SINTEF A24343- Unrestricted

Report

An Approach to Select Cost-Effective Risk Countermeasures Exemplified in CORAS

Author(s)
Le Minh Sang Tran
Bjørnar Solhaug
Ketil Stølen

SINTEF ICT
Networked Systems and Services
2013-07-29

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

SINTEF

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

Report

An Approach to Select Cost-Effective Risk Countermeasures Exemplified in CORAS

KEYWORDS:
Risk
Cost
Benefit
Countermeasure
Security
Risk modeling

VERSION Final	**DATE** 2013-07-29

AUTHOR(S)
Le Minh Sang Tran
Bjørnar Solhaug
Ketil Stølen

CLIENT(S) N/A	**CLIENT'S REF.** N/A
PROJECT NO. N/A	**NUMBER OF PAGES/APPENDICES:** 40 pages with appendices

ABSTRACT

Security risk analysis should be conducted regularly for organizations to maintain an acceptable level of security. In principle, all risks that are unacceptable according to the predefined criteria should be mitigated. However, risk mitigation comes at a cost, and only the countermeasures that cost-efficiently mitigate risks should be implemented. This report presents an approach to integrate the countermeasure cost-benefit assessment into the risk analysis, and to provide decision makers with the necessary decision support. The approach comes with the necessary modeling support, a calculus for reasoning about the countermeasure cost and effect, as well as means for visualization of the results to aid decision makers. The approach is generic in the sense that the modeling and analysis techniques can be instantiated in several established approaches to risk assessment. In this report we demonstrate the instantiation in CORAS and exemplify the approach using an eHealth scenario.

PREPARED BY Bjørnar Solhaug	SIGNATURE Bjørnar Solhaug
CHECKED BY Atle Refsdal	SIGNATURE Atle Refsdal
APPROVED BY Fredrik Seehusen	SIGNATURE

REPORT NO.	**ISBN**	**CLASSIFICATION**	**CLASSIFICATION THIS PAGE**
SINTEF A24343	978-82-14-05322-7	Unrestricted	Unrestricted

An Approach to Select Cost-Effective Risk Countermeasures Exemplified in CORAS

Le Minh Sang Tran, Bjørnar Solhaug and Ketil Stølen

July 30, 2013

Abstract

Security risk analysis should be conducted regularly for organizations to maintain an acceptable level of security. In principle, all risks that are unacceptable according to the predefined criteria should be mitigated. However, risk mitigation comes at a cost, and only the countermeasures that cost-efficiently mitigate risks should be implemented. This report presents an approach to integrate the countermeasure cost-benefit assessment into the risk analysis, and to provide decision makers with the necessary decision support. The approach comes with the necessary modeling support, a calculus for reasoning about the countermeasure cost and effect, as well as means for visualization of the results to aid decision makers. The approach is generic in the sense that the modeling and analysis techniques can be instantiated in several established approaches to risk assessment. In this report we demonstrate the instantiation in CORAS and exemplify the approach using an eHealth scenario.

Contents

1 Introduction

In order to treat risks, decision makers (or managers) have to make decisions on proper countermeasures to implement. However, such investment decisions may be complicated. An organization needs the best possible information on risks and countermeasures to decide what is the best investment. This involves deciding which countermeasures offer a good trade-off between benefit and spending. The expenditure required to implement the countermeasures, together with their ability to mitigate risks, are factors that affect the selection. Inappropriate and over-expensive countermeasures are money lost. Therefore, a systematic method that helps to reduce business exposure while balancing countermeasure investment against risks is needed. Such a method should help answering questions like *"(1): How much is it appropriate to spend on countermeasures?"* and *"(2): Where should spending be directed?"* as highlighted by Birch and McEvoy [3].

Unfortunately, there exists little support for the prescriptive and specific information that managers require to select cost-effective risk countermeasures. Several cost estimation models have been proposed, but most are only loosely coupled to risk analysis. For example, the Security Attribute Evaluation Method (SAEM) [6] is well-suited to evaluate risk reduction, but is very vague on the issue of cost effectiveness. Likewise, [9] suggests several methods to assess cost of risks (*e.g.,* Cost-Of-Illness, Willingness-To-Pay), but none of these methods provide specific support to evaluate countermeasure expenditure. Chapman et al. [7] propose a framework which justifies mitigation strategies based on cost-difference, but does not take the benefit-difference (*i.e.* level of risk reduction) between strategies into consideration.

Effective decision-making requires a correct risk model incorporating multi-aspect information on countermeasures and a method to select between cost-effective countermeasure alternatives. The multi-aspect information should contain the knowledge about the countermeasures themselves, their associated expenditures and suitability to mitigate risks, as well as to what extent they depend on each other. This report does not focus on how to obtain this information, but rather on how to make use of this information to select effective risk countermeasures. In particular, we propose a systematic approach to integrate such multi-aspect information in reasoning about and prioritization of countermeasure alternatives. We are not aware of other approaches of this kind. Our approach is sufficiently generic to be integrated within many existing risk analysis methods. We demonstrate this by instantiating our generic approach in the CORAS method for security risk analysis [16] with concrete illustrative examples.

The structure of the report is as follows. In Section 2 we describe our generic approach. Next, in Section 3 we exemplify the approach by instantiating it in the CORAS method. We present related work in Section 4, and we summarize and draw conclusions in Section 5. At the end there is a set of appendices providing a formal underpinning for the proposed approach. The main results of this report is presented in a paper by the same authors [27].

2 Our approach

Section 2.1 provides an overview of our approach which consists of three main steps. It also presents the conceptual model on which our approach builds. Section 2.2 describes the expectations to the risk model resulting from the risk assessment that our three-steps approach requires as input. Finally, in Section 2.3 to Section 2.5 we describe the three steps in further detail.

2.1 Process overview

As illustrated in Fig. 1, our approach takes a risk model resulting from a risk assessment and the associated risk acceptance criteria as input, and delivers a recommended countermeasure alternative as output. Hence, the approach assumes that the risk assessment has already been conducted, i.e. that risks have been identified, estimated and evaluated and that the overall risk analysis process is ready to proceed with the risk treatment phase. We moreover assume that the risk analysis process complies with the ISO 31000 risk management standard [13], in which risk countermeasure is the final phase. Our process consists of three main steps as follows:

Step 1 *Annotate risk model:*

Identify and document countermeasures. The results are documented by annotating the risk model taken as input with relevant information including the countermeasures, their cost, their reduction effect (i.e., effect on risk value), as well as possible effect dependencies (i.e., countervailing effects among countermeasures).

Step 2 *Perform countermeasure analysis:*

Enumerate all countermeasure alternatives (*i.e.* combinations of countermeasures to address risks) and reevaluate the risk picture for each alternative. The analysis makes use of the annotated risk model and a calculus for propagating and aggregating the reduction effect and effect dependency along the risk paths of the model.

Step 3 *Perform synergy analysis:*

Perform synergy analysis for selected risks based on decision diagrams. The output recommends countermeasure alternative cost-effectively mitigating the selected risks.

Fig. 2 presents the conceptual model, expressed as a UML class diagram [23] on which our approach builds. A *Risk Model* is a structured way of representing unwanted incidents, their causes and consequences using graphs, trees or block diagrams [22], or tables [16]. An unwanted incident is an event that harms or reduces the value of an asset, and a risk is the likelihood of an unwanted incident and its consequence for a specific asset [13]. A *Countermeasure* mitigates risk by reducing its likelihood and/or consequence. The *Expenditure* includes the expenditure of countermeasure implementation, maintenance and so on for a defined period of time. The *Effects Relation* captures the extent to which a countermeasure mitigates risks. The *Effects Relation* could be the reduction of likelihood, and/or the reduction of consequence of a risk. The *Dependency Relation* captures the countervailing effect among countermeasures that must be taken into account in order to understand the combined effect of identified

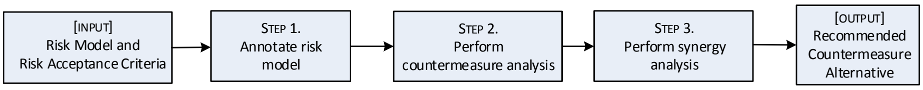


Fig. 1: Three-steps approach

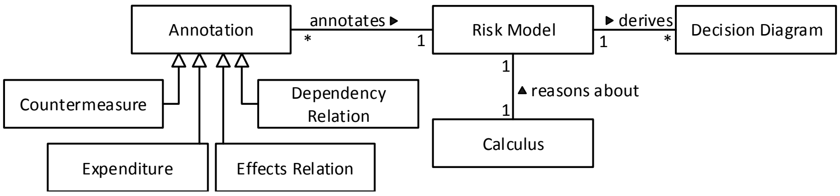


Fig. 2: Conceptual model

countermeasures. The *Calculus* provides a mechanism to reason about the annotated risk model. Using the *Calculus*, we can perform countermeasure analysis on annotated risk models to calculate the residual risk value for each individual risk. A *Decision Diagram* facilitates the decision making process based on the countermeasure analysis.

2.2 Input assumptions

As already explained, the input required by our approach is the result of a risk assessment in the form of a risk model, and the corresponding risk acceptance criteria. To ensure that our approach is compatible with established risk modeling techniques, we only require that the risk model can be understood as a risk graph. A risk graph [5] is a common abstraction of several established risk modeling techniques such as Fault Tree Analysis (FTA) [11], Event Tree Analysis (ETA) [12], Attack Trees [24], Cause-Consequence Diagrams [17, 22], Bayesian networks [8], and CORAS risk diagrams [16]. Hence, our approach complies with these risk modeling techniques, and can be instantiated by them.

A risk graph is a finite set of vertices and relations (see Fig. 3). Each vertex v represents a threat scenario, for example a set of events that may lead to a risk, and can be assigned a likelihood f, and a consequence i[1]. In [5] likelihood is represented in terms of probabilities, but in this report we work with frequencies. A *leads-to* relation from vertex v_1 to vertex v_2 means that the former may lead to the latter (but not necessarily causally). The positive real numbers decorating the relations may to the extent they are within $[0, 1]$ be understood as conditional probabilities indicating the likelihood of the former to lead to the latter when the former occurs. We allow, however, arbitrary positive real numbers to facilitate the modeling of a single occurrence of one vertex leading to multiple occurrences of another.

2.3 Detailing of Step 1 – Annotate risk model

This step is to annotate the input risk model with required information for further analysis. There are four types of annotation as follows:

[1] We use i and not c to denote consequences since we use c to denote countermeasures.

