52

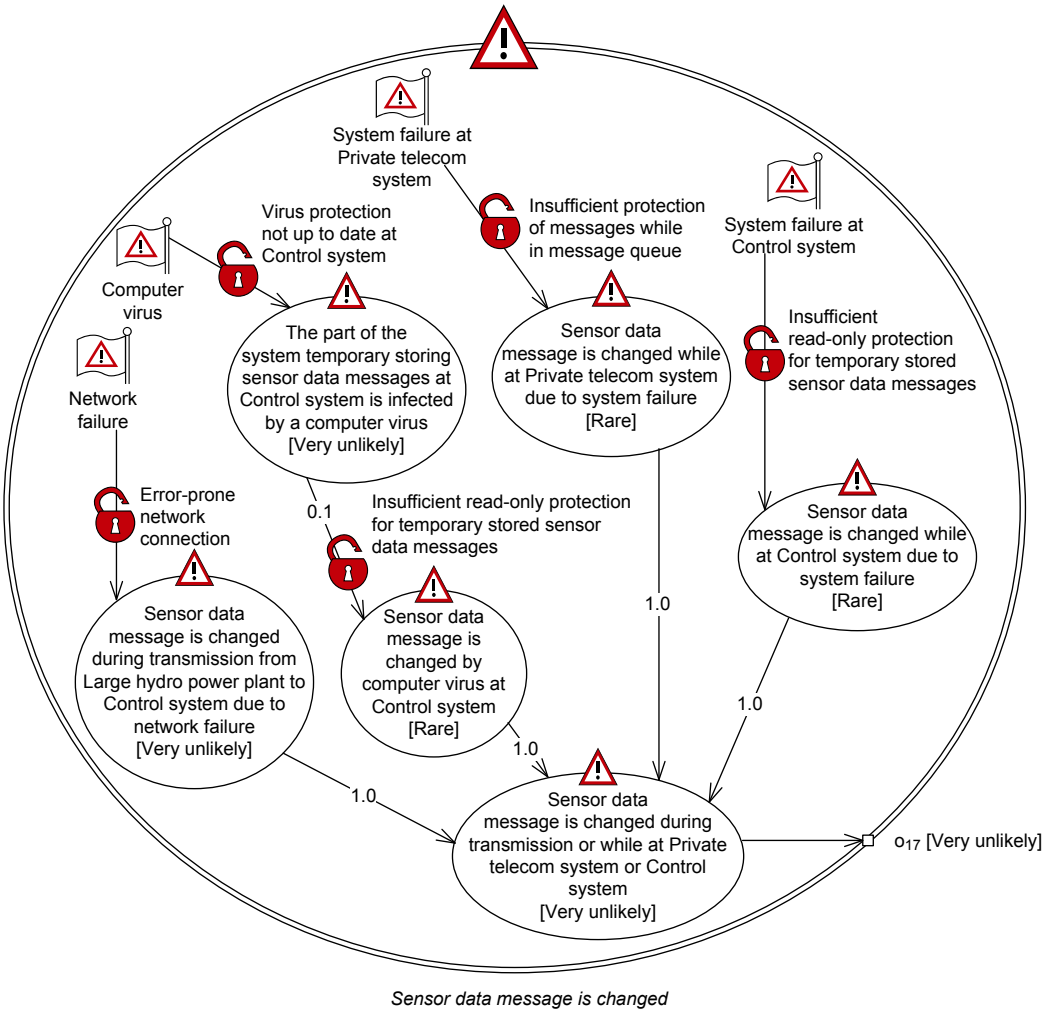


Figure 54: The referenced threat scenario “Sensor data message is changed,” referred to in Figure 52

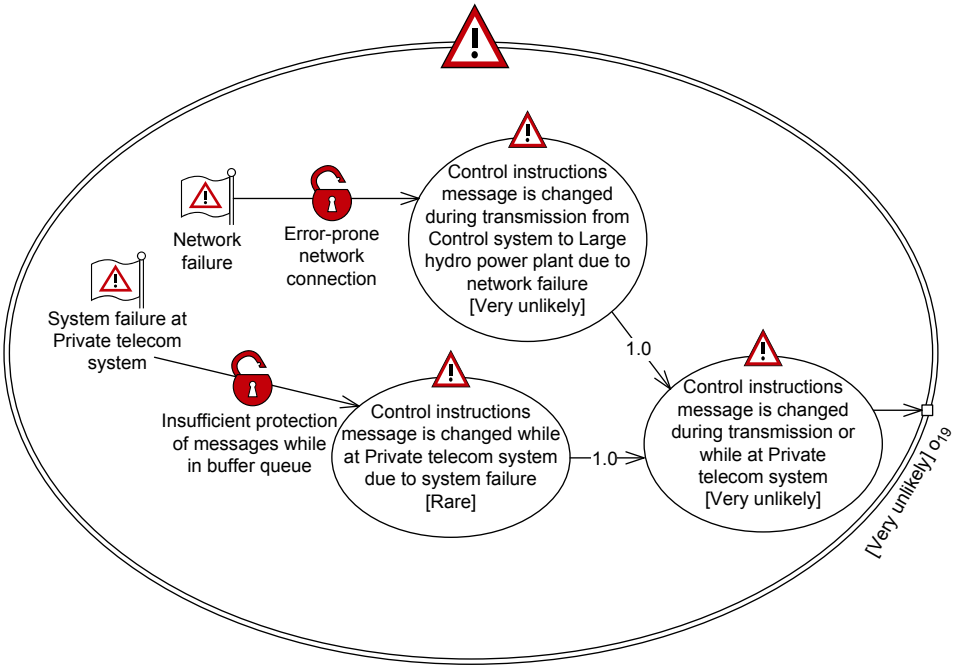


Figure 55: The referenced threat scenario "Control instructions message is changed," referred to in Figure 52

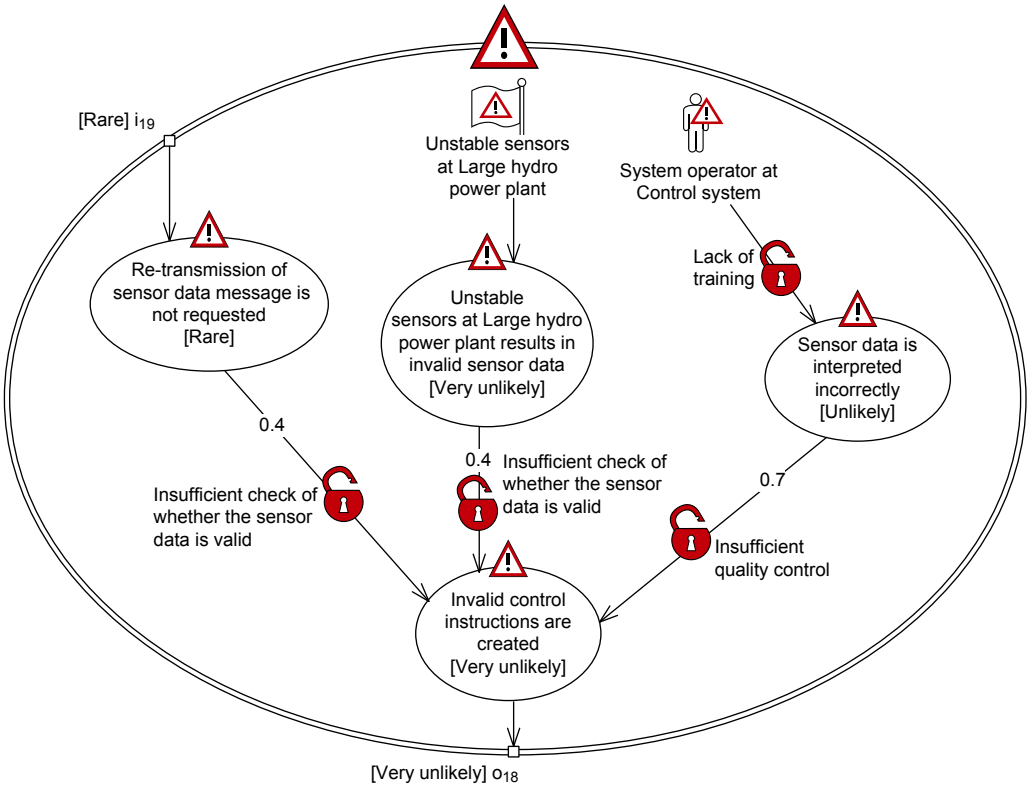


Figure 56: The referenced threat scenario "Incorrect control instructions are created," referred to in Figure 52

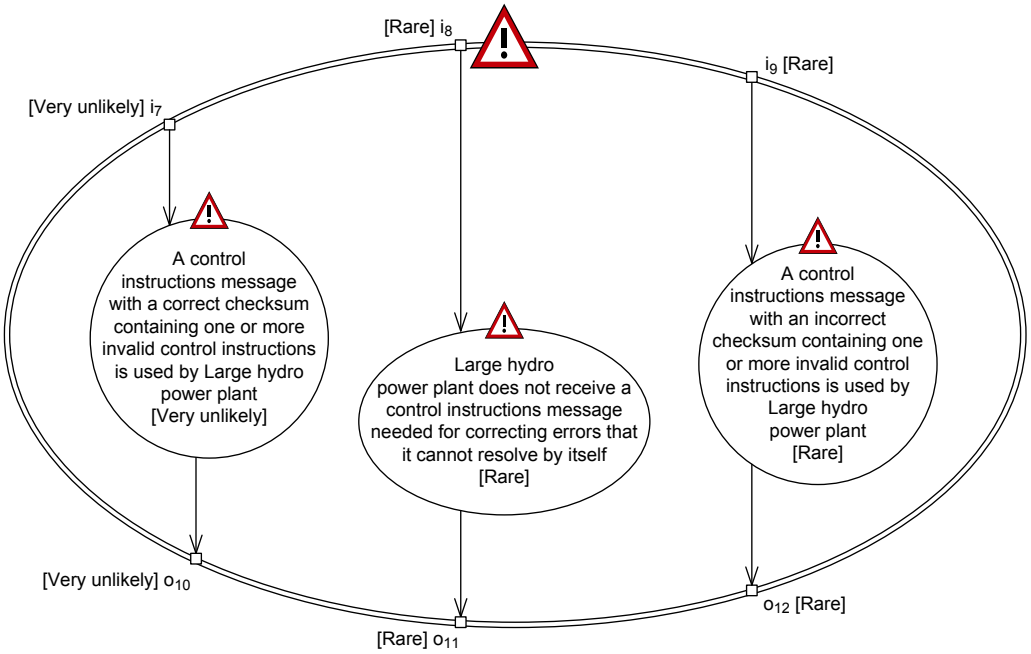


Figure 57: The referenced threat scenario "LHPP-TL electricity service is not delivered according to requirements," referred to in Figure 47

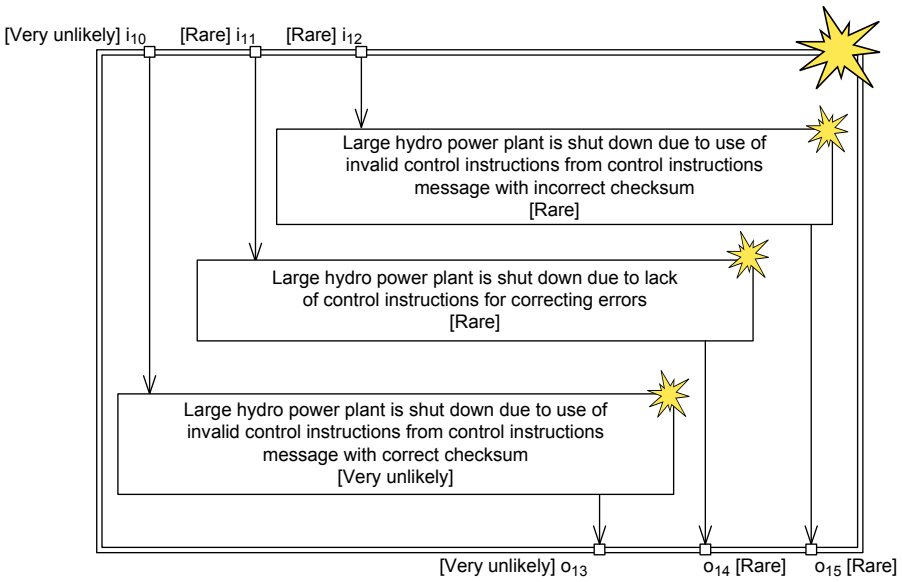


Figure 58: The referenced unwanted incident "Incident with impact on the availability of the electricity service delivered to Transmission," referred to in Figure 47

Figure 58 contains the referenced unwanted incident referred to in Figure 47. For each of the unwanted incidents, Client EPP believes that the "Large hydro power plant" will be shut down for a period of one day each time one of the incidents occurs. With an average production of 1000 kWh ($\frac{365000}{365}$) of electricity each day, the consequence for all incidents with respect to the quality asset is 24 hours and 1000 kWh.

