Risk Ontology and Service Risk Descriptor Shared Among Critical Infrastructures

CRITIS 2010
5TH INTERNATIONAL CONFERENCE ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY
SEPTEMBER 23-24, 2010, ATHENS, GREECE

Matthieu Aubigny[1] , Carlo Harpes [1], Marco Castrucci[2].

1: [aubigny, harpes]@itrust.lu ; 2: [castrucci]@dis.uniroma1.it

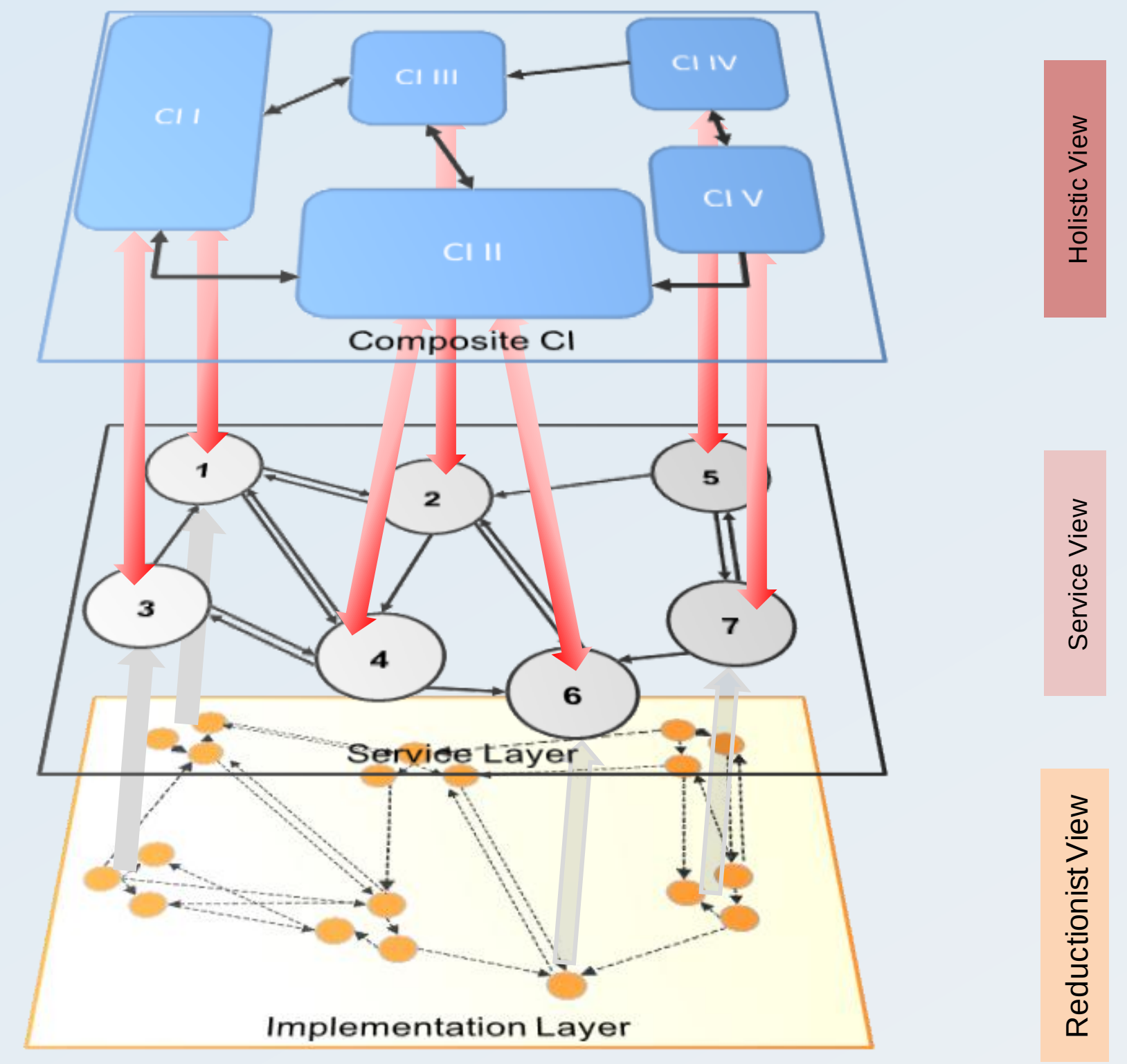
MICIE
SEVENTH FRAMEWORK PROGRAMME

Abstract

Due to their technological interdependencies, Critical Infrastructures (CIs), which represents essential assets for the functioning of contemporary societies, have to ensure the highest security levels to be able of fulfil their duty in any circumstances. This is the main goal of MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures), an FP7 ICT-SEC project: the design and implementation of a real-time CI risk level prediction and alerting system. In order to reach this objective, CIs have to exchange relevant information on their own risk in order to avoid risk cascading. The main problem is to choose what type of information can be shared without compromising commercial interest or specific security issues. This paper presents the definition of a Service Quality Descriptor (SQD) able to specify the degradation of Quality of Service of CIs and maintaining the balance between transparency and confidentiality issues. The SQD could be shared in real time and contains risk predictions, so that this information could be useful to avoid failures, identify interdependencies, or accelerate and coordinate power failure recoveries and service restoration.