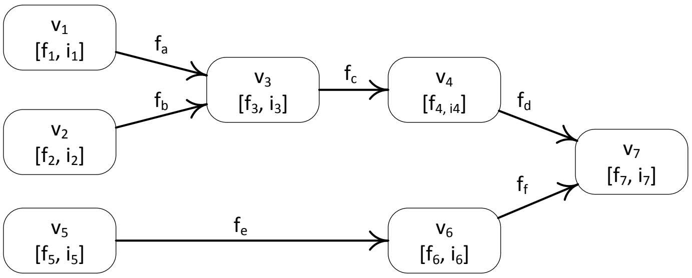


Fig. 3: Risk graph

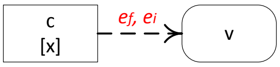


Fig. 4: Effects relation

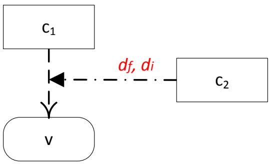


Fig. 5: Dependency relation

Countermeasure: In risk graphs, countermeasures are represented as rectangles. In Fig. 4 there is one countermeasure and this is named c.

Expenditure: An expenditure is expressed within square brackets following the countermeasure name (x in Fig. 4). This is an estimation of the expense to ensure the mitigation of countermeasure including expenditure of implementation, deployment, maintenance, and so on.

Effects relation: An effects relation is represented by a dashed arrow decorated by two numbers (e_f for *frequency effect* and e_i for *impact effect*) in Fig. 4). It captures the mitigating effect of a countermeasure in terms of reduced frequency, reduced consequence, or both. Both e_f and e_i are relative percentage values, *i.e.* $e_f, e_i \in [0, 1]$.

Dependency relation: In risk graphs, a dependency relation is represented by a dash-dot arrow with solid arrowhead decorated by two numbers, namely d_f for *frequency dependency* and d_i for *impact dependency*, as illustrated in Fig. 5. A dependency relation captures how a countermeasure effect may depend on another countermeasure, *i.e.* it can decrease the frequency effect and/or impact effect of another countermeasure. In Fig. 5 the d_f impacts e_f while the d_i impacts e_i. Both d_f and d_i are relative percentage values, *i.e.* $d_f, d_i \in [0, 1]$.

2.4 Detailing of Step 2 – Countermeasure analysis

The countermeasure analysis is conducted for every individual risk of the annotated risk model. The analysis enumerates all possible countermeasure combinations, called *countermeasure alternatives* (or *alternatives* for short) and evaluates the residual risk value (*i.e.* residual frequency and consequence value) with respect to each alternative to determine the most effective one. Residual risk value is obtained by propagating the reduction effect along the risk model to get the revised risk values.

From the leftmost threat scenarios (*i.e.* scenarios that have only outgoing *leads-to* relations), frequencies assigned to threat scenarios are propagated to the right using a formal calculus which is defined in the appendices at the end of the report. During the propagation, frequencies assigned to *leads-to* relations, reduction effects, and effect dependencies are taken into account. Finally, the propagation stops at the rightmost threat scenarios (*i.e.* scenarios that have only incoming *leads-to* relations). Based on the results from the propagation, the residual risk value is computed.

Decision Diagram (Fig. 6) is a directed graph used to visualize the outcome of a countermeasure analysis. A node in the diagram represents a *risk state* which is a triplet of a likelihood, a consequence, and a countermeasure alternative for the risk being analyzed. The frequency and consequence are the X and Y coordinates of the node. The countermeasure alternative is annotated on the path from the *initial state* S_0 (representing the situation where no countermeasure has yet been applied. Notice that we ignore all states whose residual consequence and probability are both greater than those of S_0 since it is useless to implement such countermeasures.

2.5 Detailing of Step 3 – Synergy analysis

The aim of the synergy analysis is to recommend a cost-effective countermeasure alternative for mitigating all risks. Such a recommendation is based on the decision diagrams for the individual risks (generated in Step 2), the risk acceptance criteria, and the overall cost (OC) of each countermeasure alternative. The OC is calculated as follows:

$$\mathrm{OC}(ca) = \sum_{r \in R} \mathrm{rc}(r) + \sum_{c \in ca} \mathrm{cost}(c) \tag{1}$$

Here, ca is a countermeasure alternative; R is the set of risks; rc() is a function that yields the loss (in monetary value) due to the risk taken as argument (based on its likelihood and consequence); cost() is a function that yields the expenditure of the countermeasure taken as argument.

The synergy analysis is decomposed into the following three substeps:

Step 3A *Identify countermeasure alternatives:*
Identify the set of countermeasure alternatives CA for which all risks are acceptable with respect to the risk acceptance criteria. Decision diagrams of individual risks can be exploited to determine CA.

Step 3B *Evaluate countermeasure alternatives:*
If there is no countermeasure alternative for which all risks fullfill the risk acceptance criteria ($CA = \varnothing$), do either of the following:

- identify new countermeasures and go to Step 1, or
- adjust the risk acceptance criteria and go to Step 3A.

Otherwise, if there is at least one such countermeasure alternative ($CA \neq \varnothing$), calculate the overall cost of each $ca \in CA$.

Step 3C *Select cost-effective countermeasure alternative:*
If there is at least one countermeasure $ca \in CA$ for which $\mathrm{OC}(ca)$ is acceptable (for the customer company in question) select the cheapest and terminate the analysis. Otherwise, identify more (cheaper and/or more effective) countermeasures and go to Step 1.

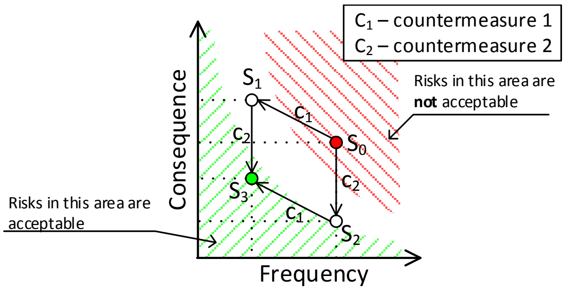


Fig. 6: Decision diagram

The above procedure may of course be detailed further based on various heuristics. For example, in many situations, with respect to Step 3A, if we already know that countermeasure alternative ca is contained in CA then we do not have to consider other countermeasure alternatives ca' such that $ca \subseteq ca'$. However, we do not go into these issues here.

3 Exemplification in CORAS

As a demonstration of applicability, this section instantiates the proposed approach into the CORAS method for security risk analysis [16] and exemplifies how the resulting extended CORAS method and language can be used to select cost-efficient risk countermeasures in an example drawn from a case study within the eHealth domain [21].

The *risk model* in the CORAS method is captured by so-called *risk diagrams*. A risk diagram is a graph consisting of potential causes (*i.e. threats*) that might (or might not) exploit flaws, weaknesses, or deficiencies (*i.e. vulnerabilities*) causing a series of events (*i.e. threat scenarios*) to happen, which could lead to *unwanted incidents* with certain likelihood and concrete consequence (*i.e. risks*) to a particular *asset*. Threat scenarios and risks are also called core elements in the risk diagram notation.

In the risk diagram, there are two kinds of relationships with assigned likelihoods: *initiate* and *leads-to* relations. The former connects a threat to a core element, and the latter connects a core element to another core element. Likelihoods assigned to *initiate* relations can be either *probabilities* or *frequencies* (as well as purely qualitative), whereas, likelihoods assigned to *leads-to* relations are *conditional likelihoods*.

Any risk diagram can be understood as an instantiation of a risk graph; such a conversion is formally defined in [5]. In this report, we adjust the steps of the generic method such that they work directly with CORAS artifacts. To make the instantiation more comprehensible, we also present a running example that exploits an eHealth scenario proposed by the NESSoS project [19] to exemplify the resulting extended CORAS method.

3.1 eHealth running example: Patient monitoring

Patients' behaviors and symptoms are monitored in real-time. This provides an improved basis for disease diagnoses and tailored therapy prescription regiments.

Patients are equipped with sensors that continuously collect patient data and send these data to a handheld smart device (*e.g.,* smart phone). This smart device, in turn, sends the patient data to external eHealth servers to update the patients' eHealth Records (EHRs).

The CORAS risk diagram in Fig. 7 presents a partial result from a risk analysis of the Patient Monitoring scenario [21]. In this risk diagram, *network failure* exploits the vulnerability *unstable/unreliable network connection* to initiate *network connection goes down*. Likewise, *handheld HW failure* exploits the vulnerability *unstable/unreliable handheld HW* to initiate *handheld goes down*. Both *handheld goes down* as well as *network connection goes down* may lead to the scenario *transmission of monitored data is interrupted*. This, consequently, may lead to *loss of monitored data* which impacts the *provisioning of monitoring service*. The rest of the diagram is interpreted in the similar manner.

We assume in the following that this diagram is a consistent and complete documentation of risks identified during the risk assessment. We moreover use frequencies to estimate likelihoods of core elements.

3.2 Applying Step 1 – Annotate risk model

In this step, we annotate the CORAS risk diagrams according to Step 1 to create CORAS treatment diagrams. Note that in CORAS, countermeasures are referred to as treatments.

Treatment annotation: Treatments can apply to most of the elements in a risk diagram, including all types of core elements, threats, and vulnerabilities. Fig. 8 shows an example in which a treatment *implement redundant network connection* treats the scenario *network connection goes down* which was initiated by *network failure* by exploiting the vulnerability *unstable/unreliable network connection*.

Expenditure annotation: The treatment expenditure, annotated as a value inside the treatment bubble, is the total expenditure spent for a treatment in a period of time. For instance, in Fig. 8, the expenditure for *implement a redundant network connection* is 5000$ in ten years.

Effects relation annotation: Following Step 1, reduction effect in the CORAS instantiation is annotated on *treats* relations as a pair of a frequency effect and an impact effect. For example, in Fig. 8, the frequency of network failure is thirty times in ten years, annotated as $30 : 10y$. In a CORAS diagram, we suffix the frequency and impact effects with the letters *'F'* and *'I'*, respectively, to distinguish between them. The treatment *implement redundant network connection* only effects the frequency (not consequence) of *network connection goes down* (NCD) by 0.7 at cost 5000$. This means the reduced frequency is

$$(1 - 0.7) \cdot (30 : 10y) = (9 : 10y).$$

Dependency relation annotation: We also suffix the frequency and impact dependencies with the letters *'F'* and *'I'*, respectively, to distinguish between them. In Fig. 8, to mitigate NCD, we could *ensure sufficient Quality-of-Service (QoS) from network provider* with the cost of 15000USD:10y. This, however, reduces the effect of a redundant connection, which means that the two identified treatments are countervailing. Ensuring such QoS will reduce the reduction effect of a redundant connection by 0.3 as annotated in the figure.