The result of the detailed analysis is three risks. Based on the risk function, defined in Equations (3)–(5) on pages 51 and 52, the maximum service levels *Maximum service level*$_T$ (8760 hours) and *Maximum service level*$_E$ (365 MWh per year), and the two availability requirements specified in the required service level of the electricity service, we can calculate the risk values of the three risks. The risk values are as follows:

- The risk value of "Large hydro power plant is shut down due to use of invalid control instructions from control instructions message with correct checksum" is *Unacceptable* since

  $$Expected\ service\ level_T = [0.9986, 0.9995]$$

  is less than

  $$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

  and since

  $$Expected\ service\ level_E = [0.9986, 0.9995]$$

  is less than

  $$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

- The risk value of "Large hydro power plant is shut down due to lack of control instructions for correcting errors" is *Acceptable* since

  $$Expected\ service\ level_T = [0.9997, 1]$$

  is greater than

  $$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

  and since

  $$Expected\ service\ level_E = [0.9997, 1]$$

  is greater than

  $$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

- The risk value of "Large hydro power plant is shut down due to use of invalid control instructions from control instructions message with incorrect checksum" is *Acceptable* since

  $$Expected\ service\ level_T = [0.9997, 1]$$

  is greater than

  $$\frac{Required\ service\ level_T}{Maximum\ service\ level_T} = [0.999, 0.999]$$

  and since

  $$Expected\ service\ level_E = [0.9997, 1]$$

  is greater than

  $$\frac{Required\ service\ level_E}{Maximum\ service\ level_E} = [0.9995, 0.9995]$$

C.4.2 Relevant indicators for risk monitoring

Client EPP believes that the likelihood value used to calculate the risk value of the risk "Large hydro power plant is shut down due to lack of control instructions for correcting errors" may be subject to change. We therefore decide to monitor this risk.

The indicators should be used to monitor likelihood values, since the likelihood value used to calculate the risk value of the risk may be subject to change. Client EPP does not find it feasible to directly monitor the likelihood of the unwanted incident occurring, and has therefore decided to monitor the conditional likelihoods of four leads-to relations in the detailed high-level threat diagram in Figure 47 that affect the likelihood of the unwanted incident occurring. The relevant indicators for the four leads-to relations are presented in Figure 59. In Appendix D.5 we show how to use the conditional likelihoods we now address as well as other factors to monitor the resulting likelihood of the risk identified for monitoring.

One composite indicator c_8, which aggregates the two basic indicators b_{13} and b_{14}, has been identified for two leads-to relations that have the same vulnerability, while another composite indicator c_9, which aggregates the three basic indicators b_{15}, b_{16}, and b_{17}, has been identified for the two other leads-to relations that also have the same vulnerability. c_8 calculates the ratio of

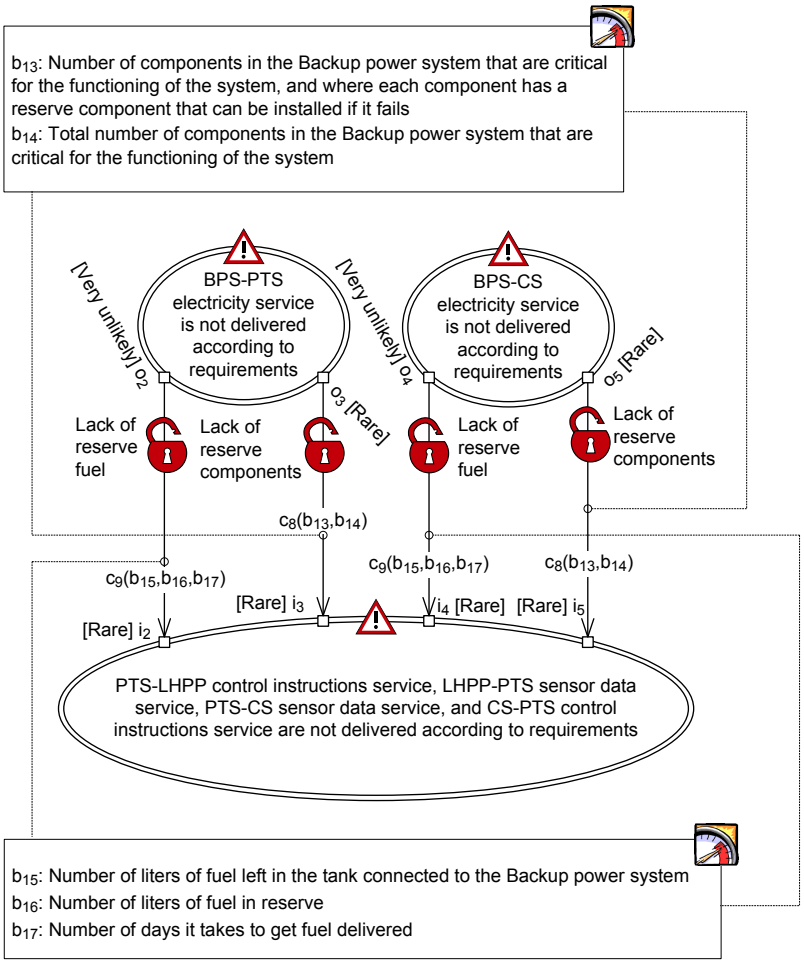


Figure 59: Relevant indicators, assigned to leads-to relations in an excerpt of the detailed high-level threat diagram in Figure 47, for monitoring the risk “Large hydro power plant is shut down due to lack of control instructions for correcting errors”

critical components for which reserve components cannot be installed if the critical components fails to all critical components, while c_9 makes a prediction about the likelihood of the "Backup power system" running out of fuel.

C.4.3 Design and deployment of indicators for risk monitoring

In Figure 59 the composite indicators c_8 and c_9 are both associated with two leads-to relations each. Conditional likelihoods were assigned to these leads-to relations during the detailed analysis described in Appendix C.4.1. We therefore obtain values for the different basic indicators from the time when the detailed high-level threat diagram in Figure 47 was constructed. For b_{13} and b_{14} we obtain the values 15 and 20, respectively, while for b_{15}, b_{16}, and b_{17} we obtain the values 15000, 10000, and 8, respectively.

In Tables 17 and 18 are the design specifications for the different basic and composite indicators with the exception of the basic indicators b_{15}, b_{16}, and b_{17}. These three basic indicators are so simple that no design specifications are needed. All the specifications have been given in the form of algorithms. The three algorithms are to be used by a risk monitor within the electrical power production infrastructure. The indicators are updated every two weeks. Afterwards, the risk picture is updated based on the updated composite indicators.

The composite indicator c_8 aggregates the two indicators b_{13} and b_{14}. Client EPP is of the opinion that c_8 should never be less than 0.1. Thus, if the aggregation of b_{13} and b_{14} results in a value that is less than 0.1, then c_8 is assigned the value 0.1. By using the obtained values for the basic indicators as input to the algorithm we get 0.25, which is close to the initial estimates. It should be noticed that the basic indicator b_{14} will never be equal to zero. Thus, we do not apply any check for this in the design specification in Table 17.

The composite indicator c_9 aggregates the three indicators b_{15}, b_{16}, and b_{17}. The number 20000 used in the algorithm of c_9 is the liters of fuel needed for running the "Backup power system" during disruptions of average length in the electrical power grid. The average length is eight hours. The value 0.1 is assigned to c_9 if there is at least 20000 liters of fuel available. If less than 20000 liters of fuel is available, then the value of c_8 is determined by the delivery time of the fuel. By using the obtained values for the basic indicators as input to the algorithm we get 0.1, which is of course in accordance with the initial estimates.

In Tables 19 and 20 are the deployment specifications for the basic and composite indicators.

Table 17: Design specifications, in the form of algorithms, for the basic indicators b_{13} and b_{14} and the composite indicator c_8

Algorithm for b_{13} and b_{14}

Input: $data_1$: "Data on the components of Backup power system"

Data maintained by the risk monitor: $list_1$: "List of names of components in the Backup power system that are critical for the functioning of the system, and where each component has a reserve component that can be installed if it fails," $list_2$: "List of names of components in the Backup power system that are critical for the functioning of the system"

Based on $data_1$, check whether $list_1$ should be updated. Add names of components to $list_1$, if applicable. Remove names of components from $list_1$, if applicable.

Based on $data_1$, check whether $list_2$ should be updated. Add names of components to $list_2$, if applicable. Remove names of components from $list_2$, if applicable.

b_{13} := "The number of elements in $list_1$"

b_{14} := "The number of elements in $list_2$"

Output: b_{13}, b_{14}

Algorithm for c_8

Input: b_{13}: "Number of components in the Backup power system that are critical for the functioning of the system, and where each component has a reserve component that can be installed if it fails," b_{14}: "Total number of components in the Backup power system that are critical for the functioning of the system"

$c_8 := 1 - \dfrac{b_{13}}{b_{14}}$

if $c_8 < 0.1$ **then**

  $c_8 := 0.1$

end if

Output: c_8

Table 18: Design specification, in the form of an algorithm, for the composite indicator c_9

Algorithm for c_9

Input: b_{15}: "Number of liters of fuel left in the tank connected to the Backup power system," b_{16}: "Number of liters of fuel in reserve," b_{17}: "Number of days it takes to get fuel delivered"
 	
if $b_{15} + b_{16} \geq 20000$ **then**
c_9 := 0.1
else
if $b_{15} + b_{16} < 20000$ **and** $0 < b_{17} \leq 7$ **then**
c_9 := 0.3
else
if $b_{15} + b_{16} < 20000$ **and** $b_{17} > 7$ **then**
c_9 := 0.5
end if
end if
end if
 	
Output: c_9

Table 19: Deployment specification for the basic indicators b_{13} and b_{14} and the composite indicator c_8

Deployment specification for b_{13}**,** b_{14}**, and** c_8
Extraction and transmission of $data_1$**:** Client EPP has a maintenance database that contains information about different components and systems in the infrastructure, including the "Backup power system." Every two weeks, an automated ICT process extracts data for components of the "Backup power system" that the database has been updated with in period of two weeks backwards. It should be noticed that the process will extract all the data that is available for the components the first time it is executed. The process transmits $data_1$ to the risk monitor by the use of the internal data network of the electrical power production infrastructure.

Table 20: Deployment specification for the basic indicators b_{15}, b_{16}, and b_{17} and the composite indicator c_9

Deployment specification for b_{15}, b_{16}, b_{17}, and c_9
Extraction and transmission of b_{15}: A sensor is used to keep track of the number of liters of fuel left in the tank connected to the "Backup power system." The sensor measures the number of liters left at least daily. The measurements are transmitted to the maintenance database of Client EPP. Every two weeks, an automated ICT process extracts the latest measurement from the database. The number extracted is the basic indicator b_{15}. The process transmits b_{15} to the risk monitor by using the internal data network of the electrical power production infrastructure. **Extraction and transmission of b_{16}:** A sensor is used to keep track of the number of liters of fuel left in the tank that stores the reserve fuel of the "Backup power system." The sensor measures the number of liters left at least daily. The measurements are transmitted to the maintenance database of Client EPP. Every two weeks, an automated ICT process extracts the latest measurement from the database. The number extracted is the basic indicator b_{16}. The process transmits b_{16} to the risk monitor by using the internal data network of the electrical power production infrastructure. **Extraction and transmission of b_{17}:** Every two weeks an employee of Client EPP obtains the expected delivery time in days for fuel from the company delivering fuel to Client EPP. The number obtained is the basic indicator b_{17}. The employee updates the maintenance database with this number. After the database has been updated, an automated ICT process extracts b_{17} and transmits it to the risk monitor by using the internal data network of the electrical power production infrastructure.

D Monitor risk values based on identified indicators

In this appendix we show how to monitor risk values for provided services based on the indicators identified in Section 6 and Appendix C. The risk values are monitored only indirectly via monitored likelihood and consequence values.

The rest of the appendix is structured as follows: in Appendix D.1 we present rules for calculating likelihoods, while in Appendices D.2–D.5 we show how to monitor risk values for the five provided services. Appendix D.4 covers both of the electricity services provided by "Small hydro power plant" because the monitoring of their risk values are identical[1].