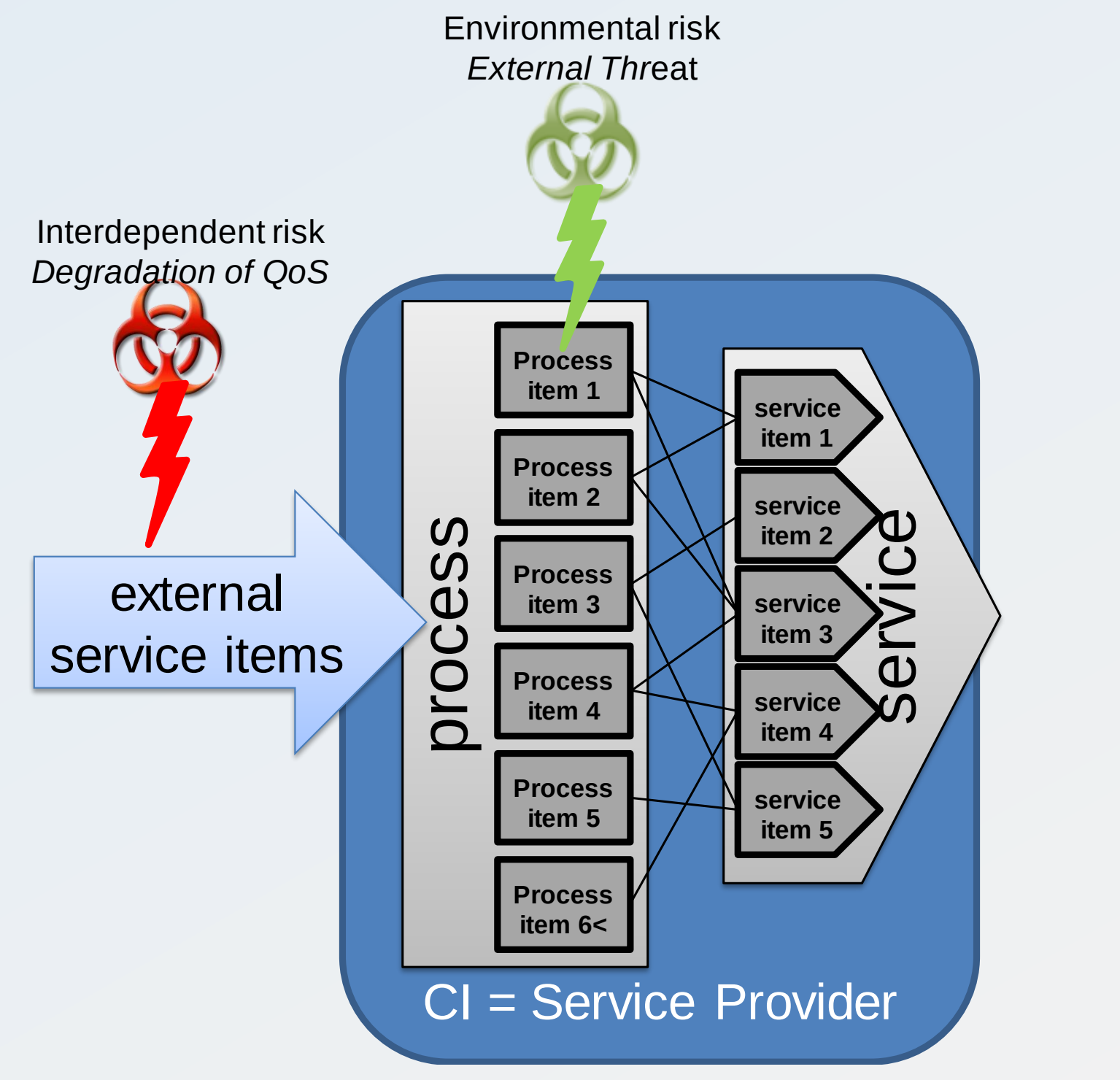
Risk Ontology in Composite CI system

Risk assessment at service layer level



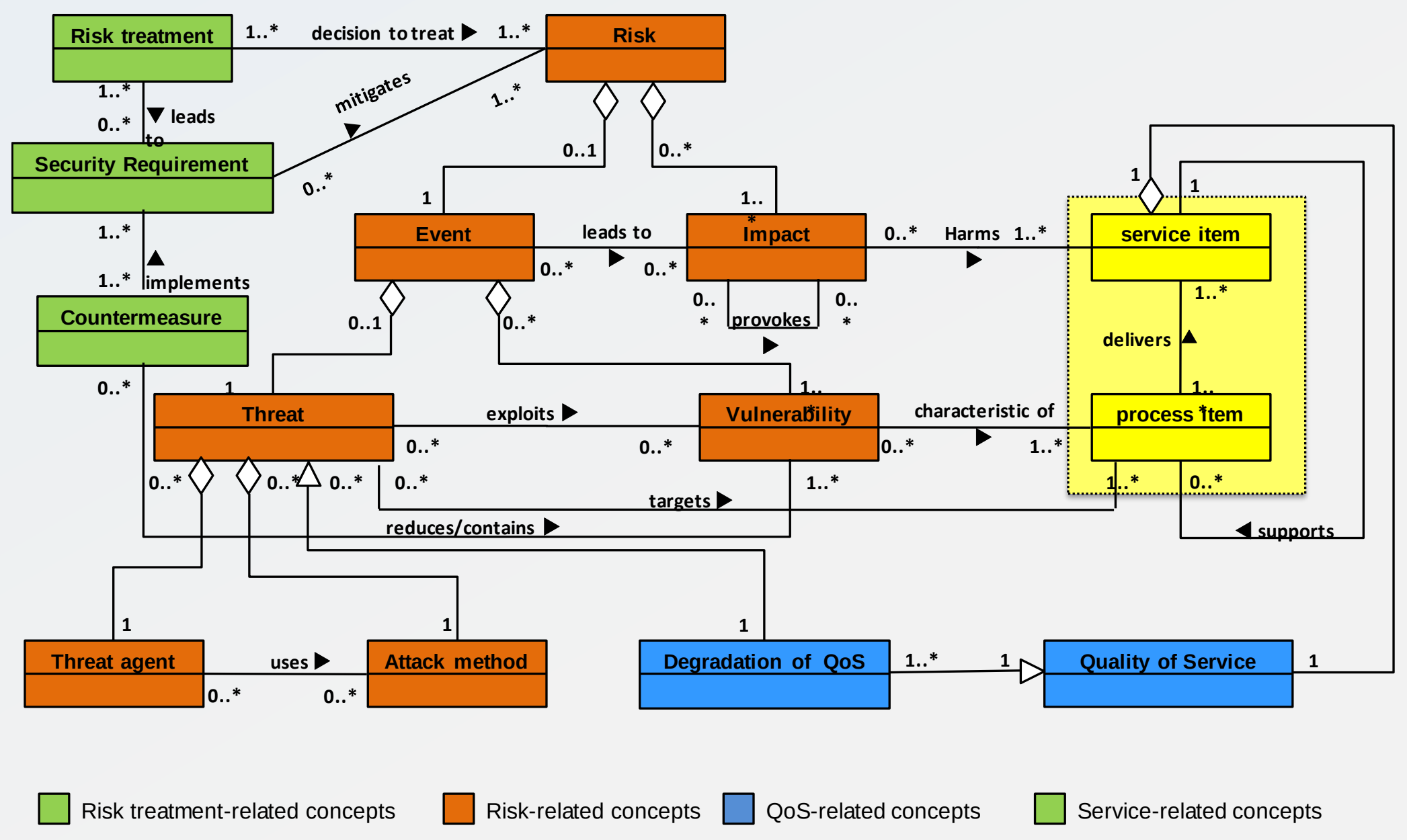
CI Modelling as service provider i.e.

- ❑ the set of process items needed to realise the main process of the CI;
- ❑ the set of service items provided by the CI to deliver its main service;
- ❑ the set of external services used by the CI to deliver its main service.