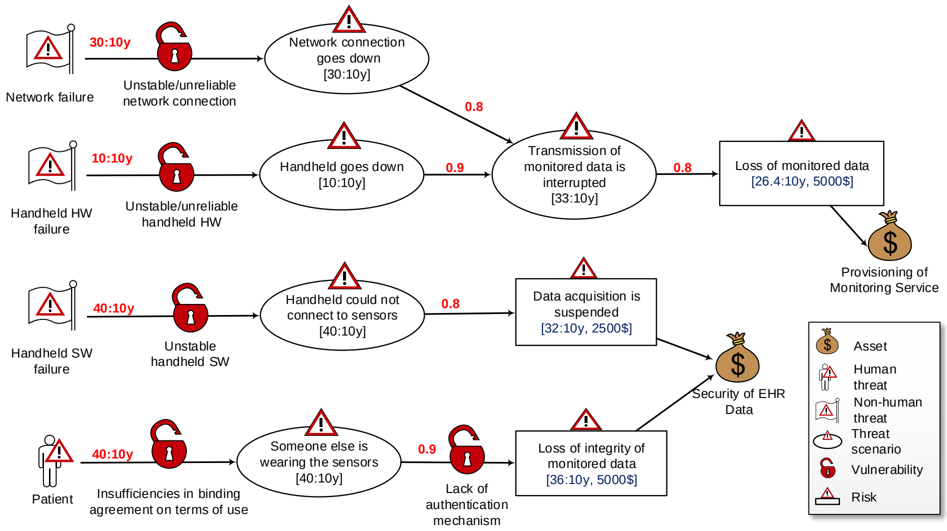

Network failure
30:10y
Unstable/unreliable network connection
Network connection goes down [30:10y]
0.8
Handheld HW failure
10:10y
Unstable/unreliable handheld HW
Handheld goes down [10:10y]
0.9
Transmission of monitored data is interrupted [33:10y]
0.8
Loss of monitored data [26.4:10y, 5000$]
Provisioning of Monitoring Service
Handheld SW failure
40:10y
Unstable handheld SW
Handheld could not connect to sensors [40:10y]
0.8
Data acquisition is suspended [32:10y, 2500$]
Security of EHR Data
Patient
40:10y
Insufficiencies in binding agreement on terms of use
Someone else is wearing the sensors [40:10y]
0.9
Lack of authentication mechanism
Loss of integrity of monitored data [36:10y, 5000$]
Asset
Human threat
Non-human threat
Threat scenario
Vulnerability
Risk

Fig. 7: Risk diagram of the scenario

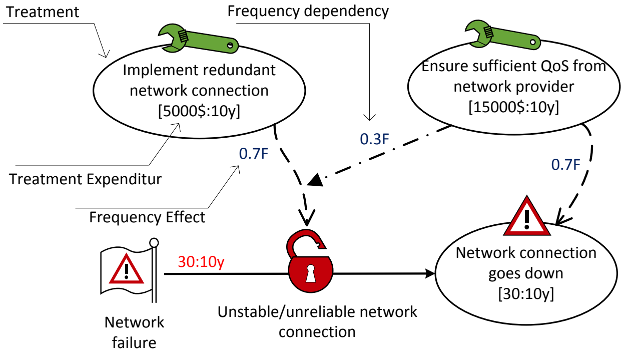

Treatment
Frequency dependency
Implement redundant network connection [5000$:10y]
Ensure sufficient QoS from network provider [15000$:10y]
0.3F
0.7F
0.7F
Treatment Expenditur
Frequency Effect
Network failure
30:10y
Unstable/unreliable network connection
Network connection goes down [30:10y]

Fig. 8: Annotated diagram

3.3 Applying Step 2 – Treatment analysis

The analysis employs the calculus formally defined for risk graphs in the appendices based on a common sense mapping to CORAS along the lines sketched in Appendix F. Fig. 9 shows the complete diagram resulting from annotating the risk diagram in Fig. 7 with frequencies recalculated.

Here, we describe an example of propagation for the risk *Loss of Monitored Data* (LMD). According to the diagram in Fig. 7, *Network Failure* initiates *Network Connection goes Down*(NCD) with frequency $30 : 10y$. *Implement Redundant Network connection*(IRN) will reduce this frequency by 0.7. However, this effect depends on the treatment *Ensure sufficient QoS from network provider* (EQS), as captured by the dependency relation. The estimated frequency dependency is of 0.3. If both these treatments are to be considered together in a treatment alternative, the dependency must be resolved. Hence, by combining rules C.4.1 and C.4.2 from the appendix, the frequency propagated to NCD is

$$(30 : 10y) \cdot (1 - 0.7 \cdot (1 - 0.3)) \approx (15 : 10y).$$

Now calculating the effect of EQS yields the frequency $4.5 : 10y$ for the scenario NCD. Similarly, the frequency propagated to *Handheld Goes Down* (HGD) (using C.4.1) is

$$(10 : 10y) \cdot (1 - 0.7) = (3 : 10y).$$

Under the assumption that any occurrence of *Transmission of monitored Data is Interrupted* (TDI) due to NCD is disjoint from any occurrence of TDI due to HGD, the frequency propagated to TDI (using B.3.3) is

$$(4.5 : 10y) \cdot 0.8 + (3 : 10y) \cdot 0.9 = (6.3 : 10y).$$

Finally, the propagated frequency of LMD (using B.3.1) is

$$(6.3 : 10y) \cdot 0.8 = (5.04 : 10y).$$

Fig. 10 presents decision diagrams for risks LMD (Loss of Monitored Data) and LID (Loss of Integrity of monitored Data). The detailed result for the risk LMD, including the listing of the different treatment alternatives, is provided in Table 1.

3.4 Applying Step 3 – Synergy analysis

To facilitate the synergy analysis described in Step 3, we define the rc() function in (1) as follows: $\text{rc}(r) = i \cdot f$, where i is the consequence and f is the frequency of the risk r. Having decision diagrams for individual risks, we may identify the set of treatment alternatives for which all risks fulfill the risk acceptance criteria, and calculate their overall costs. The result may be summarized as in Table 2. The *Treatment Alternative* indicates the set of treatments to be implemented. The next three columns explain how the treatment alternative is established from the states of individual risks. Finally, the last column reports the overall cost of the treatment alternative.

4 Related work

Mehr and Forbes [18] suggest that "risk management theory needs to merge with traditional financial theory in order to bring added realism to the decision-making process". In line with the suggestion, cost-benefit analysis (CBA) is often used with risk management to assess the effectiveness of risk countermeasures [1,4,25]. Our approach may be seen as a special case or refinement of the CBA process.

In risk management, decision on different risk mitigation alternatives has been emphasized in many studies [9, 20, 26]. The guideline in [26] proposes CBA to optimally allocate resources and implement cost-effective controls after identifying all possible countermeasures. This encompasses the determination of the impact of implementing (and not implementing) the mitigations, and the estimated costs of them. Another guideline [9] provides a semi-quantitative risk assessment. The probability and impact of risks are put into categories which are assigned scores. The differences between the total score for all risks before and after any proposed risk reduction strategy relatively show the efficiency among

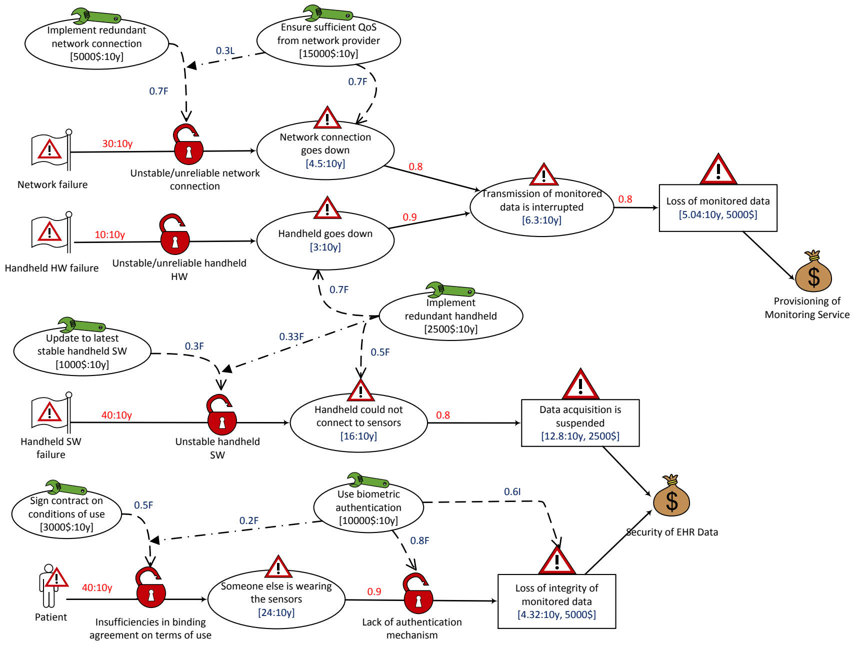

Implement redundant network connection [5000$:10y]
Ensure sufficient QoS from network provider [15000$:10y]
0.3L
0.7F
0.7F
Network failure
30:10y
Unstable/unreliable network connection
Network connection goes down [4.5:10y]
0.8
Transmission of monitored data is interrupted [6.3:10y]
0.8
Loss of monitored data [5.04:10y, 5000$]
Provisioning of Monitoring Service
Handheld HW failure
10:10y
Unstable/unreliable handheld HW
Handheld goes down [3:10y]
0.9
0.7F
Implement redundant handheld [2500$:10y]
Update to latest stable handheld SW [1000$:10y]
0.3F
0.33F
0.5F
Handheld SW failure
40:10y
Unstable handheld SW
Handheld could not connect to sensors [16:10y]
0.8
Data acquisition is suspended [12.8:10y, 2500$]
Security of EHR Data
Sign contract on conditions of use [3000$:10y]
0.5F
0.2F
Use biometric authentication [10000$:10y]
0.6I
0.8F
Patient
40:10y
Insufficiencies in binding agreement on terms of use
Someone else is wearing the sensors [24:10y]
0.9
Lack of authentication mechanism
Loss of integrity of monitored data [4.32:10y, 5000$]

Fig. 9: Annotated treatment diagram with frequencies propagated

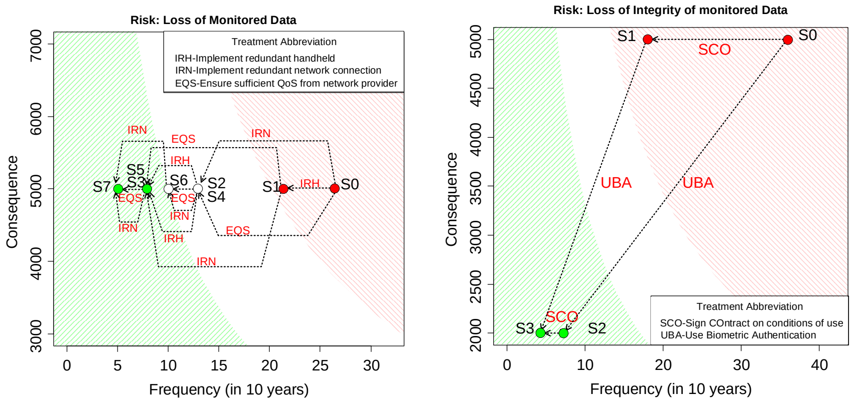
Table 1: Analysis for the risk LMD

The name of each treatment alternative is shown in the first column (Risk State). The *Frequency* column is number of occurrences in ten years. Both *Frequency* and *Consequence* columns are values after considering the treatments.