In Appendices D.2–D.5 we present CORAS diagrams based on the CORAS diagrams presented in Section 5 and Appendices C.1.1, C.2.1, and C.4.1. The CORAS diagrams in Appendices D.2–D.5 contain only the fragments that are necessary for calculating frequencies of risks. The fragments have been assigned some additional conditional likelihoods that were left out earlier to keep things simple. We have also included a shorthand notation in the description of each threat scenario (TS) and unwanted incident (UI) to make it easier to refer to them during the likelihood calculation.

D.1 Likelihood calculation rules

To reason about likelihoods, we use the likelihood calculation rules defined in [7]. In Appendices D.2–D.5, all the likelihoods assigned to threat scenarios, unwanted incidents, or gates are given in the form of frequencies, while conditional likelihoods assigned to leads-to relations are given in the form of probabilities. Furthermore, the frequencies are given in the form of intervals with respect to a period of one year. This period for calculating risk values has been chosen since the two risk functions (defined in Equations (1) and (2) on page 32 and in Equations (3)–(5) on pages 51 and 52) use values that are given for the period of one year.

As can be seen in Table 1 on page 31, the maximum value of the likelihood scale is the frequency interval "Certain" ($[50, \infty\rangle : 1$ year). Thus, a "certain" event has 50 times per year, i.e., almost one time per week, as its lower frequency threshold, while it has ∞ times per year as its upper frequency threshold. To make use of this frequency interval in a practical setting, e.g., to calculate risk values, we need to replace ∞ with a more reasonable value. Client EPP is of the opinion that the events of relevance (i.e., those that have been identified in the risk analysis) never occur more than 100 times per year. We therefore decide that ∞ should be replaced by 100 times per year, i.e., almost two times a week. Thus, in the remainder of this report, "Certain" will equal $[50, 100] : 1$ year.

In the likelihood calculations, we use the rules for interval arithmetic defined in Section 5.3. In addition, we use rules for determining the minimum and maximum value of two closed intervals. For two intervals $[a, b]$ and $[c, d]$, where both are subsets of the positive real line $\mathbb{R}^+$, we use the following rules to calculate the minimum and maximum value:

- **Minimum value:** $min([a, b], [c, d]) = min(a, c)$
- **Maximum value:** $max([a, b], [c, d]) = max(b, d)$

Notice that in addition to calculating the minimum and maximum value of two intervals, we also calculate the minimum and maximum value of two positive real numbers and single intervals in this appendix. In those cases, normal rules for minimum and maximum value calculation apply.

In the following we present rules for calculating and reasoning about frequencies in CORAS diagrams. First we present two rules from [7] for calculating and reasoning about exact frequencies. Afterwards we present three rules that apply to frequency intervals. The examples in Figure

[1] See Appendix C.3 for more information.

60 are used during the presentation to explain the rules. The rules are given on the following form:

$$\frac{P_1 \quad P_2 \quad \ldots \quad P_n}{C}$$

We refer to $P_1, \ldots, P_n$ as the premises and to C as the conclusion. The interpretation is that if the premises are valid, so is the conclusion.

Rule 1 (Leads-to) For the scenarios/incidents e_1 and e_2 related by the leads-to relation, we have:

$$\frac{e_1(f) \quad e_1 \xrightarrow{l} e_2}{(e_1 \sqcap\!| \, e_2)(f \cdot l)}$$

The leads-to rule captures the conditional likelihood semantics embedded in the leads-to relation. The frequency of the occurrences of the scenario/incident e_2 that are due to the scenario/incident e_1 is equal to the frequency f of e_1 multiplied with the conditional likelihood l that e_1 will lead to e_2 given that e_1 occurs. $e_1 \sqcap\!| \, e_2$ is to be understood as the subset of the scenarios/incidents e_2 that are preceded by e_1.

We let f_1 and p_1 in Figure 60 be equal to $3 : 1$ year and 0.3, respectively. Recall that we only use probabilities for conditional likelihoods. We calculate the frequency of $e_1 \sqcap\!| \, e_2$ as follows:

$$f_{e_1 \sqcap\!| \, e_2} = f_1 \cdot p_1 = 3 \cdot 0.3 = 0.9$$

The frequency of $e_1 \sqcap\!| \, e_2$ occurring is approximately 1 time per year. Notice that $f_{e_1 \sqcap\!| \, e_2}$ is equal to f_2 if e_1 is the only scenario that can lead to e_2.

Rule 2 (Separate scenarios/incidents) If the scenarios/incidents e_1 and e_2 are separate, we have:

$$\frac{e_1(f_1) \quad e_2(f_2)}{(e_1 \sqcup e_2)(f_1 + f_2)}$$

Two scenarios/incidents e_1 and e_2 are separate if they do not overlap in content. If this is the case, then neither of the two scenarios/incidents is an instance of the other. It also means that one scenario/incident cannot be a special case of the other. For instance, if e_1 is the scenario "Virus

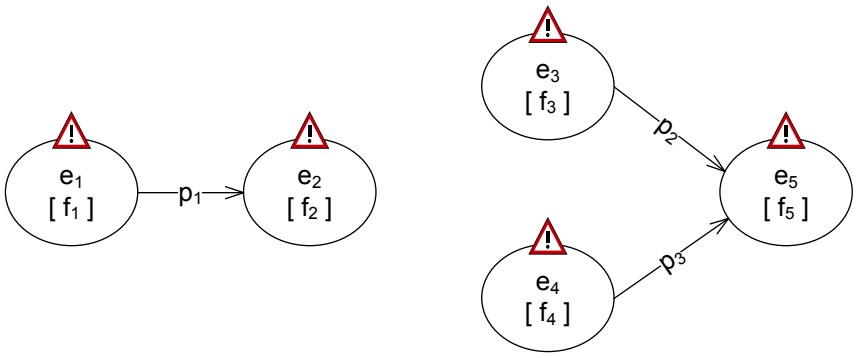


Figure 60: Examples used for explaining the rules for calculating and reasoning about frequencies

infects computer," while e_2 is the scenario "Malware infects computer," then e_1 is a special case of e_2 and the two scenarios overlap in content.

Lets assume that $e_3 \sqcap\!| \, e_5$ and $e_4 \sqcap\!| \, e_5$ in Figure 60 are separate. Moreover, we let f_3 and p_2 be equal to $3 : 1$ year and 0.9, respectively, while we let f_4 and p_3 be equal to $4 : 1$ year and 0.6, respectively. We then calculate the frequency of $(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)$ as follows:

$$\begin{aligned} f_{(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)} &= f_{e_3 \sqcap\!| \, e_5} + f_{e_4 \sqcap\!| \, e_5} \\ &= (f_3 \cdot p_2) + (f_4 \cdot p_3) = (3 \cdot 0.9) + (4 \cdot 0.6) \\ &= 2.7 + 2.4 = 5.1 \end{aligned}$$

The frequency of $(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)$ occurring is approximately 5 times per year. Notice that $f_{(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)}$ is equal to f_5 if e_3 and e_4 are the only scenarios that can lead to e_5.

Rule 3 (Leads-to – frequency interval) For the scenarios/incidents e_1 and e_2 related by the leads-to relation, we have:

$$\frac{e_1([f_a, f_b]) \quad e_1 \xrightarrow{[l_a, l_b]} e_2}{(e_1 \sqcap\!| \, e_2)([f_a \cdot l_a, f_b \cdot l_b]}$$

The rule above is a generalization of **Rule 1** to frequency intervals.

We let f_1 and p_1 in Figure 60 be equal to $[0.6, 1.9] : 1$ year ("Unlikely") and $[0.1, 0.3]$, respectively. Moreover, we let $f_{e_1 \sqcap\!| \, e_2}$ be the frequency of $e_1 \sqcap\!| \, e_2$. We then have:

$$f_{e_1 \sqcap\!| \, e_2} = f_1 \cdot p_1 = [0.6, 1.9] \cdot [0.1, 0.3] = [0.06, 0.57]$$

The frequency of $e_1 \sqcap\!| \, e_2$ is $[0.06, 0.57] : 1$ year.

Rule 4 (Separate scenarios/incidents – frequency interval) If the scenarios/incidents e_1 and e_2 are separate, we have:

$$\frac{e_1([f_a, f_b]) \quad e_2([f_c, f_d])}{(e_1 \sqcup e_2)([f_a + f_c, f_b + f_d])}$$

The rule above is a generalization of **Rule 2** to frequency intervals.

Lets assume that $e_3 \sqcap\!| \, e_5$ and $e_4 \sqcap\!| \, e_5$ in Figure 60 are separate. Moreover, we let f_3 and p_2 be equal to $[0, 0.1] : 1$ year ("Rare") and 0.9, respectively, while we let f_4 and p_3 be equal to $[0.2, 0.5] : 1$ year ("Very unlikely") and 0.6, respectively. We then calculate the frequency of $(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)$ as follows:

$$\begin{aligned} f_{(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)} &= f_{e_3 \sqcap\!| \, e_5} + f_{e_4 \sqcap\!| \, e_5} \\ &= (f_3 \cdot p_2) + (f_4 \cdot p_3) = ([0, 0.1] \cdot 0.9) + ([0.2, 0.5] \cdot 0.6) \\ &= [0, 0.09] + [0.12, 0.3] = [0.12, 0.39] \end{aligned}$$

The frequency of $(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)$ is $[0.12, 0.39] : 1$ year.

Rule 5 (General – frequency interval) For two scenarios/incidents e_1 and e_2, we have:

$$\frac{e_1([f_a, f_b]) \quad e_2([f_c, f_d])}{(e_1 \sqcup e_2)([max(f_a, f_c), f_b + f_d])}$$

The rule above is the general rule for calculating with frequency intervals. We can for instance use this rule if two scenarios/incidents are not separate.

Lets assume that $e_3 \sqcap\!| \, e_5$ and $e_4 \sqcap\!| \, e_5$ in Figure 60 are not separate. Moreover, we let f_3 and p_2 be equal to $[5, 9.9] : 1$ year ("Likely") and 0.4, respectively, while we let f_4 and p_3 be equal to $[2, 4.9] : 1$ year ("Possible") and 0.7, respectively. We first calculate the frequencies of $e_3 \sqcap\!| \, e_5$ and $e_4 \sqcap\!| \, e_5$ as follows:

$$f_{e_3 \sqcap\!| \, e_5} = f_3 \cdot p_2 = [5, 9.9] \cdot 0.4 = [2, 3.96]$$
$$f_{e_4 \sqcap\!| \, e_5} = f_4 \cdot p_3 = [2, 4.9] \cdot 0.7 = [1.4, 3.43]$$

To calculate the minimum frequency value f_{min} and the maximum frequency value f_{max} of $(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)$ we do as follows:

$$\begin{aligned} f_{min} &= max(min(f_{e_3 \sqcap\!| \, e_5}), min(f_{e_4 \sqcap\!| \, e_5})) \\ &= max(min([2, 3.96]), min([1.4, 3.43])) = max(2, 1.4) = 2 \\ f_{max} &= max(f_{e_3 \sqcap\!| \, e_5}) + max(f_{e_4 \sqcap\!| \, e_5}) \\ &= max([2, 3.96]) + max([1.4, 3.43]) = 3.96 + 3.43 = 7.39 \end{aligned}$$

The frequency of $(e_3 \sqcap\!| \, e_5) \sqcup (e_4 \sqcap\!| \, e_5)$ is $[2, 7.39] : 1$ year.

D.2 Sensor data service provided to Public telecom system

The risk values of the risks "Incorrect sensor data is sent to Public telecom system due to sensors being infected with a computer virus" and "Sensor data is sent in plain text from Small hydro power plant to an outsider" are indirectly monitored based on two conditional likelihoods. The two likelihoods are monitored by the use of the composite indicators c_1 and c_2 in Figure 21 on page 43. The two conditional likelihoods are assigned to two leads-to relations. The two likelihoods can be used to calculate frequencies assigned to vertices that the two leads-to relations lead up to, including the frequencies of the two risks.

In Figures 61 and 62, we have replaced the frequencies to be calculated, based on the composite indicators, with variables. The two figures contain CORAS diagrams that are based on different CORAS diagrams in Section 5. We assume that the CORAS diagrams in the two figures are based on complete CORAS diagrams. This means that no other threat scenarios or unwanted incidents than the ones specified in Figures 61 and 62 can lead to other threat scenarios, unwanted incidents, or out-gates. Based on this assumption we can for instance state that $f_2 = f_{TS1 \ \sqcap\!| \ TS2}$, where $f_{TS1 \ \sqcap\!| \ TS2}$ is the frequency of $TS1 \sqcap\!| \, TS2$. In other words, $TS1$ is the only threat scenario that can lead to $TS2$.