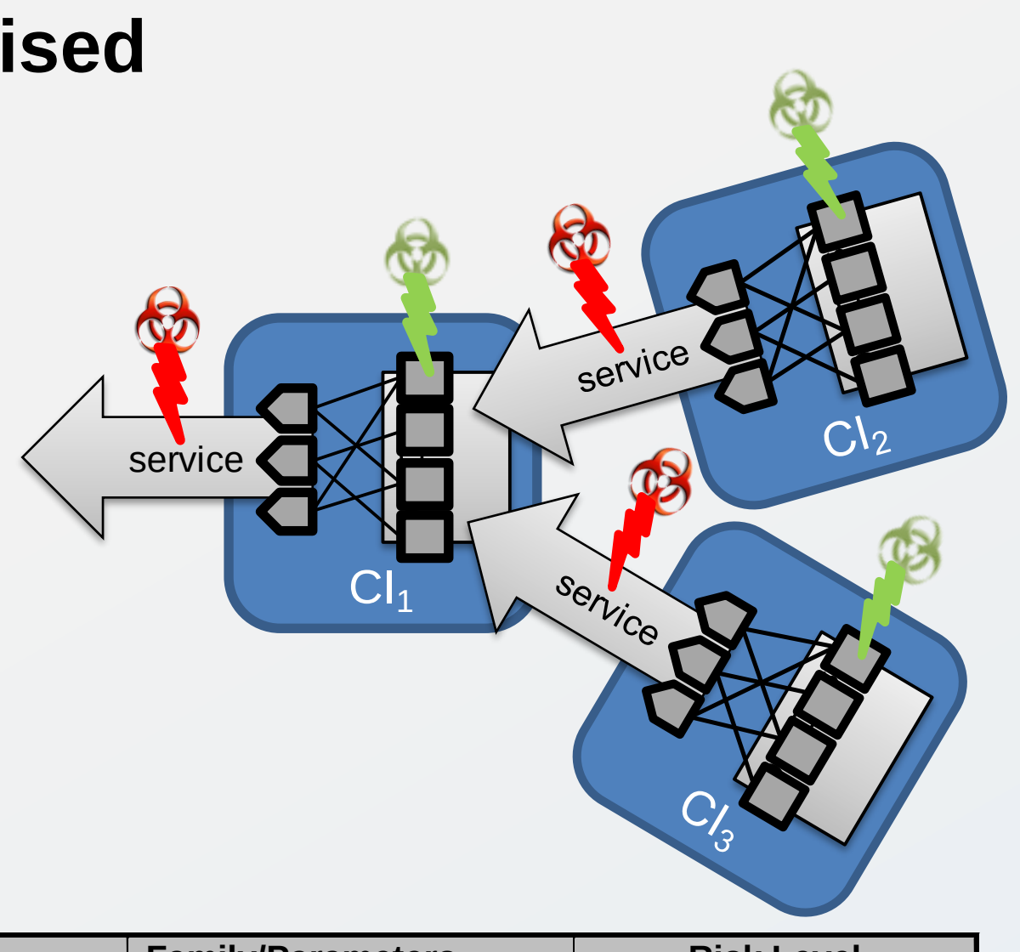
Risk Ontology based on the notion of QoS degradation describing

- ❑ environmental risk i.e. mixed between external threat and vulnerability of the service
- ❑ interdependency risk bound with the degradation of the needed external services.



Computing the risk level of a CI

The SRD value allows assigning all the time a normalised risk level of one CI in three steps:



❑ **Compute** values of the SQD parameters according to some mathematical prediction model, e.g. as linear function of the SQDs of interconnected CI, whose coefficients depend on the status of the CI.