Risk/Risk State	Treatment			Frequency	Consequence
	Implement Redundant Handheld	Implement Redundant Network connection	Ensure sufficient QoS from network provider		
Risk : Loss of Monitored Data					
S0				26.4	5000
S1	•			21.36	5000
S2		•		12.96	5000
S3	•	•		7.92	5000
S4			•	12.96	5000
S5	•		•	7.92	5000
S6		•	•	10.08	5000
S7	•	•	•	5.04	5000

strategies, and effectiveness of their costs. It also suggests that the economic costs for baseline risks should be evaluated using one of the following methods: Cost-Of-Illness, Willingness-To-Pay, Qualified-Adjusted Life Years, Disability-Adjusted Life Years. However, these methods have not been designed to assess cost of treatments, but rather cost of risks.

Norman [20] advocates the use of Decision Matrix to agree on countermea-



(a)

(b)

Fig. 10: Decision diagrams of risks in the eHealth scenario

Table 2: Results from synergy analysis

	Individual Risk			
Treatment Alternative	LID	LMD	DAS	Overall Cost
{UBA,SCO,IRH,IRN,USW}	S3	S3	S3	101740
{UBA,SCO,IRH,IRN,EQS,USW}	S3	S7	S3	102340
{UBA,IRH,IRN,USW}	S2	S3	S3	104500
{UBA,IRH,IRN,EQS,USW}	S2	S7	S3	105100
{UBA,SCO,IRH,IRN}	S3	S3	S2	108740
{UBA,SCO,IRH,IRN,EQS}	S3	S7	S2	109340
{UBA,IRH,IRN}	S2	S3	S2	111500
{UBA,IRH,IRN,EQS}	S2	S7	S2	112100

sure alternative. A Decision Matrix is a simple spreadsheet which contains a list of countermeasures and a list of risks which those countermeasures mitigate. For each countermeasure there are estimates with respect to cost, effectiveness, and convenience. The countermeasure effectiveness is measured by metrics contained within the Sandia Vulnerability Assessment Model[2]. The proposed approach is however not clearly defined, and all metrics are developed as spreadsheets which are complicated to implement and follow. Meanwhile, our proposal is graphical and backed up with a formal definition and reasoning. Butler [6] proposes the Security Attribute Evaluation Method (SAEM) to evaluate alternative security designs. It employs a four-step process, namely benefit assessment, threat index evaluation, coverage assessment, and cost analysis. This approach, however, focuses mostly on the consequence of risks rather than cost of countermeasures, whereas in our approach we capture both.

Chapman and Leng [7] describes a decision methodology to measure the economic performance of risk mitigation alternatives. The methodology is based on two kinds of analysis (baseline and sensitivity), four methods of economic evaluation, and a cost-accounting framework. The cost is broken down into several dimensions and types. The advantage is to provide a clear economic justification among mitigation alternatives. However, it does not differentiate alternatives

[2] http://www.sandia.gov/ram/

based on their suitability to mitigate risks. In other words, the methodology focuses on the cost-difference aspect, but does not take into account the benefit-difference (in terms of level of risks reduced) among alternatives.

Houmb et al. [10] introduce SecInvest, a security investment support framework which derives a security solution fitness score to compare alternatives and decide whether to invest or to take the associated risk. SecInvest relies on an eight-step trade-off analysis which employs existing risk assessment techniques for risk level. SecInvest scores alternatives with respect to their cost and effect, trade-off parameters, and investment opportunities. However, this approach does not provide a systematic way to assess the effects of alternatives on risks, and does not take into account the dependency among countermeasures in an alternative.

There exist studies on Real Options Thinking [2, 14, 15] to articulate and compare different security solutions in terms of their business value. However, these solutions are on the management aspect such as postpone, abandon, or continue to invest in security. Meanwhile, our alternatives are more focused on the technical aspect. The output of our approach could be taken as the input for Real Options Thinking based assessment.

5 Conclusion

We have presented a generic approach to select a cost-effective countermeasure alternative to mitigate risks. The approach requires input in the form of risk models represented as risk graphs. The approach analyses risk countermeasures with respect to different properties such as the amount of risk mitigation (Effects relation), how countermeasures affect others (Dependency relation), and how much countermeasures cost (Countermeasure expenditure). We have developed a formal calculus extending the existing calculus for risk graphs. The extended calculus can be used to propagate likelihoods and consequences along risk graphs, thereby facilitating a quantitative countermeasure analysis on individual risks, and a synergy analysis on all the risks. The outcome is a list of countermeasure alternatives quantitatively ranked according to the their overall cost. These alternatives are represented not only in tabular format, but also graphically in the form of decision diagrams.

We have exemplified the generic approach by embedding it within the CORAS method. The resulting CORAS approach is illustrated on an example from the eHealth domain. Notations and rules have been adapted to comply with CORAS. The example illustrates how our approach can work with existing defensive risk analysis methods whose risk models can be converted to risk graphs.

Acknowledgement

This work has received funding from the European Commission via the NESSoS NoE (256980) and the RASEN project (316853), and from the Research Council of Norway via the DIAMONDS project (201579/S10).

References

[1] M. D. Adler and E. A. Posner. *Cost-Benefit Analysis: Legal, Economic and Philosophical Perspectives*. University of Chicago Press, 2000.

[2] M. Amram and N. Kulatilaka. *Real Options: Managing Strategic Investment in an Uncertain World*. Harvard Business School Press, 1999.

[3] D. G. Birch and N. A. McEvoy. Risk analysis for information systems. *Journal of Information Technology*, 7:44–53, 1992.

[4] A. E. Boardman, D. H. Greenberg, A. R. Vining, and D. L. Weimer. *Cost-Benefit Analysis: Concepts and Practice*. Prentice Hall, 3rd edition, 2006.

[5] G. Brændeland, A. Refsdal, and K. Stølen. Modular analysis and modelling of risk scenarios with dependencies. *J. Syst. Softw.*, 83(10):1995–2013, 2010.

[6] S. A. Butler. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering (ICSE'02)*, pages 232–240. ACM, 2002.

[7] R. E. Chapman and C. J. Leng. Cost-effective responses to terrorist risks in constructed facilities. Technical report, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2004.

[8] E. Charniak. Bayesian networks without tears. *AI Magazine*, 12(4):50–63, 1991.

[9] *Risk Characterization of Microbiological Hazards in Food: Guidelines*. Microbiological Risk Assessment Series No. 17. Food and Agriculture Organization of the United Nations (FAO)/World Health Organization (WHO), 2009.

[10] S. H. Houmb, I. Ray, and I. Ray. SecInvest : Balancing security needs with financial and business constraints. In *Dependability and Computer Engineering*, pages 306–328. IGI Global, 2012.

[11] International Electrotechnical Commission. *IEC 61025 Fault Tree Analysis (FTA)*, 1990.

[12] International Electrotechnical Commission. *IEC 60300-3-9 Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems – Event Tree Analysis (ETA)*, 1995.

[13] International Organization for Standardization. *ISO 31000 Risk management – Principles and guidelines*, 2009.

[14] N. Kulatilaka, P. Balasubramanian, and J. Strock. Using real options to frame the IT investment problem. In *Real Options and Business Strategy: Applications to Decision-Making*. Risk Publications, 1999.

[15] J. Li and X. Su. Making cost effective security decision with real option thinking. In *International Conference on Software Engineering Advances (ICSEA'07)*, 2007.

[16] M. S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis: The CORAS Approach.* Springer, 2011.

[17] S. Mannan, editor. *Lees' Loss Prevention in the Process Industries*, volume 1. Elsevier Butterworth-Heinemann, 3rd edition, 2005.

[18] R. I. Mehr and S. W. Forbes. The risk management decision in the total business setting. *Journal of Risk and Insurance*, 40(10):389–401, 1973.

[19] NESSoS project. Deliverable D11.2: Selection and Documentation of the Two Major Application Case Studies. Technical report, 2011.

[20] T. L. Norman. *Risk Analysis and Security Countermeasure Selection.* CRC Press, 2010.

[21] A. Omerovic, A. Kofod-Petersen, B. Solhaug, I. Svagård, and L. M. S. Tran. Report on ESUMS Risk Analysis. Technical Report A23344, SINTEF ICT, 2012.

[22] R. M. Robinson, K. Anderson, B. Browning, G. Francis, M. Kanga, T. Millen, and C. Tillman. *Risk and Reliability – An Introductory Text.* R2A, 5th edition, 2001.

[23] J. Rumbaugh, I. Jacobson, and G. Booch. *Unified Modeling Language Reference Manual, The (2nd Edition).* Pearson Higher Education, 2004.

[24] B. Schneier. Attack trees: Modeling security threats. *Dr. Dobbs Journal*, 24(12):21–29, 1999.

[25] A. K. Sen. The discipline of cost-benefit analysis. *Journal of Legal Studies*, 29(S2):931–952, 2000.

[26] G. Stoneburner, A. Goguen, and A. Feringa. *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology, 2002. NIST Special Publication 800-30.