As can be seen in the figures, some of the variables have been used for a number of frequencies. The same variable is assigned to all frequencies that should be equal. For instance, the out-gate o_{19} in Figure 62 has been assigned the frequency variable f_1 of the threat scenario "Small hydro power plant's sensors are infected with a computer virus," since the threat scenario leads to the out-gate with the conditional likelihood 1.0, and since $f_1 \cdot 1.0 = f_1$ (**Rule 3**).

To monitor the risk value of the risk "Incorrect sensor data is sent to Public telecom system due to sensors being infected with a computer virus," we start by calculating the frequency f_1 of the threat scenario $TS3$ in Figure 62. We calculate this frequency as follows:

$$\begin{aligned} f_1 &= f_{TS1 \ \sqcap\!| \ TS3} \\ &= [0.6, 1.9] \cdot c_1 \text{ (**Rule 3**)} \\ &= [0.6 \cdot c_1, 1.9 \cdot c_1] \end{aligned}$$

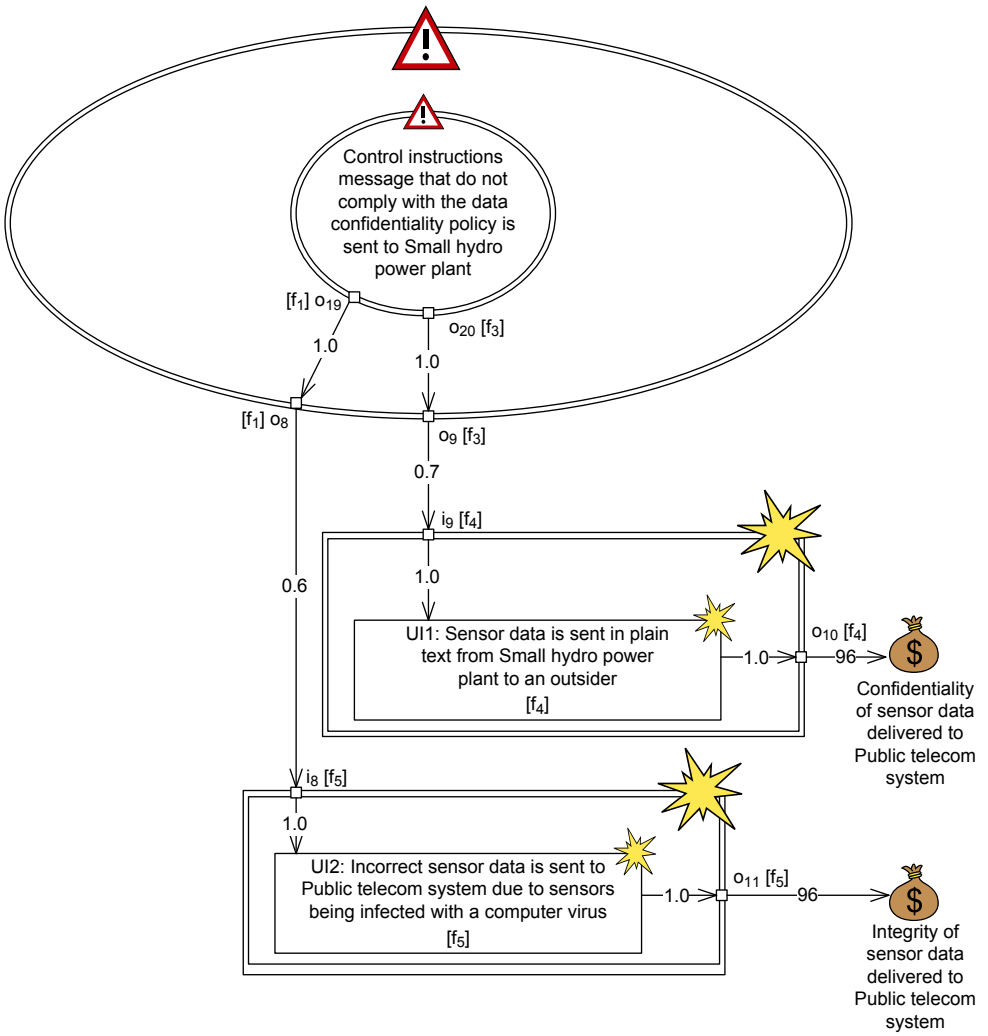


Figure 61: CORAS diagram based on CORAS diagrams in Figures 14, 16, and 20 on pages 33, 36, and 39, respectively

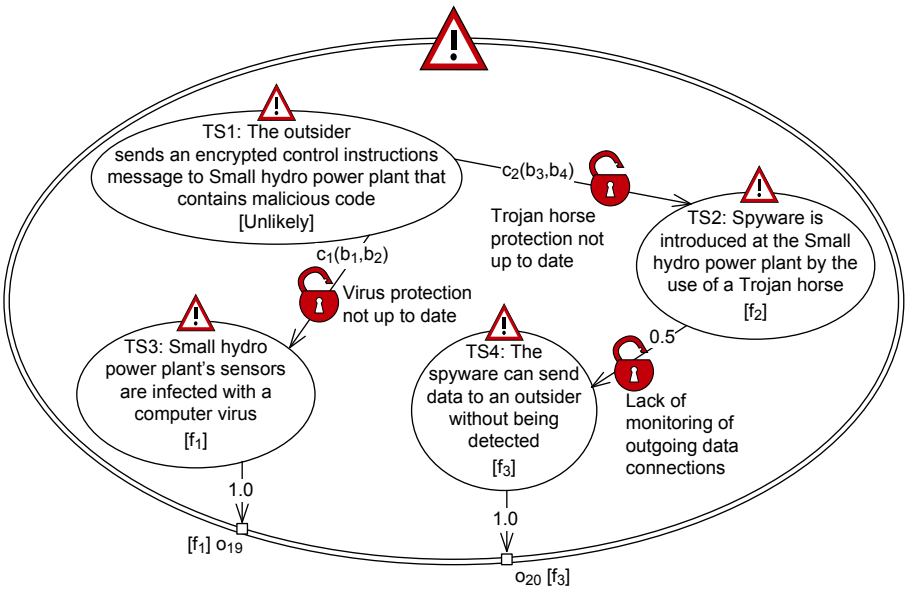


Figure 62: CORAS diagram based on the CORAS diagram in Figure 19 on page 38

Notice that the frequency "Unlikely" is given for the period of one year, and that **Rule 3** is used to calculate f_1. Based on this frequency, we can calculate the frequency f_5 of the unwanted incident $UI2$ in Figure 61 occurring. We calculate the frequency as follows:

$$
\begin{aligned}
f_5 &= f_{TS3 \sqcap\!| \ UI2} \\
&= f_1 \cdot 0.6 \text{ (\textbf{Rule 3})} \\
&= [0.6 \cdot c_1, 1.9 \cdot c_1] \cdot 0.6 = [0.36 \cdot c_1, 1.14 \cdot c_1]
\end{aligned}
$$

We continue by calculating the *Expected service level*. We calculate it as follows:

$$
\begin{aligned}
\textit{Expected service level} &= \frac{\textit{Maximum service level} - (\textit{Likelihood} \cdot \textit{Consequence})}{\textit{Maximum service level}} \\
&= \frac{5000 - (f_5 \cdot 96)}{5000} \\
&= \frac{5000 - ([0.36 \cdot c_1, 1.14 \cdot c_1] \cdot 96)}{5000} \\
&= \frac{5000 - [34.56 \cdot c_1, 109.44 \cdot c_1]}{5000}
\end{aligned}
$$

The final step is to define how *Risk Value* should be calculated. We calculate it as follows:

if $\dfrac{5000 - [34.56 \cdot c_1, 109.44 \cdot c_1]}{5000} \geq \dfrac{5000 \cdot 0.999}{5000}$ **then**

$\quad \textit{Risk value} = \textit{Acceptable}$

else

$\quad \textit{Risk value} = \textit{Unacceptable}$

endif

To monitor the risk value of the risk "Sensor data is sent in plain text from Small hydro power plant to an outsider," we start by calculating the frequency f_2 of the threat scenario $TS2$

in Figure 62. We calculate this frequency as follows:

$$\begin{aligned} f_2 &= f_{TS1} \sqcap\!| \ _{TS2} \\ &= [0.6, 1.9] \cdot c_2 \textbf{ (Rule 3)} \\ &= [0.6 \cdot c_2, 1.9 \cdot c_2] \end{aligned}$$

The threat scenario $TS2$ leads to $TS4$ in the same figure. We calculate the frequency of $TS4$ as follows:

$$\begin{aligned} f_3 &= f_{TS2} \sqcap\!| \ _{TS4} \\ &= f_2 \cdot 0.5 \textbf{ (Rule 3)} \\ &= [0.6 \cdot c_2, 1.9 \cdot c_2] \cdot 0.5 = [0.3 \cdot c_2, 0.95 \cdot c_2] \end{aligned}$$

Based on this frequency, we can calculate the frequency f_4 of the unwanted incident $UI1$ in Figure 61 occurring. We calculate the frequency as follows:

$$\begin{aligned} f_4 &= f_{TS4} \sqcap\!| \ _{UI1} \\ &= f_3 \cdot 0.7 \textbf{ (Rule 3)} \\ &= [0.3 \cdot c_2, 0.95 \cdot c_2] \cdot 0.7 = [0.21 \cdot c_2, 0.665 \cdot c_2] \end{aligned}$$

We continue by calculating the *Expected service level*. We calculate it as follows:

$$\begin{aligned} \textit{Expected service level} &= \frac{\textit{Maximum service level} - (\textit{Likelihood} \cdot \textit{Consequence})}{\textit{Maximum service level}} \\ &= \frac{5000 - (f_4 \cdot 96)}{5000} \\ &= \frac{5000 - ([0.21 \cdot c_2, 0.665 \cdot c_2] \cdot 96)}{5000} \\ &= \frac{5000 - [20.16 \cdot c_2, 63.84 \cdot c_2]}{5000} \end{aligned}$$

The final step is to define how *Risk Value* should be calculated. We calculate it as follows:

if $\dfrac{5000 - [20.16 \cdot c_2, 63.84 \cdot c_2]}{5000} \geq \dfrac{5000 \cdot 0.995}{5000}$ **then**
  Risk value = Acceptable
else
  Risk value = Unacceptable
endif

D.3 Control instructions service provided to Public telecom system

The risk value of the risk "No control instructions message is sent to Public telecom system due to lack of sensor data or use of invalid sensor data" is indirectly monitored based on three conditional likelihoods. The three likelihoods are monitored by the use of the composite indicators c_3 and c_4 in Figures 34 and 35 on pages 65 and 66, respectively. The three conditional likelihoods are assigned to three leads-to relations. The three likelihoods can be used to calculate frequencies assigned to vertices that the three leads-to relations lead up to, including the frequency of the risk.