[27] L. M. S. Tran, B. Solhaug, and K. Stølen. An approach to select cost-effective risk countermeasures. In *Data and Applications Security and Privacy XXVII*, volume 7964 of *LNCS*, pages 266–273. Springer, 2013.

A Formal foundation

In the following we introduce the formal machinery.

A.1 Basics

$\mathbb{N}$ and $\mathbb{R}$ denote the sets of natural numbers and real numbers, respectively. We use $\mathbb{N}_0$ to denote the set of natural numbers including 0, while $\mathbb{R}^+$ denotes the set of nonnegative real numbers. This means that:

$$\mathbb{N}_0 \overset{\mathsf{def}}{=} \mathbb{N} \cup \{0\}, \quad \mathbb{R}^+ \overset{\mathsf{def}}{=} \{r \in \mathbb{R} \mid r \geq 0\}$$

For any set of elements, we use $\mathbb{P}(A)$ to denote the powerset of A.

A tuple is an element of a Cartesian product. We use π_j to extract the jth element of a tuple. Hence, if

$$(a, a') \in A \times A'$$

then $\pi_1.(a, a') = a$ and $\pi_2.(a, a') = a'$.

A.2 Sequences

By A^{∞}, A^{ω} and A^{*} we denote the set of all infinite sequences, the set of all finite and infinite sequences and the set of all finite sequences over some set of elements A, respectively. Hence, we have that

$$A^{\omega} = A^{\infty} \cup A^{*}$$

We define the functions

$$\#\_ \in A^{\omega} \to \mathbb{N}_0 \cup \{\infty\}, \quad \_[\_] \in A^{\omega} \times \mathbb{N} \to A$$

to yield the length and the nth element of a sequence. Hence, $\#s$ yields the number of elements in s, and $s[n]$ yields the nth element of s if $n \leq \#s$.

We also need functions for concatenation and filtering:

$$\_ \frown \_ \in A^{\omega} \times A^{\omega} \to A^{\omega}, \quad \_ \circledS \_ \in \mathbb{P}(A) \times A^{\omega} \to A^{\omega}$$

Concatenating two sequences implies gluing them together. Hence, $s_1 \frown s_2$ denotes a sequence of length $\#s_1 + \#s_2$ that equals s_1 if s_1 is infinite, and is prefixed by s_1 and suffixed by s_2, otherwise.

The filtering operator is used to filter away elements. $B \circledS s$ denotes the subsequence obtained from s by removing all elements in s that are not in the set B.

A.3 Timed events

$\mathbb{E}$ denotes the set of all events, while the set of all timestamps is defined by

$$\mathbb{T} \overset{\mathsf{def}}{=} \mathbb{R}^{+}$$

A timed event is an element of

$$\mathbb{E} \times \mathbb{T}$$

A.4 Histories

A history is an infinite sequence of timed events that is ordered by time and progresses beyond any finite point in time. Hence, a history is an element of:[3]

$$\begin{aligned} \mathbb{H} \overset{\mathsf{def}}{=} \{ \quad & h \in (\mathbb{E} \times \mathbb{T})^{\infty} \mid \\ & \quad \forall\, n \in \mathbb{N} : \pi_2.h[n] \leq \pi_2.h[n+1] \\ & \quad \forall\, t \in \mathbb{T} : \exists\, n \in \mathbb{N} : \pi_2.h[n] > t \quad \} \end{aligned}$$

[3] We often use indentation to represent conjunction.

The first conjunct requires the timestamp of a timed event to be at least as great as that of its predecessor. The second conjunct makes sure that time will always progress beyond any finite point in time. That is, for any timestamp t and history h there is a timed event in h whose timestamp is greater than t.

We also need a function for truncating histories

$$\_|\_ \in \mathbb{H} \times \mathbb{T} \rightarrow (\mathbb{E} \times \mathbb{T})^{*}$$

The truncation operator captures the prefix of a history up to and including a certain point in time. Hence, $h|_t$ describes the maximal prefix of h whose timed events all have timestamps less than or equal to t.

A.5 Frequencies

As explained above, we use the nonnegative real numbers to represent time. The time unit is equal to 1. For simplicity, we assume that all frequencies are per time unit. The set of frequencies F is therefore defined as follows:

$$\mathbb{F} \overset{\mathsf{def}}{=} \mathbb{R}^{+}$$

Hence, $f \in \mathbb{F}$ denotes the frequency of f occurrences per time unit.

B Risk graphs

B.1 Syntax of risk graph formulas

B.1.1 Risk graphs

A risk graph is a pair of two sets (V, R) where

$$V \subseteq \mathbb{P}(\mathbb{E}) \times \mathbb{F}, \quad R \subseteq V \times \mathbb{R}^{+} \times V$$

We refer to the elements of V as vertices and to the elements of R as relations. We use $v(f)$ to denote a vertex, while $v \xrightarrow{r} v'$ denotes a relation.

B.1.2 Vertex expressions

The set of vertex expressions is the smallest set X_V such that

$$\mathbb{P}(\mathbb{E}) \subseteq X_V, \quad v, v' \in X_V \Rightarrow v \sqcup v' \in X_V \wedge v \sqcap\!| \, v' \in X_V$$

We need a function

$$s \in X_V \rightarrow \mathbb{P}(\mathbb{E})$$

that for any vertex expression yields its set of events. Formally, s is defined recursively as follows:

$$s(v) \overset{\mathsf{def}}{=} \begin{cases} v & \text{if } v \in \mathbb{P}(\mathbb{E}) \\ s(v_1) \cup s(v_2) & \text{if } v = v_1 \sqcup v_2 \\ s(v_2) & \text{if } v = v_1 \sqcap\!| \, v_2 \end{cases}$$

B.1.3 Risk graph formula

A risk graph formula is of one of the following two forms

$$H \vdash v(f), \quad H \vdash v \xrightarrow{r} v'$$

where

- $H \in \mathbb{P}(\mathbb{H}) \setminus \varnothing$,
- $v, v' \in X_V$,
- $f \in \mathbb{F}$,
- $r \in \mathbb{R}^+$.

B.2 Semantics of risk graph formulas

We use the brackets $[\![\ \ ]\!]$ to extract the semantics of a risk graph formula. If $v \in \mathbb{P}(\mathbb{E})$ we define:

$$[\![\ H \vdash v(f)\ ]\!] \ \stackrel{\mathsf{def}}{=}$$
$$\quad \forall\, h \in H :$$
$$\qquad f = \lim_{t \to \infty} \frac{\#((v \times \mathbb{T}) \circledS (h|_t))}{t}$$

The semantics of any other risk graph formula is defined recursively as follows:

$$[\![\ H \vdash v_1 \sqcup v_2(f)\ ]\!] \ \stackrel{\mathsf{def}}{=}$$
$$\quad \exists\, f_1, f_2, f_3 \in \mathbb{F} :$$
$$\qquad [\![\ H \vdash v_1(f_1)\ ]\!]$$
$$\qquad [\![\ H \vdash v_2(f_2)\ ]\!]$$
$$\qquad [\![\ H \vdash s(v_1) \cap s(v_2)(f_3)\ ]\!]$$
$$\qquad f_1 + f_2 - f_3 \le f \le f_1 + f_2$$

$$[\![\ H \vdash v_1 \sqcap\!| \, v_2(f)\ ]\!] \ \stackrel{\mathsf{def}}{=}$$
$$\quad \exists\, r \in \mathbb{R}^+;\ f_1, f_2 \in \mathbb{F} :$$
$$\qquad [\![\ H \vdash v_1(f_1)\ ]\!]$$
$$\qquad [\![\ H \vdash v_2(f_2)\ ]\!]$$
$$\qquad f = f_1 \cdot r$$
$$\qquad f \le f_2$$

$$[\![\ H \vdash v_1 \xrightarrow{r} v_2\ ]\!] \ \stackrel{\mathsf{def}}{=}$$
$$\quad \exists\, f_1, f_2 \in \mathbb{F} :$$
$$\qquad [\![\ H \vdash v_1(f_1)\ ]\!]$$
$$\qquad [\![\ H \vdash v_2(f_2)\ ]\!]$$
$$\qquad f_2 \ge f_1 \cdot r$$

B.3 Calculus of risk graph formulas

The three rules below correspond to rules 13.10, 13.11 and 13.12 in the CORAS book, respectively. There are some minor differences. In the CORAS book the real number decorating a leads-to relation is restricted to $[0, 1]$. The statistical independence constraint in Rule 13.12 of the CORAS book is not needed.

B.3.1 Rule for leads-to

$$\frac{H \vdash v_1(f) \quad H \vdash v_1 \xrightarrow{r} v_2}{H \vdash v_1 \sqcap\!\!| \, v_2(f \cdot r)}$$

Soundness Assume

(1) $H \vdash v_1(f)$

(2) $H \vdash v_1 \xrightarrow{r} v_2$

Then

(3) $H \vdash (v_1 \sqcap\!\!| \, v_2)(f \cdot r)$

Proof: (2) implies there are $f_1, f_2 \in \mathbb{F}$ such that

(4) $[\![\ H \vdash v_1(f_1) \ ]\!]$

(5) $[\![\ H \vdash v_2(f_2) \ ]\!]$

(6) $f_2 \geq f_1 \cdot r$

(1) and (4) imply

(7) $f = f_1$

(6) and (7) imply

(8) $f_2 \geq f \cdot r$

(4), (5), (7) and (8) imply (3).

B.3.2 Rule for mutually exclusive vertices

$$\frac{H_1 \vdash v_1(f) \wedge v_2(0) \quad H_2 \vdash v_2(f) \wedge v_1(0)}{H_1 \cup H_2 \vdash v_1 \sqcup v_2(f)}$$

For simplicity we have merged four premises into two using logical conjunction.[4]

Soundness Assume

(1) $H_1 \vdash v_1(f) \wedge v_2(0)$

(2) $H_2 \vdash v_2(f) \wedge v_1(0)$

[4] Hence, $H \vdash X \wedge Y$ means $H \vdash X$ and $H \vdash Y$.

Then

(3) $H_1 \cup H_2 \vdash v_1 \sqcup v_2(f)$

Proof: (1) and (2) imply

(4) $H_1 \cap H_2 = \varnothing \vee f = 0$

(1) and (2) imply

(5) $H_1 \vdash v_1 \sqcup v_2(f)$
(6) $H_2 \vdash v_1 \sqcup v_2(f)$

(4), (5) and (6) imply (3).