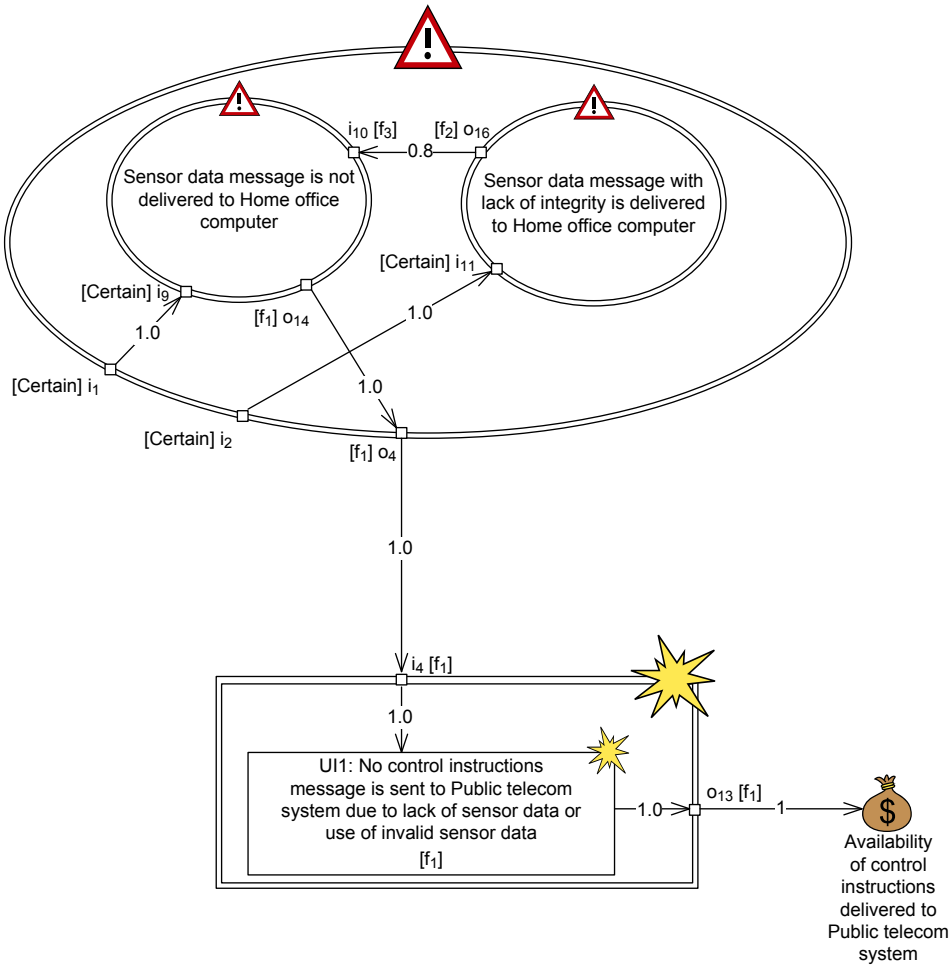


Figure 63: CORAS diagram based on CORAS diagrams in Figures 27, 29, and 33 on pages 58, 60, and 64, respectively

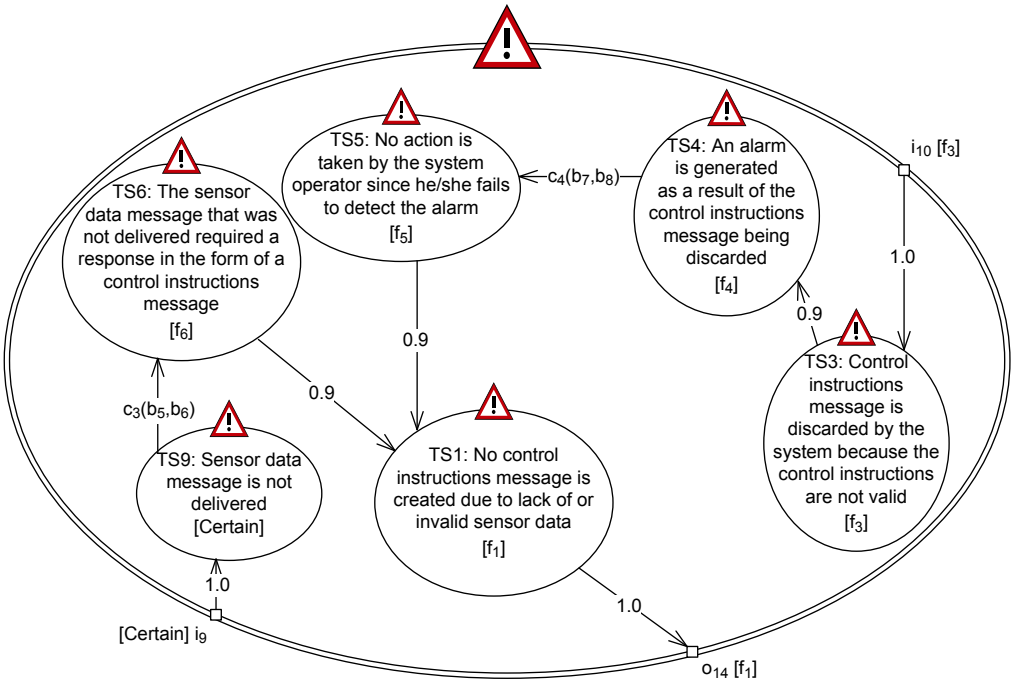


Figure 64: CORAS diagram based on the CORAS diagram in Figure 30 on page 61

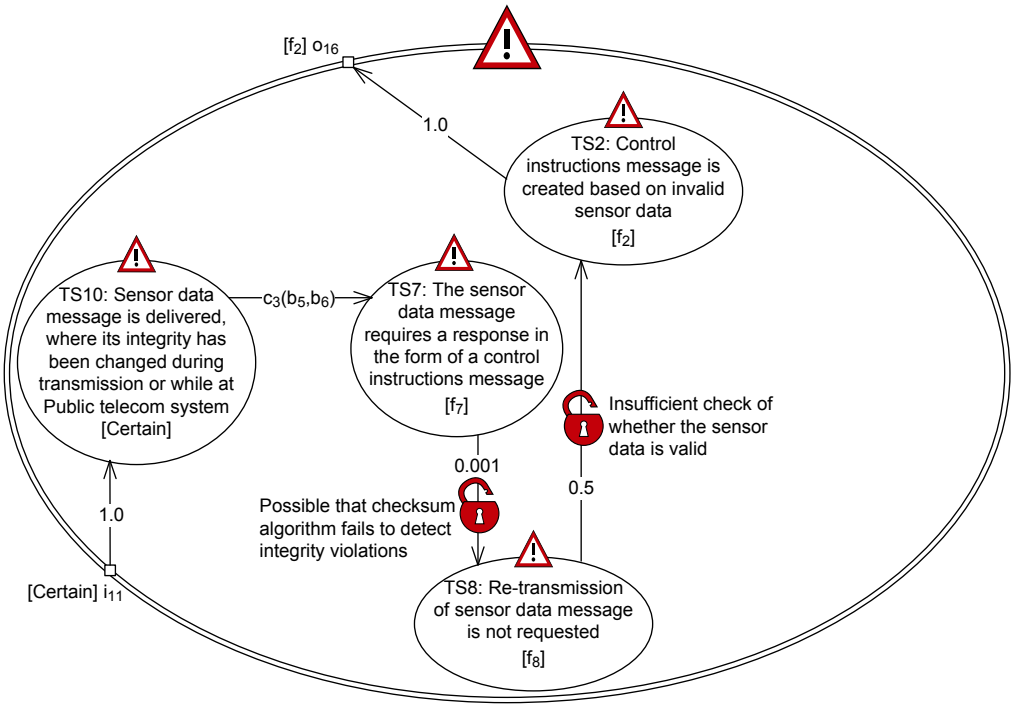


Figure 65: CORAS diagram based on the CORAS diagram in Figure 31 on page 62

In Figures 63–65, we have replaced the frequencies to be calculated, based on the composite indicators, with variables. The three figures contain CORAS diagrams that are based on different CORAS diagrams in Appendix C.1.1. As in Appendix D.2, we assume that the CORAS diagrams in the figures are based on complete CORAS diagrams.

To monitor the risk value of the risk "No control instructions message is sent to Public telecom system due to lack of sensor data or use of invalid sensor data," we need to define how the different frequencies, represented by the variables, should be calculated. We start by showing how this is done for the threat scenarios in Figure 65. As can be seen in Figure 65, the frequency of the threat scenario $TS2$, i.e., f_2, depends on the frequency of $TS8$, i.e., f_8. This frequency depends again on the frequency of $TS7$, i.e., f_7, which again depends on the frequency of $TS10$, i.e., "Certain." We therefore start by calculating f_7. We calculate f_7, f_8, and f_2 as follows:

$$
\begin{aligned}
f_7 &= f_{TS10 \sqcap\!| \ TS7} \\
&= [50, 100] \cdot c_3 \text{ (\textbf{Rule 3})} \\
&= [50 \cdot c_3, 100 \cdot c_3] \\
f_8 &= f_{TS7 \sqcap\!| \ TS8} \\
&= f_7 \cdot 0.001 \text{ (\textbf{Rule 3})} \\
&= [50 \cdot c_3, 100 \cdot c_3] \cdot 0.001 = [0.05 \cdot c_3, 0.1 \cdot c_3] \\
f_2 &= f_{TS8 \sqcap\!| \ TS2} \\
&= f_8 \cdot 0.5 \text{ (\textbf{Rule 3})} \\
&= [0.05 \cdot c_3, 0.1 \cdot c_3] \cdot 0.5 = [0.025 \cdot c_3, 0.05 \cdot c_3]
\end{aligned}
$$

The next step is to calculate the different frequencies of the threat scenarios in Figure 64. Here, f_3 depends on the frequency f_2 and the conditional likelihood 0.8 given in Figure 63, while f_4 depends on f_3. Moreover, f_5 depends on f_4. We therefore start by calculating f_3, before we calculate f_4 and f_5. We calculate the frequencies as follows:

$$
\begin{aligned}
f_3 &= f_{TS2 \sqcap\!| \ TS3} \\
&= f_2 \cdot 0.8 \text{ (\textbf{Rule 3})} \\
&= [0.025 \cdot c_3, 0.05 \cdot c_3] \cdot 0.8 = [0.02 \cdot c_3, 0.04 \cdot c_3] \\
f_4 &= f_{TS3 \sqcap\!| \ TS4} \\
&= f_3 \cdot 0.9 \text{ (\textbf{Rule 3})} \\
&= [0.02 \cdot c_3, 0.04 \cdot c_3] \cdot 0.9 = [0.018 \cdot c_3, 0.036 \cdot c_3] \\
f_5 &= f_{TS4 \sqcap\!| \ TS5} \\
&= f_4 \cdot c_4 \text{ (\textbf{Rule 3})} \\
&= [0.018 \cdot c_3, 0.036 \cdot c_3] \cdot c_4 = [0.018 \cdot c_3 \cdot c_4, 0.036 \cdot c_3 \cdot c_4]
\end{aligned}
$$

As can be seen in Figure 64, the frequency of the threat scenario $TS1$ depends on the frequencies of $TS5 \sqcap\!| \ TS1$ and $TS6 \sqcap\!| \ TS1$. We use **Rule 4** to calculate the frequency f_1, since $TS5 \sqcap\!| \ TS1$ and $TS6 \sqcap\!| \ TS1$ are separate. Before we calculate f_1, we calculate the frequencies of $TS9 \sqcap\!| \ TS6$, i.e., f_6, $TS5 \sqcap\!| \ TS1$, and $TS6 \sqcap\!| \ TS1$. We calculate the frequencies as

follows:

$$
\begin{aligned}
f_6 &= f_{TS9 \sqcap\!| \ TS6} \\
&= [50, 100] \cdot c_3 \text{ (\textbf{Rule 3})} \\
&= [50 \cdot c_3, 100 \cdot c_3] \\
f_{TS5 \sqcap\!| \ TS1} &= f_5 \cdot 0.9 \text{ (\textbf{Rule 3})} \\
&= [0.018 \cdot c_3 \cdot c_4, 0.036 \cdot c_3 \cdot c_4] \cdot 0.9 \\
&= [0.0162 \cdot c_3 \cdot c_4, 0.0324 \cdot c_3 \cdot c_4] \\
f_{TS6 \sqcap\!| \ TS1} &= f_6 \cdot 0.9 \text{ (\textbf{Rule 3})} \\
&= [50 \cdot c_3, 100 \cdot c_3] \cdot 0.9 \\
&= [45 \cdot c_3, 90 \cdot c_3] \\
f_1 &= f_{(TS5 \sqcap\!| \ TS1) \sqcup (TS6 \sqcap\!| \ TS1)} \\
&= [min_{f_1}, max_{f_1}] \text{ (\textbf{Rule 4}) where} \\
min_{f_1} &= min(f_{TS5 \sqcap\!| \ TS1}) + min(f_{TS6 \sqcap\!| \ TS1}) \\
&= (0.0162 \cdot c_3 \cdot c_4) + (45 \cdot c_3) \\
max_{f_1} &= max(f_{TS5 \sqcap\!| \ TS1}) + max(f_{TS6 \sqcap\!| \ TS1}) \\
&= (0.0324 \cdot c_3 \cdot c_4) + (90 \cdot c_3)
\end{aligned}
$$

As can be seen in Figure 63, f_1 is also the frequency of $TS1 \sqcap\!| \, UI1$. In other words, f_1 is the frequency of the unwanted incident $UI1$ occurring. We continue by calculating the *Expected service level*. We calculate it as follows:

$$
\begin{aligned}
\textit{Expected service level} &= \frac{\textit{Maximum service level} - (\textit{Likelihood} \cdot \textit{Consequence})}{\textit{Maximum service level}} \\
&= \frac{1000 - (f_1 \cdot 1)}{1000} = \frac{1000 - f_1}{1000}
\end{aligned}
$$

The final step is to define how *Risk Value* should be calculated. We calculate it as follows:

if $\dfrac{1000 - f_1}{1000} \geq \dfrac{1000 \cdot 0.9999}{1000}$ **then**
  $\textit{Risk value} = \textit{Acceptable}$
else
  $\textit{Risk value} = \textit{Unacceptable}$
endif

D.4 Electricity services provided to Distribution line 2 and Distribution line 3

The unwanted incident "Small hydro power plant is shut down due to damage to unstable power generator" is given in both Figures 42 and 46 on pages 77 and 87, respectively. It impacts the two assets "Availability of electricity delivered to Distribution line 2" and "Availability of electricity delivered to Distribution line 3" with the same consequence if it occurs. Thus, the risk values for the two risks are identical. In the following we focus on the monitoring of the risk that impacts "Availability of electricity delivered to Distribution line 2." The monitoring of the other risk is identical.

The risk value of the risk "Small hydro power plant is shut down due to damage to unstable power generator" is indirectly monitored based on one conditional likelihood and one consequence. The conditional likelihood and the consequence are monitored by the use of the

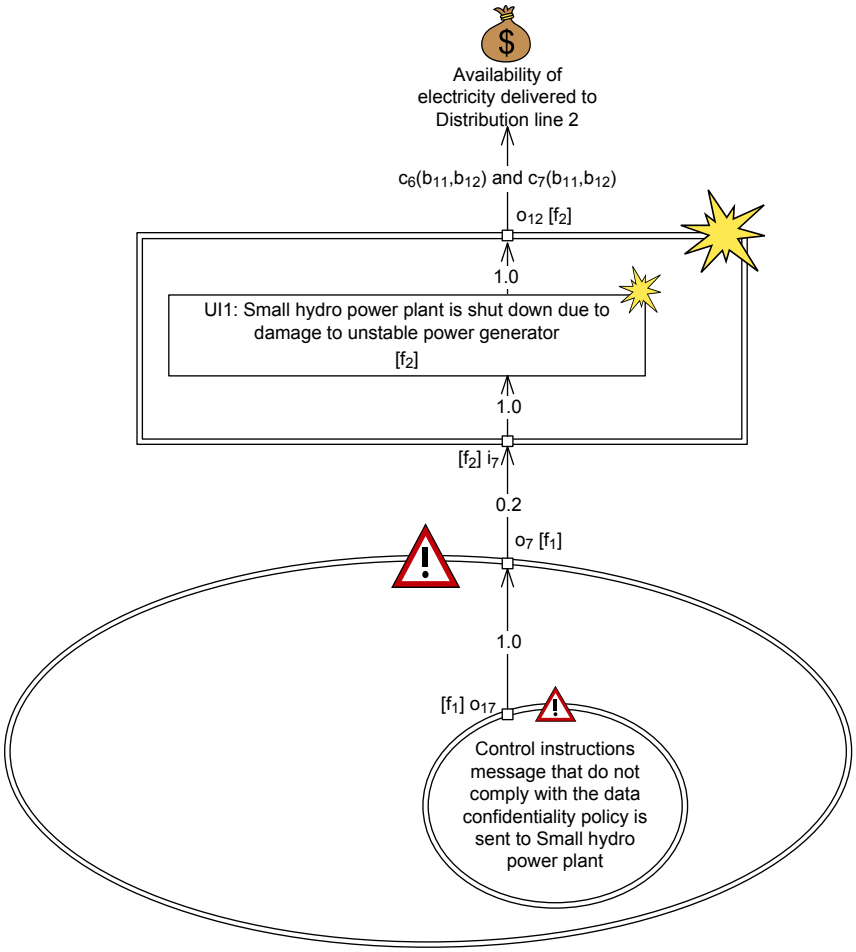


Figure 66: CORAS diagram based on CORAS diagrams in Figures 36, 38, and 42 on pages 72, 74, and 77, respectively

composite indicators c_5, c_6, and c_7 in Figures 43 and 44 on pages 81 and 82, respectively. The conditional likelihood is assigned to a leads-to relation. It can be used to calculate frequencies assigned to vertices that the leads-to relation leads up to, including the frequency of the risk.

In Figures 66 and 67, we have replaced the frequencies to be calculated, based on the composite indicator, with variables. The two figures contain CORAS diagrams that are based on different CORAS diagrams in Appendix C.2.1. As in Appendix D.2, we assume that the CORAS diagrams in the figures are based on complete CORAS diagrams.

To monitor the risk value of the risk "Small hydro power plant is shut down due to damage to unstable power generator," we start by calculating the frequency f_1 of the threat scenario $TS2$ in Figure 67. We calculate this frequency as follows:

$$\begin{aligned} f_1 &= f_{TS1 \sqcap\!| \ TS2} \\ &= [0.6, 1.9] \cdot c_5 \ \textbf{(Rule 3)} \\ &= [0.6 \cdot c_5, 1.9 \cdot c_5] \end{aligned}$$

The next step is to calculate the frequency of the unwanted incident $UI1$ occurring. We calculate

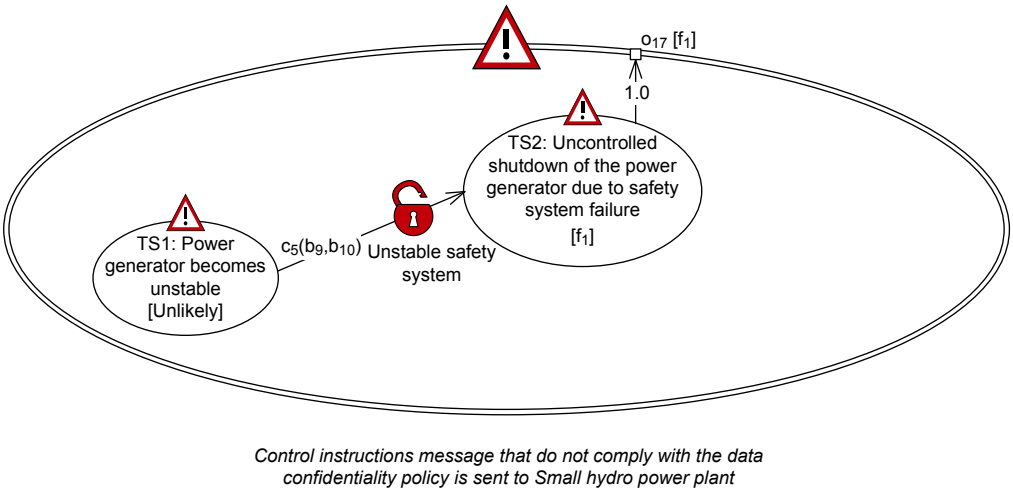


Figure 67: CORAS diagram based on the CORAS diagram in Figure 41 on page 76

this frequency as follows:

$$
\begin{aligned}
f_2 &= f_{TS2 \sqcap\!| \; UI1} \\
&= f_1 \cdot 0.2 \text{ (\textbf{Rule 3})} \\
&= [0.6 \cdot c_5, 1.9 \cdot c_5] \cdot 0.2 = [0.12 \cdot c_5, 0.38 \cdot c_5]
\end{aligned}
$$

We can now calculate *Expected service level*$_T$ and *Expected service level*$_E$. We calculate these as follows:

$$
\begin{aligned}
\textit{Expected service level}_T &= \frac{\textit{Maximum service level}_T - (\textit{Likelihood} \cdot \textit{Consequence}_T)}{\textit{Maximum service level}_T} \\
&= \frac{8760 - (f_2 \cdot c_6)}{8760} \\
&= \frac{8760 - ([0.12 \cdot c_5, 0.38 \cdot c_5] \cdot c_6)}{8760} \\
&= \frac{8760 - [0.12 \cdot c_5 \cdot c_6, 0.38 \cdot c_5 \cdot c_6]}{8760} \\
\textit{Expected service level}_E &= \frac{\textit{Maximum service level}_E - (\textit{Likelihood} \cdot \textit{Consequence}_E)}{\textit{Maximum service level}_E} \\
&= \frac{37000 - (f_2 \cdot c_7)}{37000} \\
&= \frac{37000 - ([0.12 \cdot c_5, 0.38 \cdot c_5] \cdot c_7)}{37000} \\
&= \frac{37000 - [0.12 \cdot c_5 \cdot c_7, 0.38 \cdot c_5 \cdot c_7]}{37000}
\end{aligned}
$$

The composite indicators c_6 (*Consequence*$_T$) and c_7 (*Consequence*$_E$) represent the consequence of the unwanted incident $UI1$ occurring. The final step is to define how *Risk Value* should be

calculated. We calculate *Risk Value* as follows:

$$\textbf{if } \frac{8760 - [0.12 \cdot c_5 \cdot c_6, 0.38 \cdot c_5 \cdot c_6]}{8760} \geq \frac{8760 \cdot 0.999}{8760} \textbf{ and}$$
$$\frac{37000 - [0.12 \cdot c_5 \cdot c_7, 0.38 \cdot c_5 \cdot c_7]}{37000} \geq \frac{36980}{37000} \textbf{ then}$$
$$\mathit{Risk\ value} = \mathit{Acceptable}$$
$$\textbf{else}$$
$$\mathit{Risk\ value} = \mathit{Unacceptable}$$
$$\textbf{endif}$$

D.5 Electricity service provided to Transmission line

The risk value of the risk "Large hydro power plant is shut down due to lack of control instructions for correcting errors" is indirectly monitored based on four conditional likelihoods. The four likelihoods are monitored by the use of the composite indicators c_8 and c_9 in Figure 59 on page 99. The four conditional likelihoods are assigned to four leads-to relations. The four likelihoods can be used to calculate frequencies assigned to vertices that the four leads-to relations lead up to, including the frequency of the risk.

In Figures 68–72, we have replaced the frequencies to be calculated, based on the composite indicators, with variables. The five figures contain CORAS diagrams that are based on different CORAS diagrams in Appendix C.4.1. As in Appendix D.2, we assume that the CORAS diagrams in the figures are based on complete CORAS diagrams. Notice that we let both of the referring threat scenarios "BPS-PTS electricity service is not delivered according to requirements" and "BPS-CS electricity service is not delivered according to requirements" in Figure 68 refer to the referenced threat scenario in Figure 69. We have done this, since the referenced threat scenario is based on the (almost) identical referenced threat scenarios in Figures 50 and 51 on page 91.

To monitor the risk value of the risk "Large hydro power plant is shut down due to lack of control instructions for correcting errors," we need to define how the different frequencies, represented by the variables, should be calculated. We start by showing how this is done for the threat scenarios in Figure 71. The frequency f_6 of the threat scenario $TS5$ depends on the frequencies of $TS1 \sqcap\!| \, TS5$, $TS2 \sqcap\!| \, TS5$, and $TS3 \sqcap\!| \, TS5$. The threat scenarios $TS1$ and $TS2$ are given in Figure 69, while the threat scenario $TS3$ is given in Figure 70. The frequencies of $TS1 \sqcap\!| \, TS5$ and $TS2 \sqcap\!| \, TS5$ are equal to f_1 and f_2, respectively, while the frequency of $TS3 \sqcap\!| \, TS5$ equals the frequency of $TS3$, i.e., "Likely," since $TS3$ and $TS5$ are connected by a path of leads-to relations where each leads-to relations has the conditional likelihood 1.0. To calculate the frequencies of $TS1 \sqcap\!| \, TS5$ and $TS2 \sqcap\!| \, TS5$, we do as follows:

$$\begin{aligned} f_{TS1 \sqcap\!| \, TS5} &= f_1 \\ &= [0.2, 0.5] \cdot c_9 \textbf{ (Rule 3)} \\ &= [0.2 \cdot c_9, 0.5 \cdot c_9] \\ f_{TS2 \sqcap\!| \, TS5} &= f_2 \\ &= [0, 0.1] \cdot c_8 \textbf{ (Rule 3)} \\ &= [0, 0.1 \cdot c_8] \end{aligned}$$

We use the general rule (**Rule 5**) to calculate the frequency f_6, since we do not know whether