B.3.3 Rule for separate vertices

$$\frac{H \vdash v_1(f_1) \quad H \vdash v_2(f_2) \quad s(v_1) \cap s(v_2) = \varnothing}{H \vdash v_1 \sqcup v_2(f_1 + f_2)}$$

Soundness Assume

(1) $H \vdash v_1(f_1)$
(2) $H \vdash v_2(f_2)$
(3) $s(v_1) \cap s(v_2) = \varnothing$

Then

(4) $H \vdash v_1 \sqcup v_2(f_1 + f_2)$

Proof: (3) implies

(5) $H \vdash s(v_1) \cap s(v_2)(0)$

(1), (2), (5) and the fact that $f_1 + f_2 - 0 \leq f_1 + f_2 \leq f_1 + f_2$ imply (4).

C Introducing countermeasures

C.1 Formal foundation extended with countermeasures

We start by extending the basic formal machinery to take countermeasures into consideration.

C.1.1 Timed events with countermeasures

$\mathbb{C}$ denotes the set of all countermeasures. To record treatments each timed event is extended with a possibly empty set of countermeasures. A timed event with an empty set of countermeasures is untreated, while a timed event with a nonempty set is treated by the countermeasures in the set. Hence, a timed event is from this point onwards an element of

$$\mathbb{E} \times \mathbb{T} \times \mathbb{P}(\mathbb{C})$$

C.1.2 Histories with countermeasures

The notion of history is generalized straightforwardly to deal with timed events with countermeasures as follows:

$$\begin{aligned} \mathbb{H} \overset{\mathsf{def}}{=} \{ \quad & h \in (\mathbb{E} \times \mathbb{T} \times \mathbb{P}(\mathbb{C}))^{\,\infty} \mid \\ & \forall\, n \in \mathbb{N} : \pi_2.h[n] \leq \pi_2.h[n+1] \\ & \forall\, t \in \mathbb{T} : \exists\, n \in \mathbb{N} : \pi_2.h[n] > t \quad \} \end{aligned}$$

The truncation operator

$$\_|\_ \in \mathbb{H} \times \mathbb{T} \to (\mathbb{E} \times \mathbb{T} \times \mathbb{P}(\mathbb{C}))^{\,*}$$

is generalized accordingly.

C.2 Syntax extended with countermeasures

The next step is to generalize the notion of risk graph.

C.2.1 Risk graphs

A risk graph with treatments is a tuple of five sets (V, C, R_l, R_e, R_d) where

$$\begin{aligned} & V \subseteq \mathbb{P}(\mathbb{E}) \times \mathbb{F}, \\ & C \subseteq \mathbb{C}, \\ & R_l \subseteq V \times \mathbb{R}^+ \times V, \\ & R_e \subseteq C \times [0,1] \times V, \\ & R_d \subseteq C \times [0,1] \times R_e \end{aligned}$$

We refer to the elements of V as the set of vertices, C as the set of countermeasures, and to R_l, R_e, R_d as the leads-to relations, the effects relations and the dependency relations, respectively.

We use $v(f)$ to denote a vertex, c to denote a countermeasure, $\xrightarrow{l}$ to denote a leads-to relation, $\xrightarrow{e}$ to denote an effects relation and $\xrightarrow{d}$ to denote a dependency relation.

C.2.2 Vertex expressions

The set of vertex expressions is the smallest set X_V such that

$$\begin{aligned} & v \in \mathbb{P}(\mathbb{E}) \wedge cs \in \mathbb{P}(\mathbb{C}) \Rightarrow v_{cs} \in X_V \\ & v, v' \in X_V \Rightarrow v \sqcup v' \in X_V \wedge v \sqcap\!\!| \; v' \in X_V \end{aligned}$$

We need a function

$$s \in X_V \rightarrow \mathbb{P}(\mathbb{E})$$

that for any vertex expression calculates its set of events. Formally, s is defined recursively as follows:

$$s(v) \overset{\mathsf{def}}{=} \begin{cases} v' & \text{if } v = v'_{cs} \\ s(v_1) \cup s(v_2) & \text{if } v = v_1 \sqcup v_2 \\ s(v_2) & \text{if } v = v_1 \sqcap\!| \, v_2 \end{cases}$$

C.2.3 Risk graph formula

A risk graph formula is of one of the following four forms

$$H \vdash c \xrightarrow{e}_{cs} v, \quad H \vdash c \xrightarrow{d} (c' \xrightarrow{e}_{cs} v), \quad H \vdash v'(f), \quad H \vdash v' \xrightarrow{r} v''$$

where

- $H \in \mathbb{P}(\mathbb{H})$,
- $c, c' \in \mathbb{C}$ where $c \neq c'$,
- $e, d \in [0, 1]$,
- $cs \in \mathbb{P}(\mathbb{C})$ where $c, c' \notin cs$,
- $v \in \mathbb{P}(\mathbb{E})$,
- $v', v'' \in X_V$,
- $f \in \mathbb{F}$,
- $r \in \mathbb{R}^+$.

C.3 Semantics extended with countermeasures

The semantics of a risk graph formula is defined recursively as before. In particular, the definitions are unchanged in the case of

$$[\![\; H \vdash v_1 \sqcup v_2(f) \;]\!], \quad [\![\; H \vdash v_1 \sqcap\!| \, v_2(f) \;]\!], \quad [\![\; H \vdash v_1 \xrightarrow{r} v_2 \;]\!]$$

The vertex base-case must however be updated to take countermeasures into account:

$$\begin{aligned} &[\![\; H \vdash v_{cs}(f) \;]\!] \overset{\mathsf{def}}{=} \\ &\qquad \forall\, h \in H : \\ &\qquad\qquad f = \lim_{t \rightarrow \infty} \tfrac{\#((v \times \mathbb{T} \times \mathbb{P}(\mathbb{C} \setminus cs)) \, \circledS \, (h|_t))}{t} \end{aligned}$$

Hence, we only take into consideration those events in v that are not treated by a countermeasure in cs.

In the case of the effects relation the semantics is defined as follows:

$$
\begin{aligned}
&[\![\ H \vdash c \xrightarrow{e}_{cs} v\ ]\!] \ \overset{\mathsf{def}}{=}\\
&\quad \exists f_1, f_2 \in \mathbb{F} :\\
&\qquad [\![\ H \vdash v_{cs}(f_1)\ ]\!]\\
&\qquad [\![\ H \vdash v_{cs\cup\{c\}}(f_2)\ ]\!]\\
&\qquad f_1 \neq 0 \Rightarrow e = \tfrac{f_1 - f_2}{f_1}
\end{aligned}
$$

Hence, e is the fraction of v events whose set of countermeasures contains c but no countermeasure in cs.

Also the dependency relation captures a fraction:

$$
\begin{aligned}
&[\![\ H \vdash c \xrightarrow{d} (c' \xrightarrow{e}_{cs} v)\ ]\!] \ \overset{\mathsf{def}}{=}\\
&\quad [\![\ H \vdash c' \xrightarrow{e}_{cs} v\ ]\!] \Rightarrow\\
&\qquad \exists\, e' \in [0,1] :\\
&\qquad\quad [\![\ H \vdash c' \xrightarrow{e'}_{cs\cup\{c\}} v\ ]\!]\\
&\qquad\quad e \neq 0 \Rightarrow d = 1 - \tfrac{e'}{e}
\end{aligned}
$$

Hence, d is the fraction of v events treated by countermeasure c' that is also treated by countermeasure c.

C.4 Calculus extended with countermeasures

C.4.1 Rule for countermeasure effect

$$\frac{H \vdash c \xrightarrow{e}_{cs} v \quad H \vdash v_{cs}(f)}{H \vdash v_{cs\cup\{c\}}(f \cdot \overline{e})}$$

Soundness Assume

(1) $H \vdash c \xrightarrow{e}_{cs} v$

(2) $H \vdash v_{cs}(f)$

Then

(3) $H \vdash v_{cs\cup\{c\}}(f \cdot \overline{e})$

Proof: (1) implies there are $f_1, f_2 \in \mathbb{F}$ such that

(4) $[\![\ H \vdash v_{cs}(f_1)\ ]\!]$

(5) $[\![\ H \vdash v_{cs\cup\{c\}}(f_2)\ ]\!]$

(6) $f_1 \neq 0 \Rightarrow e = \frac{f_1 - f_2}{f_1}$

(2) and (4) imply

(7) $f = f_1$

There are two cases to consider:

- Assume

  (8) $f_1 = 0$

  (4), (7) and (8) imply

  (9) $[\![\ H \vdash v_{cs \cup \{c\}}(0) \ ]\!]$

  (7) and (8) imply

  (10) $f = 0$

  (9), (10) and $0 \cdot \overline{e} = 0$ imply (3).

- Assume

  (11) $f_1 \neq 0$

  (6), (7) and (11) imply

  (12) $e = \frac{f - f_2}{f}$

  (12) implies

  (13) $\frac{f_2}{f} = 1 - e$

  (13) implies

  (14) $f_2 = f \cdot \overline{e}$

  (5) and (14) imply (3).

C.4.2 Rule for countermeasure dependency

$$\frac{H \vdash c \xrightarrow{d} (c' \xrightarrow{e}_{cs} v) \quad H \vdash c' \xrightarrow{e}_{cs} v}{H \vdash c' \xrightarrow{e \cdot \overline{d}}_{cs \cup \{c\}} v}$$

Soundness Assume

(1) $H \vdash c \xrightarrow{d} (c' \xrightarrow{e}_{cs} v)$
(2) $H \vdash c' \xrightarrow{e}_{cs} v$

Then

(3) $H \vdash c' \xrightarrow{e \cdot \overline{d}}_{cs \cup \{c\}} v$

Proof: There are two cases to consider:

- Assume

  (4) $e \neq 0$

  (1), (2) and (4) imply there is $e' \in [0,1]$ such that

  (5) $[\![\ H \vdash c' \xrightarrow{e'}_{cs \cup \{c\}} v \ ]\!]$
  (6) $d = 1 - \frac{e'}{e}$

  (6) implies

  (7) $\frac{e'}{e} = 1 - d = \overline{d}$

  (5) and (7) imply (3).

- Assume

  (8) $e = 0$

  (2) implies there are $f_1, f_2 \in \mathbb{F}$ such that

  (9) $[\![\ H \vdash v_{cs}(f_1) \ ]\!]$
  (10) $[\![\ H \vdash v_{cs \cup \{c'\}}(f_2) \ ]\!]$
  (11) $f_1 \neq 0 \Rightarrow e = \frac{f_1 - f_2}{f_1}$

  Again, there are two cases to consider:

  - Assume

    (12) $f_1 = 0$

    (9) and (12) imply

    (13) $[\![\ H \vdash v_{cs \cup cs'}(0) \ ]\!]$

    for arbitrary cs'. This implies (3).