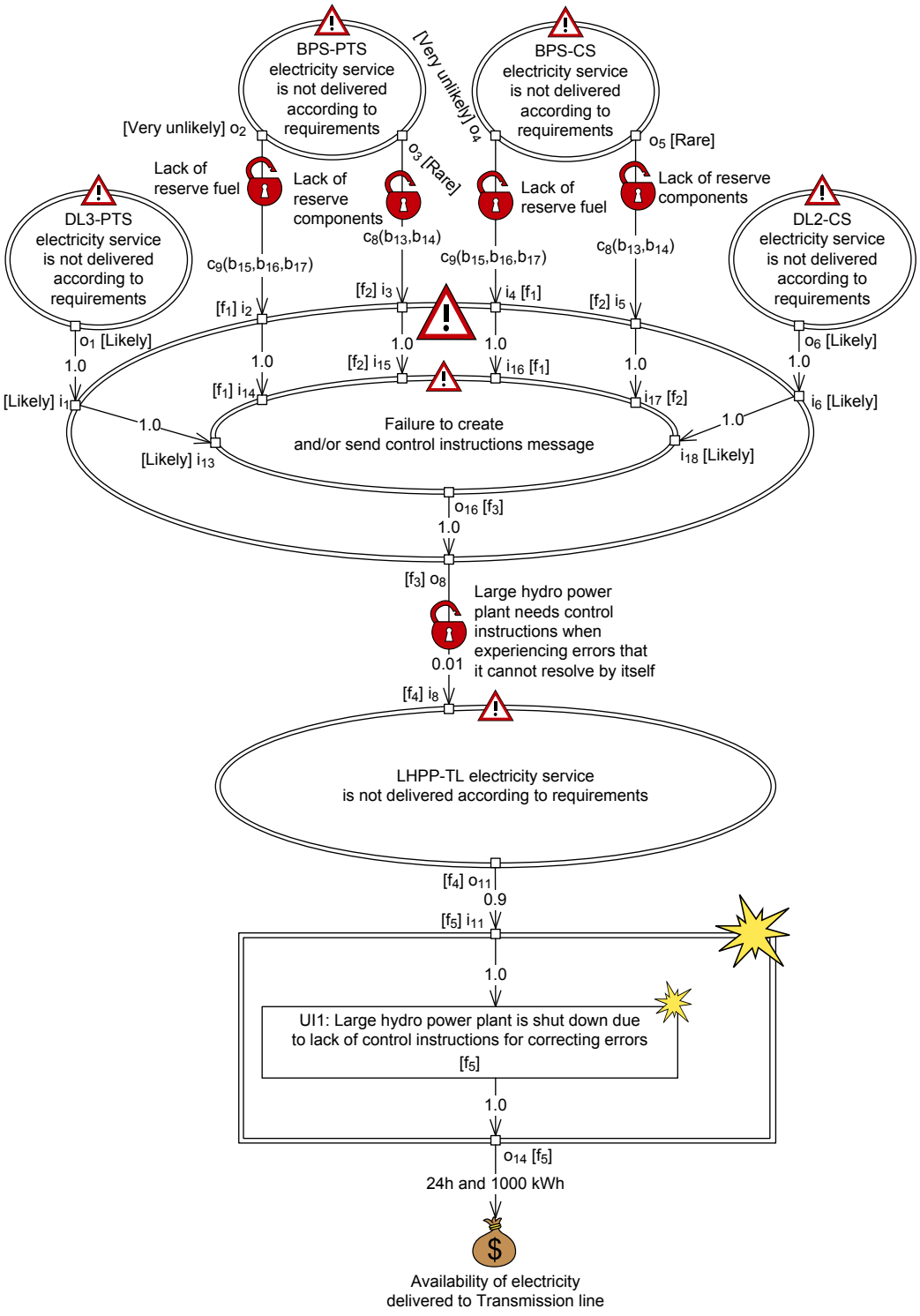
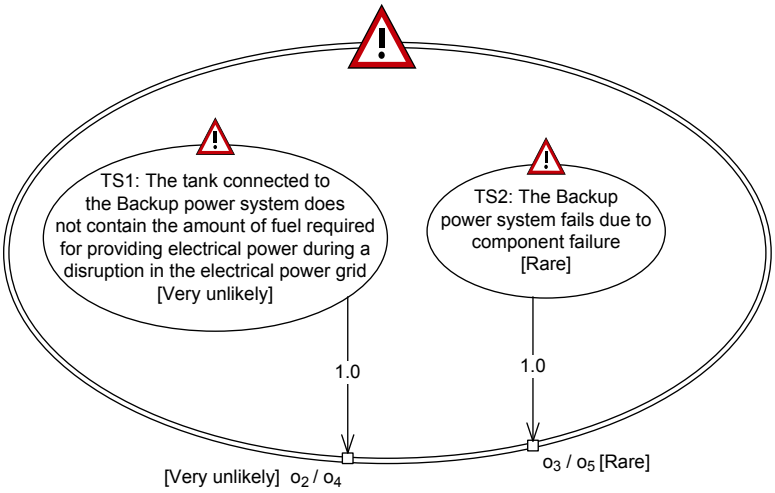
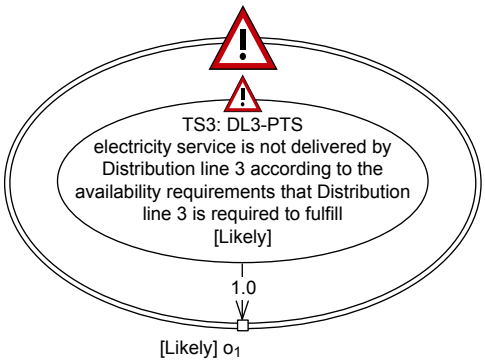


Figure 68: CORAS diagram based on CORAS diagrams in Figures 47, 52, and 58 on pages 88, 92, and 97, respectively

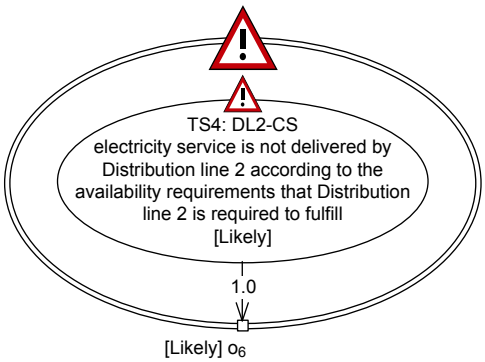


BPS-PTS electricity service is not delivered according to requirements / BPS-CS electricity service is not delivered according to requirements

Figure 69: CORAS diagram based on CORAS diagrams in Figures 50 and 51 on page 91



DL3-PTS electricity service is not delivered according to requirements



DL2-CS electricity service is not delivered according to requirements

Figure 70: CORAS diagrams based on CORAS diagrams in Figures 48 and 49 on page 89

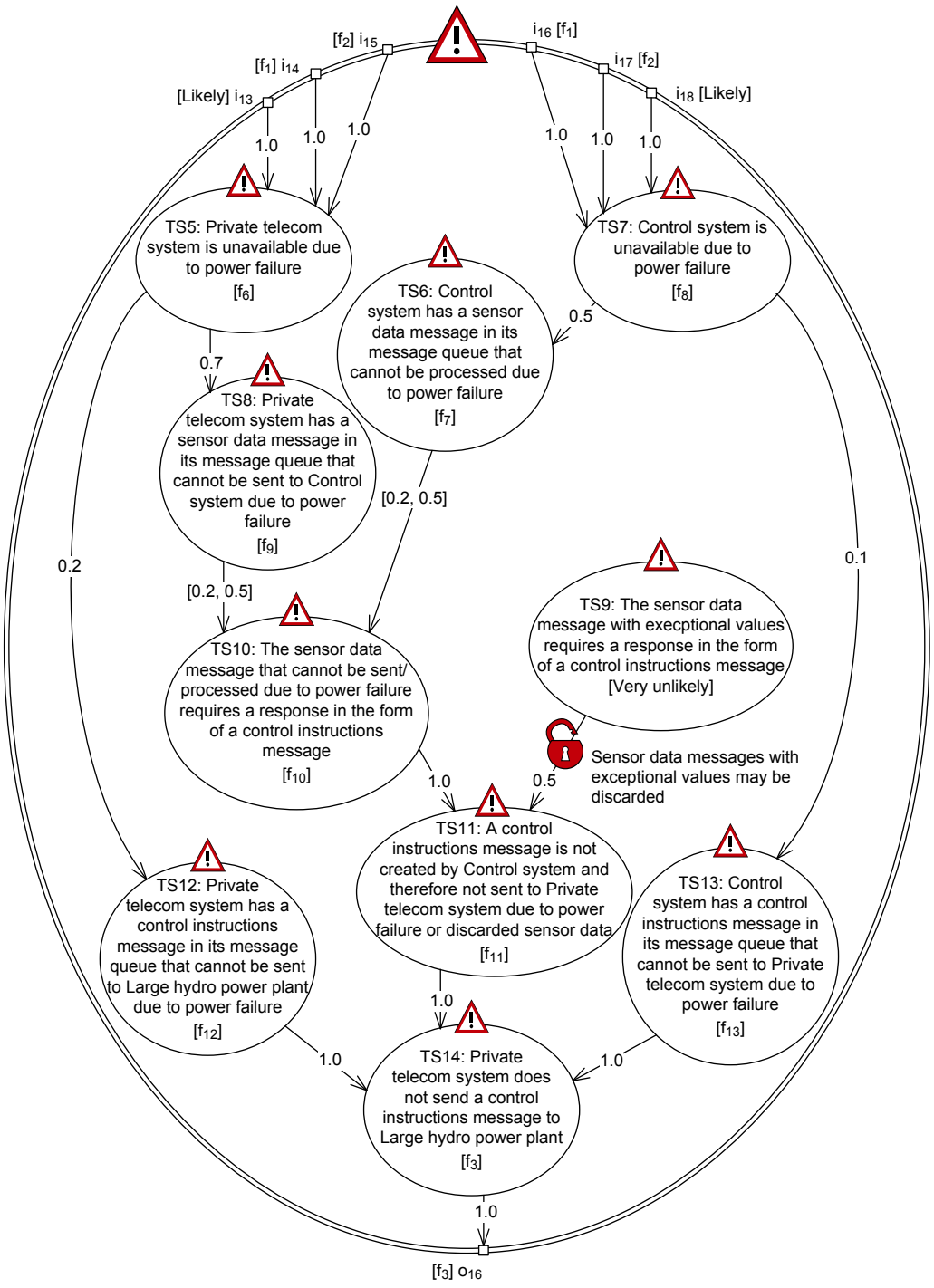


Figure 71: CORAS diagram based on the CORAS diagram in Figure 53 on page 93

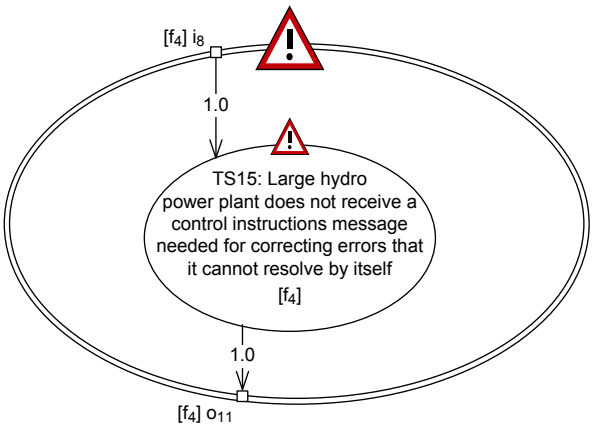


Figure 72: CORAS diagram based on the CORAS diagram in Figure 57 on page 96

$TS1 \sqcap\!| \, TS5$, $TS2 \sqcap\!| \, TS5$, and $TS3 \sqcap\!| \, TS5$ are separate. We calculate f_6 as follows:

$$
\begin{aligned}
f_6 &= f_{(TS1 \ \sqcap\!| \ TS5) \sqcup (TS2 \ \sqcap\!| \ TS5) \sqcup (TS3 \ \sqcap\!| \ TS5)} \\
&= [min_{f_6}, max_{f_6}] \text{ (\textbf{Rule 5}) where} \\
min_{f_6} &= max(min(f_{TS1 \ \sqcap\!| \ TS5}), min(f_{TS2 \ \sqcap\!| \ TS5}), min(f_{TS3 \ \sqcap\!| \ TS5})) \\
&= max(min([0.2 \cdot c_9, 0.5 \cdot c_9]), min([0, 0.1 \cdot c_8]), min([5, 9.9])) \\
&= max(0.2 \cdot c_9, 0, 5) = max(0.2 \cdot c_9, 5) \\
max_{f_6} &= max(f_{TS1 \ \sqcap\!| \ TS5}) + max(f_{TS2 \ \sqcap\!| \ TS5}) + max(f_{TS3 \ \sqcap\!| \ TS5}) \\
&= max([0.2 \cdot c_9, 0.5 \cdot c_9]) + max([0, 0.1 \cdot c_8]) + max([5, 9.9]) \\
&= (0.5 \cdot c_9) + (0.1 \cdot c_8) + 9.9
\end{aligned}
$$

The frequency interval calculated for $TS5$ can also be used as a frequency for $TS7$ since $f_{TS1 \ \sqcap\!| \ TS5}$ equals $f_{TS1 \ \sqcap\!| \ TS7}$, $f_{TS2 \ \sqcap\!| \ TS5}$ equals $f_{TS2 \ \sqcap\!| \ TS7}$, and $f_{TS3 \ \sqcap\!| \ TS5}$ equals $f_{TS4 \ \sqcap\!| \ TS7}$. In addition, the frequency of $TS7$ needs to be calculated by the use of **Rule 5**, since we do not know whether $TS1 \sqcap\!| \, TS7$, $TS2 \sqcap\!| \, TS7$, and $TS4 \sqcap\!| \, TS7$ are separate. We end with the following value for f_8:

$$
\begin{aligned}
f_8 &= f_{(TS1 \ \sqcap\!| \ TS7) \sqcup (TS2 \ \sqcap\!| \ TS7) \sqcup (TS4 \ \sqcap\!| \ TS7)} \\
&= [min_{f_8}, max_{f_8}] \text{ (\textbf{Rule 5}) where} \\
min_{f_5} &= (max(0.2 \cdot c_9, 5) \\
max_{f_5} &= (0.5 \cdot c_9) + (0.1 \cdot c_8) + 9.9
\end{aligned}
$$

We continue by calculating the frequency of $TS10$, i.e., f_{10}. Before we can calculate this frequency, we need to calculate the frequencies of $TS5 \sqcap\!| \, TS8$, i.e., f_9, $TS7 \sqcap\!| \, TS6$, i.e., f_7,

$TS8 \sqcap\!| \, TS10$, and $TS6 \sqcap\!| \, TS10$. We calculate these as follows:

$$
\begin{aligned}
f_9 &= f_{TS5 \ \sqcap\!| \ TS8} \\
&= f_5 \cdot 0.7 \textbf{ (Rule 3)} \\
&= [max(0.2 \cdot c_9, 5), (0.5 \cdot c_9) + (0.1 \cdot c_8) + 9.9] \cdot 0.7 \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.7, (0.35 \cdot c_9) + (0.07 \cdot c_8) + 6.93] \\
f_{TS8 \ \sqcap\!| \ TS10} &= f_9 \cdot [0.2, 0.5] \textbf{ (Rule 3)} \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.7, (0.35 \cdot c_9) + (0.07 \cdot c_8) + 6.93] \cdot [0.2, 0.5] \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.14, (0.175 \cdot c_9) + (0.035 \cdot c_8) + 3.465] \\
f_7 &= f_{TS7 \ \sqcap\!| \ TS6} \\
&= f_8 \cdot 0.5 \textbf{ (Rule 3)} \\
&= [max(0.2 \cdot c_9, 5), (0.5 \cdot c_9) + (0.1 \cdot c_8) + 9.9] \cdot 0.5 \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.5, (0.25 \cdot c_9) + (0.05 \cdot c_8) + 4.95] \\
f_{TS6 \ \sqcap\!| \ TS10} &= f_7 \cdot [0.2, 0.5] \textbf{ (Rule 3)} \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.5, (0.25 \cdot c_9) + (0.05 \cdot c_8) + 4.95] \cdot [0.2, 0.5] \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.1, (0.125 \cdot c_9) + (0.025 \cdot c_8) + 2.475]
\end{aligned}
$$

We use **Rule 4** to calculate the frequency of $(TS8 \ \sqcap\!| \ TS10) \sqcup (TS6 \ \sqcap\!| \ TS10)$, i.e., f_{10}, since $TS8 \sqcap\!| \, TS10$ and $TS6 \sqcap\!| \, TS10$ are separate. We calculate f_{10} as follows:

$$
\begin{aligned}
f_{10} &= f_{(TS8 \ \sqcap\!| \ TS10) \sqcup (TS6 \ \sqcap\!| \ TS10)} \\
&= [min_{f_{10}}, max_{f_{10}}] \textbf{ (Rule 4)} \text{ where} \\
min_{f_{10}} &= min(f_{TS8 \ \sqcap\!| \ TS10}) + min(f_{TS6 \ \sqcap\!| \ TS10}) \\
&= (max(0.2 \cdot c_9, 5) \cdot 0.14) + (max(0.2 \cdot c_9, 5) \cdot 0.1) = max(0.2 \cdot c_9, 5) \cdot 0.24 \\
max_{f_{10}} &= max(f_{TS8 \ \sqcap\!| \ TS10}) + max(f_{TS6 \ \sqcap\!| \ TS10}) \\
&= ((0.175 \cdot c_9) + (0.035 \cdot c_8) + 3.465) + ((0.125 \cdot c_9) + (0.025 \cdot c_8) + 2.475) \\
&= (3 \cdot c_9) + (0.06 \cdot c_8) + 5.94
\end{aligned}
$$

We continue by calculating the frequency of $TS11$, i.e., f_{11}. This frequency is based on the frequencies of $TS10 \sqcap\!| \, TS11$ and $TS9 \sqcap\!| \, TS11$. The events $TS10 \sqcap\!| \, TS11$ and $TS9 \sqcap\!| \, TS11$ are separate. Thus, we use **Rule 4** to calculate f_{11}. We calculate the frequencies of $TS10 \sqcap\!| \, TS11$, $TS9 \sqcap\!| \, TS11$, and $(TS10 \sqcap\!| \, TS11) \sqcup (TS9 \sqcap\!| \, TS11)$, i.e., f_{11}, as follows:

$$
\begin{aligned}
f_{TS10 \ \sqcap\!| \ TS11} &= f_{10} \cdot 1.0 \textbf{ (Rule 3)} \\
&= f_{10} \\
f_{TS9 \ \sqcap\!| \ TS11} &= [0.2, 0.5] \cdot 0.5 \textbf{ (Rule 3)} \\
&= [0.1, 0.25] \\
f_{11} &= f_{(TS10 \ \sqcap\!| \ TS11) \sqcup (TS9 \ \sqcap\!| \ TS11)} \\
&= [min_{f_{11}}, max_{f_{11}}] \textbf{ (Rule 4)} \text{ where} \\
min_{f_{11}} &= min(f_{TS10 \ \sqcap\!| \ TS11}) + min(f_{TS9 \ \sqcap\!| \ TS11})) \\
&= (max(0.2 \cdot c_9, 5) \cdot 0.24) + 0.1 \\
max_{f_{11}} &= max(f_{TS10 \ \sqcap\!| \ TS11}) + max(f_{TS9 \ \sqcap\!| \ TS11}) \\
&= ((3 \cdot c_9) + (0.06 \cdot c_8) + 5.94) + 0.25 \\
&= (3 \cdot c_9) + (0.06 \cdot c_8) + 6.19
\end{aligned}
$$

We continue by calculating the frequency of $TS14$, i.e., f_3. This frequency is based on the frequencies of $TS12 \sqcap\!| \, TS14$, $TS11 \sqcap\!| \, TS14$, and $TS13 \sqcap\!| \, TS14$. These frequencies belong to events that are separate. Thus, we use **Rule 4** to calculate f_3. In order to calculate the frequencies of $TS12 \sqcap\!| \, TS14$ and $TS13 \sqcap\!| \, TS14$, we first need to calculate the frequencies of $TS5 \sqcap\!| \, TS12$, i.e., f_{12}, and $TS7 \sqcap\!| \, TS13$, i.e., f_{13}. In the following, we first calculate f_{12} and f_{13}, before we calculate f_3 based on the frequencies of $TS12 \sqcap\!| \, TS14$, $TS11 \sqcap\!| \, TS14$, and $TS13 \sqcap\!| \, TS14$.

$$
\begin{aligned}
f_{12} &= f_{TS5 \sqcap\!| \, TS12} \\
&= f_6 \cdot 0.2 \text{ (\textbf{Rule 3})} \\
&= [max(0.2 \cdot c_9, 5), (0.5 \cdot c_9) + (0.1 \cdot c_8) + 9.9] \cdot 0.2 \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.2, (0.1 \cdot c_9) + (0.02 \cdot c_8) + 1.98] \\
f_{13} &= f_{TS7 \sqcap\!| \, TS13} \\
&= f_8 \cdot 0.1 \text{ (\textbf{Rule 3})} \\
&= [max(0.2 \cdot c_9, 5), (0.5 \cdot c_9) + (0.1 \cdot c_8) + 9.9] \cdot 0.1 \\
&= [max(0.2 \cdot c_9, 5) \cdot 0.1, (0.05 \cdot c_9) + (0.01 \cdot c_8) + 0.99] \\
f_{TS12 \sqcap\!| \, TS14} &= f_{12} \cdot 1.0 \text{ (\textbf{Rule 3})} \\
&= f_{12} \\
f_{TS11 \sqcap\!| \, TS14} &= f_{11} \cdot 1.0 \text{ (\textbf{Rule 3})} \\
&= f_{11} \\
f_{TS13 \sqcap\!| \, TS14} &= f_{13} \cdot 1.0 \text{ (\textbf{Rule 3})} \\
&= f_{13} \\
f_3 &= f_{(TS12 \sqcap\!| \, TS14) \sqcup (TS11 \sqcap\!| \, TS14) \sqcup (TS13 \sqcap\!| \, TS14)} \\
&= [min_{f_3}, max_{f_3}] \text{ (\textbf{Rule 4}) where} \\
min_{f_3} &= min(f_{TS12 \sqcap\!| \, TS14}) + min(f_{TS11 \sqcap\!| \, TS14}) + min(f_{TS13 \sqcap\!| \, TS14}) \\
&= (max(0.2 \cdot c_9, 5) \cdot 0.2) + ((max(0.2 \cdot c_9, 5) \cdot 0.24) + 0.1) + \\
&\quad (max(0.2 \cdot c_9, 5) \cdot 0.1) \\
&= (max(0.2 \cdot c_9, 5) \cdot 0.54) + 0.1 \\
max_{f_3} &= max(f_{TS12 \sqcap\!| \, TS14}) + max(f_{TS11 \sqcap\!| \, TS14}) + max(f_{TS13 \sqcap\!| \, TS14}) \\
&= ((0.1 \cdot c_9) + (0.02 \cdot c_8) + 1.98) + ((3 \cdot c_9) + (0.06 \cdot c_8) + 6.19) + \\
&\quad ((0.05 \cdot c_9) + (0.01 \cdot c_8) + 0.99) \\
&= (3.15 \cdot c_9) + (0.09 \cdot c_8) + 9.16
\end{aligned}
$$

We have now calculated frequencies for all the threat scenarios in Figure 71. We continue by calculating the frequency f_4 of the threat scenario $TS15$ in Figure 72. We calculate f_4 as follows:

$$
\begin{aligned}
f_4 &= f_{TS14 \sqcap\!| \, TS15} \\
&= f_3 \cdot 0.01 \text{ (\textbf{Rule 3})} \\
&= [(max(0.2 \cdot c_9, 5) \cdot 0.54) + 0.1, (3.15 \cdot c_9) + (0.09 \cdot c_8) + 9.16] \cdot 0.01 \\
&= [(max(0.2 \cdot c_9, 5) \cdot 0.0054) + 0.001, (0.0315 \cdot c_9) + (0.00081 \cdot c_8) + 0.0916]
\end{aligned}
$$

The next step is to calculate the frequency f_5 of the unwanted incident $UI1$ occurring. We

calculate this frequency as follows:

$$
\begin{aligned}
f_5 &= f_{TS15 \ \sqcap\!\!| \ UI1} \\
&= f_4 \cdot 0.9 \textbf{ (Rule 3)} \\
&= [(max(0.2 \cdot c_9, 5) \cdot 0.0054) + 0.001, (0.0315 \cdot c_9) + (0.0009 \cdot c_8) + 0.0916] \cdot 0.9 \\
&= [(max(0.2 \cdot c_9, 5) \cdot 0.00486) + 0.0009, (0.02835 \cdot c_9) + (0.0009 \cdot c_8) + 0.08244]
\end{aligned}
$$

We continue by calculating *Expected service level*$_T$ and *Expected service level*$_E$. We calculate these as follows:

$$
\begin{aligned}
\textit{Expected service level}_T &= \frac{\textit{Maximum service level}_T - (\textit{Likelihood} \cdot \textit{Consequence}_T)}{\textit{Maximum service level}_T} \\
&= \frac{8760 - (f_5 \cdot 24)}{8760} \\
\textit{Expected service level}_E &= \frac{\textit{Maximum service level}_E - (\textit{Likelihood} \cdot \textit{Consequence}_E)}{\textit{Maximum service level}_E} \\
&= \frac{365000 - (f_5 \cdot 1000)}{365000}
\end{aligned}
$$

The final step is to define how *Risk Value* should be calculated. We calculate *Risk Value* as follows:

if $\dfrac{8760 - (f_5 \cdot 24)}{8760} \geq \dfrac{8760 \cdot 0.999}{8760}$ **and**
$\dfrac{365000 - (f_5 \cdot 1000)}{365000} \geq \dfrac{364800}{365000}$ **then**
Risk value = *Acceptable*
else
Risk value = *Unacceptable*
endif

Technology for a better society

www.sintef.no