  - Assume

    (14) $f_1 \neq 0$

    (8), (11) and (14) imply that $f_1 = f_2$ which means that the treatment c' has no effect in addition to the effect of cs. This implies (3).

D Introducing consequences

D.1 Formal foundation extended with consequences

We start by extending the basic formal machinery to take consequences into consideration.

D.1.1 Timed events with consequences

$\mathbb{I}$ denotes the set of all consequences (or impacts). To facilitate arithmetic operations on consequences we assume that

$$\mathbb{I} \overset{\mathsf{def}}{=} \mathbb{R}^+$$

To record consequences each timed event is extended with an additional component characterizing the consequence of this event with respect to the various combinations of countermeasures. A timed event is from this point onwards an element of

$$\mathbb{E} \times \mathbb{T} \times \mathbb{P}(\mathbb{C}) \times (\mathbb{P}(\mathbb{C}) \to \mathbb{I})$$

For any timed event e we require

$$c \subseteq c' \Rightarrow (\pi_4.e)(c) \geq (\pi_4.e)(c')$$

Hence, adding a countermeasure will never increase the consequence.

D.1.2 Histories with consequences

The notion of history is generalized straightforwardly to deal with consequences as follows:

$$\begin{array}{lll} \mathbb{H} \overset{\mathsf{def}}{=} \{ & h \in (\mathbb{E} \times \mathbb{T} \times \mathbb{P}(\mathbb{C}) \times (\mathbb{P}(\mathbb{C}) \to \mathbb{I}))^{\,\infty} \mid & \\ & \quad \forall\, n \in \mathbb{N} : \pi_2.h[n] \leq \pi_2.h[n+1] & \\ & \quad \forall\, t \in \mathbb{T} : \exists\, n \in \mathbb{N} : \pi_2.h[n] > t & \} \end{array}$$

The truncation operator

$$\_|\_ \in \mathbb{H} \times \mathbb{T} \to (\mathbb{E} \times \mathbb{T} \times \mathbb{P}(\mathbb{C}) \times (\mathbb{P}(\mathbb{C}) \to \mathbb{I}))^{\,*}$$

is generalized accordingly.

D.2 Syntax extended with consequences

The next step is to generalize the notion of risk graph.

D.2.1 Risk graphs

The notion of risk graph is a tuple of five sets (V, C, R_l, R_e, R_d) where

$$V \subseteq \mathbb{P}(\mathbb{E}) \times \mathbb{F} \times \mathbb{I},$$
$$C \subseteq \mathbb{C},$$
$$R_l \subseteq V \times \mathbb{R}^+ \times V,$$
$$R_e \subseteq C \times [0,1] \times [0,1] \times V,$$
$$R_d \subseteq C \times [0,1] \times [0,1] \times R_e$$

We use $v(f, i)$ to denote a vertex, $\xrightarrow{(e_f, e_i)}$ to denote an effects relation and $\xrightarrow{(d_f, d_i)}$ to denote a dependency relation. The remaining conventions are as before.

D.2.2 Vertex expressions

The notion of vertex expression is left unchanged.

D.2.3 Risk graph formula

A risk graph formula is of one of the following four forms

$$H \vdash c \xrightarrow{(e_f, e_i)}_{cs} v, \quad H \vdash c \xrightarrow{(d_f, d_i)} (c' \xrightarrow{(e_f, e_i)}_{cs} v), \quad H \vdash v'(f, i), \quad H \vdash v' \xrightarrow{r} v''$$

where

- $H \in \mathbb{P}(\mathbb{H})$,
- $c, c' \in \mathbb{C}$ where $c \neq c'$,
- $e_f, e_i, d_f, d_i \in [0, 1]$,
- $cs \in \mathbb{P}(\mathbb{C})$ where $c, c' \notin cs$,
- $v \in \mathbb{P}(\mathbb{E})$,
- $v', v'' \in X_V$,
- $f \in \mathbb{F}$,
- $i \in \mathbb{I}$,
- $r \in \mathbb{R}^+$.

D.3 Semantics extended with consequences

```
$[\![ \ H \vdash v_{cs}(f, i) \ ]\!] \overset{\mathsf{def}}{=}$
    $\forall\, h \in H :$
        let
            $x = (v \times \mathbb{T} \times \mathbb{P}(\mathbb{C} \setminus cs) \times (\mathbb{P}(\mathbb{C}) \rightarrow \mathbb{I})) \circledS h$
        in
            $\#x = 0 \Rightarrow$
                $f = 0$
                $i = 0$
            $\#x \neq 0 \Rightarrow$
                $f = \lim_{t \rightarrow \infty} \frac{\#(x|_t)}{t}$
                $i = \lim_{t \rightarrow \infty} \frac{\sum_{1 \leq j \leq \#(x|_t)} \pi_4 . x[j](cs)}{\#(x|_t)}$
```

$$
\begin{aligned}
&[\![\ H \vdash v_1 \sqcup v_2(f, i)\ ]\!] \ \overset{\mathsf{def}}{=} \\
&\qquad \exists\, f_1, f_2, f_3 \in \mathbb{F} : \\
&\qquad\qquad [\![\ H \vdash v_1(f_1, i)\ ]\!] \\
&\qquad\qquad [\![\ H \vdash v_2(f_2, i)\ ]\!] \\
&\qquad\qquad [\![\ H \vdash s(v_1) \cap s(v_2)(f_3, i)\ ]\!] \\
&\qquad\qquad f_1 + f_2 - f_3 \le f \le f_1 + f_2
\end{aligned}
$$

$$
\begin{aligned}
&[\![\ H \vdash v_1 \sqcap\!\shortmid v_2(f, i)\ ]\!] \ \overset{\mathsf{def}}{=} \\
&\qquad \exists\, r \in \mathbb{R}^+;\ f_1, f_2 \in \mathbb{F};\ i' \in \mathbb{I} : \\
&\qquad\qquad [\![\ H \vdash v_1(f_1, i')\ ]\!] \\
&\qquad\qquad [\![\ H \vdash v_2(f_2, i)\ ]\!] \\
&\qquad\qquad f = f_1 \cdot r \\
&\qquad\qquad f \le f_2
\end{aligned}
$$

$$
\begin{aligned}
&[\![\ H \vdash v_1 \xrightarrow{r} v_2\ ]\!] \ \overset{\mathsf{def}}{=} \\
&\qquad \exists\, f_1, f_2 \in \mathbb{F};\ i_1, i_2 \in \mathbb{I} : \\
&\qquad\qquad [\![\ H \vdash v_1(f_1, i_1)\ ]\!] \\
&\qquad\qquad [\![\ H \vdash v_2(f_2, i_2)\ ]\!] \\
&\qquad\qquad f_2 \ge f_1 \cdot r
\end{aligned}
$$

$$
\begin{aligned}
&[\![\ H \vdash c \xrightarrow{(e_f, e_i)}_{cs} v\ ]\!] \ \overset{\mathsf{def}}{=} \\
&\qquad \exists\, f_1, f_2 \in \mathbb{F};\ i_1, i_2 \in \mathbb{I} : \\
&\qquad\qquad [\![\ H \vdash v_{cs}(f_1, i_1)\ ]\!] \\
&\qquad\qquad [\![\ H \vdash v_{cs \cup \{c\}}(f_2, i_2)\ ]\!] \\
&\qquad\qquad f_1 \ne 0 \Rightarrow e_f = \tfrac{f_1 - f_2}{f_1} \\
&\qquad\qquad i_1 \ne 0 \Rightarrow e_i = \tfrac{i_1 - i_2}{i_1}
\end{aligned}
$$

$$
\begin{aligned}
&[\![\ H \vdash c \xrightarrow{(d_f, d_i)} (c' \xrightarrow{(e_f, e_i)}_{cs} v)\ ]\!] \ \overset{\mathsf{def}}{=} \\
&\qquad [\![\ H \vdash c' \xrightarrow{(e_f, e_i)}_{cs} v\ ]\!] \Rightarrow \\
&\qquad\qquad \exists\, e'_f, e'_i \in [0, 1] : \\
&\qquad\qquad\qquad [\![\ H \vdash c' \xrightarrow{(e'_f, e'_i)}_{cs \cup \{c\}} v\ ]\!] \\
&\qquad\qquad\qquad e_f \ne 0 \Rightarrow d_f = 1 - \tfrac{e'_f}{e_f} \\
&\qquad\qquad\qquad e_i \ne 0 \Rightarrow d_i = 1 - \tfrac{e'_i}{e_i}
\end{aligned}
$$

D.4 Calculus extended with consequences

D.4.1 Rule for leads-to

$$\frac{H \vdash v_1(f_1, i_1) \quad H \vdash v_1 \xrightarrow{r} v_2 \quad H \vdash v_2(f_2, i_2)}{H \vdash v_1 \sqcap\!\!| \; v_2(f_1 \cdot r, i_2)}$$

Soundness We need an additional premise to conclude that i_2 is the impact of v_2. Except for that the introduction of consequences is irrelevant for the validity of the rule. Hence, the soundness follows from the soundness of Rule B.3.1.

D.4.2 Rule for mutually exclusive vertices

$$\frac{H_1 \vdash v_1(f, i) \wedge v_2(0, i) \quad H_2 \vdash v_2(f, i) \wedge v_1(0, i)}{H_1 \cup H_2 \vdash v_1 \sqcup v_2(f, i)}$$

Soundness The introduction of consequences is irrelevant for the validity of the rule. Hence, the soundness follows from the soundness of Rule B.3.2.

D.4.3 Rule for separate vertices

$$\frac{H \vdash v_1(f_1, i) \quad H \vdash v_2(f_2, i) \quad s(v_1) \cap s(v_2) = \varnothing}{H \vdash v_1 \sqcup v_2(f_1 + f_2, i)}$$

Soundness The introduction of consequences is irrelevant for the validity of the rule. Hence, the soundness follows from the soundness of Rule B.3.3.

D.4.4 Rule for countermeasure effect

$$\frac{H \vdash c \xrightarrow{(e_f, e_i)}_{cs} v \quad H \vdash v_{cs}(f, i)}{H \vdash v_{cs \cup \{c\}}(f \cdot \overline{e_f}, i \cdot \overline{e_i})}$$

Soundness Assume

(1) $H \vdash c \xrightarrow{(e_f, e_i)}_{cs} v$

(2) $H \vdash v_{cs}(f, i)$

Then

(3) $H \vdash v_{cs \cup \{c\}}(f \cdot \overline{e_f}, i \cdot \overline{e_i})$

Proof: The soundness of the frequency deduction follows from the soundness of Rule C.4.1. Hence, we focus only on the consequence deduction. (1) implies there are $f_1, f_2 \in \mathbb{F}$ and $i_1, i_2 \in \mathbb{I}$ such that

(4) $[\![\ H \vdash v_{cs}(f_1, i_1)\ ]\!]$

(5) $[\![\ H \vdash v_{cs\cup\{c\}}(f_2, i_2)\ ]\!]$

(6) $i_1 \neq 0 \Rightarrow e_i = \frac{i_1 - i_2}{i_1}$

(2) and (4) imply

(7) $i = i_1$

There are two cases to consider:

- Assume

  (8) $i_1 = 0$

  (4), (5) and (7) imply

  (9) $[\![\ H \vdash v_{cs\cup\{c\}}(f_2, 0)\ ]\!]$

  (7) and (8) imply

  (10) $i = 0$

  (9), (10) and $0 \cdot \overline{e_i} = 0$ imply (3).

- Assume

  (11) $i_1 \neq 0$

  (6), (7) and (11) imply

  (12) $e_i = \frac{i - i_2}{i}$

  (12) implies

  (13) $\frac{i_2}{i} = 1 - e_i$

  (13) implies

  (14) $i_2 = i \cdot \overline{e_i}$

  (5) and (14) imply (3).

D.4.5 Rule for countermeasure dependency

$$\frac{H \vdash c \xrightarrow{(d_f, d_i)} (c' \xrightarrow{(e_f, e_i)}_{cs} v) \quad H \vdash c' \xrightarrow{(e_f, e_i)}_{cs} v}{H \vdash c' \xrightarrow{(e_f \cdot \overline{d_f}, e_i \cdot \overline{d_i})}_{cs\cup\{c\}} v}$$

Soundness Assume

$$\begin{array}{ll} (1) & H \vdash c \xrightarrow{(d_f, d_i)} (c' \xrightarrow{(e_f, e_i)}_{cs} v) \\ (2) & H \vdash c' \xrightarrow{(e_f, e_i)}_{cs} v \end{array}$$

Then

$$(3) \quad H \vdash c' \xrightarrow{(e_f \cdot \overline{d_f}, e_i \cdot \overline{d_i})}_{cs \cup \{c\}} v$$

Proof: The soundness of the frequency deduction follows from the soundness of Rule D.4.5. Hence, we focus only on the consequence deduction. There are two cases to consider:

- Assume

  $$(4) \quad e_i \neq 0$$

  (1), (2) and (4) imply there are $e_f', e_i' \in [0, 1]$ such that

  $$\begin{array}{ll} (5) & [\![\ H \vdash c' \xrightarrow{(e_f', e_i')}_{cs \cup \{c\}} v \ ]\!] \\ (6) & d_i = 1 - \frac{e_i'}{e_i} \end{array}$$

  (6) implies

  $$(7) \quad \frac{e_i'}{e_i} = 1 - d_i = \overline{d_i}$$

  (5) and (7) imply (3).

- Assume

  $$(8) \quad e_i = 0$$

  (2), (8) and the constraint that adding a countermeasure will never increase the consequence imply (3).

E Introducing intervals

E.1 Syntax extended with intervals

The syntax is as before with the exception that we now have intervals where we earlier had singular values.

E.2 Semantics extended with intervals

The semantics is generalized to intervals in a point-wise manner:

$$\begin{array}{l} [\![\ H \vdash v_{cs}(F, I) \ ]\!] \overset{\text{def}}{=} \\ \qquad \forall\, h \in H;\ \exists f \in F;\ i \in I : \\ \qquad\qquad [\![\ \{h\} \vdash v_{cs}(f, i) \ ]\!] \end{array}$$

$$\begin{aligned}
&\llbracket\, H \vdash v_1 \sqcup v_2(F, I) \,\rrbracket \overset{\mathsf{def}}{=} \\
&\qquad \forall\, h \in H;\ \exists\, f \in F;\ i \in I : \\
&\qquad\qquad \llbracket\, \{h\} \vdash v_1 \sqcup v_2(f, i) \,\rrbracket
\end{aligned}$$

$$\begin{aligned}
&\llbracket\, H \vdash v_1 \sqcap\!| \, v_2(F, I) \,\rrbracket \overset{\mathsf{def}}{=} \\
&\qquad \forall\, h \in H;\ \exists\, f \in F;\ i \in I : \\
&\qquad\qquad \llbracket\, \{h\} \vdash v_1 \sqcap\!| \, v_2(f, i) \,\rrbracket
\end{aligned}$$

$$\begin{aligned}
&\llbracket\, H \vdash v_1 \xrightarrow{R} v_2 \,\rrbracket \overset{\mathsf{def}}{=} \\
&\qquad \forall\, h \in H;\ \exists\, r \in R : \\
&\qquad\qquad \llbracket\, \{h\} \vdash v_1 \xrightarrow{r} v_2 \,\rrbracket
\end{aligned}$$

$$\begin{aligned}
&\llbracket\, H \vdash c \xrightarrow{(E_F, E_I)}_{cs} v \,\rrbracket \overset{\mathsf{def}}{=} \\
&\qquad \forall\, h \in H;\ \exists\, e_f \in E_F, e_i \in E_I : \\
&\qquad\qquad \llbracket\, \{h\} \vdash c \xrightarrow{(e_f, e_i)}_{cs} v \,\rrbracket
\end{aligned}$$

$$\begin{aligned}
&\llbracket\, H \vdash c \xrightarrow{(D_F, D_I)} (c' \xrightarrow{(E_F, E_I)}_{cs} v) \,\rrbracket \overset{\mathsf{def}}{=} \\
&\qquad \forall\, h \in H;\ \exists\, d_f \in D_F;\ d_i \in D_I;\ e_f \in E_F;\ e_i \in E_I : \\
&\qquad\qquad \llbracket\, \{h\} \vdash c \xrightarrow{(d_f, d_i)} (c' \xrightarrow{(e_f, e_i)}_{cs} v) \,\rrbracket
\end{aligned}$$

E.3 Calculus extended with intervals

E.3.1 Rule for leads-to

$$\frac{H \vdash v_1(F_1, I_1) \quad H \vdash v_1 \xrightarrow{R} v_2 \quad H \vdash v_2(F_2, I_2)}{H \vdash v_1 \sqcap\!| \, v_2(F_1 \cdot R, I_2)}$$

Soundness By pointwise application of Rule D.4.1.

E.3.2 Rule for mutually exclusive vertices

$$\frac{H_1 \vdash v_1(F, I) \wedge v_2(\{0\}, I) \quad H_2 \vdash v_2(F, I) \wedge v_1(\{0\}, I)}{H_1 \cup H_2 \vdash v_1 \sqcup v_2(F, I)}$$

Soundness By pointwise application of Rule D.4.2.

E.3.3 Rule for separate vertices

$$\frac{H \vdash v_1(F_1, I) \quad H \vdash v_2(F_2, I) \quad s(v_1) \cap s(v_2) = \varnothing}{H \vdash v_1 \sqcup v_2(F_1 + F_2, I)}$$

Soundness By pointwise application of Rule D.4.3.

E.3.4 Rule for countermeasure effect

$$\frac{H \vdash c \xrightarrow{(E_F,E_I)}_{cs} v \quad H \vdash v_{cs}(F,I)}{H \vdash v_{cs\cup\{c\}}(F \cdot \overline{E_F}, I \cdot \overline{E_I})}$$

Soundness By pointwise application of Rule D.4.4.

E.3.5 Rule for countermeasure dependency

$$\frac{H \vdash c \xrightarrow{(D_F,D_I)} (c' \xrightarrow{(E_F,E_I)}_{cs} v) \quad H \vdash c' \xrightarrow{(E_F,E_I)}_{cs} v}{H \vdash c' \xrightarrow{(E_F\cdot\overline{D_F},E_I\cdot\overline{D_I})}_{cs\cup\{c\}} v}$$

Soundness By pointwise application of Rule D.4.5.

E.3.6 Rule for arbitrary vertices

$$\frac{H \vdash v_1(F_1,I) \quad H \vdash v_2(F_2,I)}{H \vdash v_1 \sqcup v_2([\mathsf{max}(\{\mathsf{min}(F_1),\mathsf{min}(F_2)\}),\mathsf{max}(F_1)+\mathsf{max}(F_2)],I)}$$

Soundness The upper bound corresponds to the case where the set of events of the two vertices in a history are disjoint, while the lower bound corresponds to the case where the set of events in a history belonging to one of the vertices is fully contained in the history's set of events belonging to the other vertex.

F Relating CORAS to risk graphs

We distinguish between two kinds of CORAS elements, namely the set $\mathbb{E}_{UI}$ of unwanted elements, and the set $\mathbb{E}_{TS}$ of scenario elements. We assume that

$$\mathbb{E}_{UI} \cap \mathbb{E}_{TS} = \varnothing$$

We refer to the sequences in ${\mathbb{E}_{TS}}^*$ as the threat scenarios elements. An unwanted incident in CORAS may be thought of as a set of unwanted elements, while a threat scenario corresponds to a set of threat scenario elements.

A timed CORAS event is a quadruple of the following type

$$(\mathbb{E}_{UI} \cup {\mathbb{E}_{TS}}^*) \times \mathbb{T} \times \mathbb{P}(\mathbb{C}) \times (\mathbb{P}(\mathbb{C}) \rightarrow \mathbb{I})$$

While an unwanted incident element is instantaneous a threat scenario element is not. The timestamp of a threat scenario element denotes its time of termination. In CORAS only unwanted incidents may have a consequence. Hence, in the case of threat scenario elements, any set of countermeasures is mapped to 0.

The relationship between a timed CORAS event and a timed risk graph event is defined by a function *map* such that

$$map(e, t, co, im) \overset{\mathsf{def}}{=} (m(e), t, co, im)$$

where

$$m \in \mathbb{E}_{UI} \cup \mathbb{E}_{TS}{}^{*} \rightarrow \mathbb{E}$$

is a bijective function. This means that

$$m(e) = m(e') \Rightarrow e = e'$$