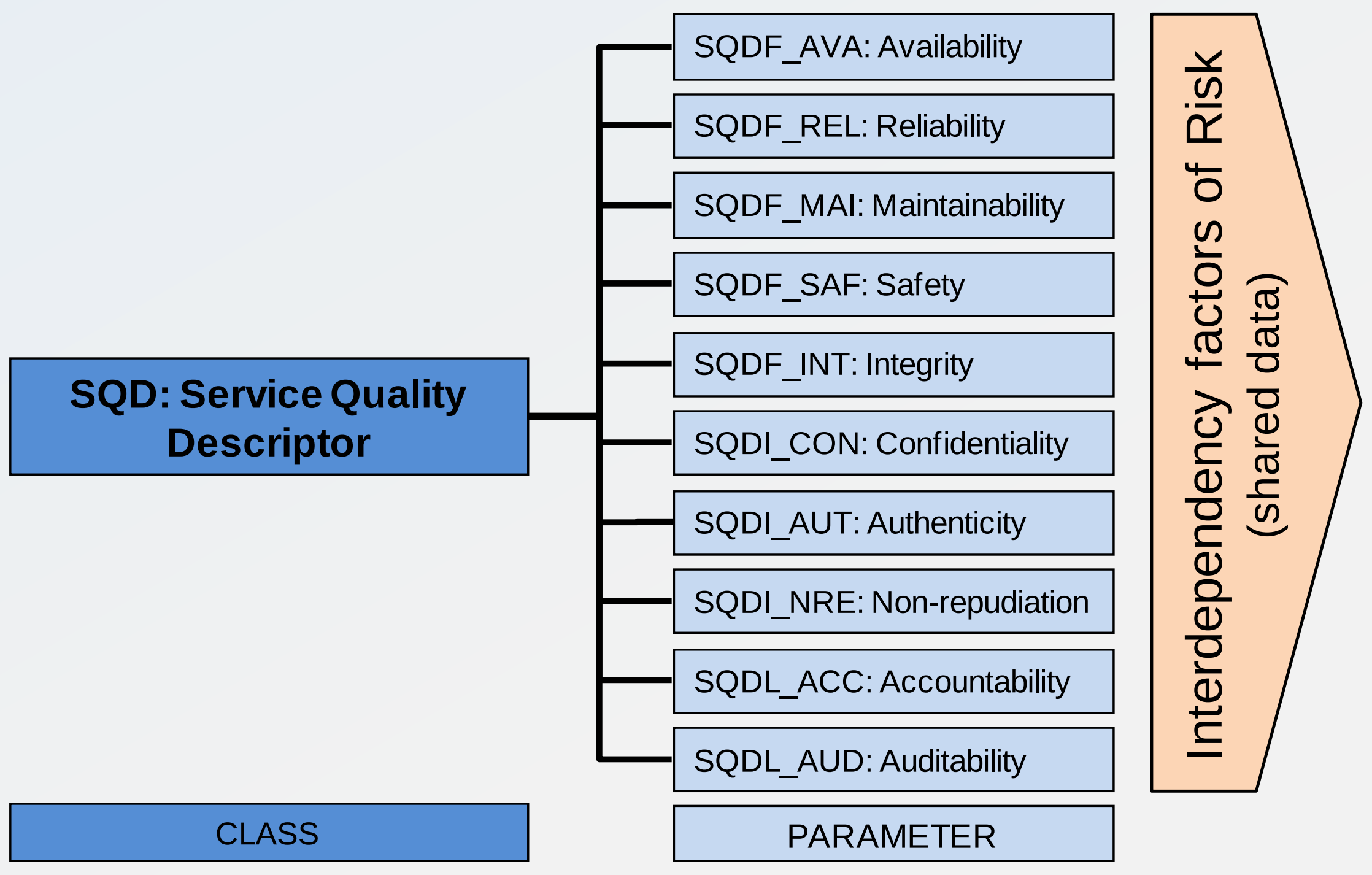
❑ **Map** the values onto a discreet risk level based on some thresholds.

❑ **Aggregate**, i.e., find the overall risk level by using the table beneath as function of the discreet risk levels of each aspect (similar approach as in ISO 15408). The risk level is assessed from 1 (low risk level) to 7 (very high risk level).

Service Quality Descriptor [SQD]	Class	Family/Parameters	Risk Level						
			1	2	3	4	5	6	7
	Class TH: Threat	TH_FT: Fault	1	2	3	3	4	4	4
		TH_ER: Error		1	2	3	3	3	3
		TH_FR: Failures			1	2	3	4	5
	Class SD: Service Dependability	SD_AVA: Availability	1	2	3	4	5	6	7
		SD_REL: Reliability	1	1	2	2	3	4	4
		SD_MAI: Maintainability	1	1	2	2	3	4	4
		SD_SAF: Safety	1	1	2	2	3	4	4
		SD_CON: Confidentiality	1	1	2	2	3	4	4
		SD_INT: Integrity	1	1	2	2	3	4	4
		SD_ACC: Accountability	1	1	2	2	3	4	5
		SD_AUT: Authenticity	1	1	2	2	3	4	5
		SD_NRE: Non repudiation	1	1	2	2	3	4	5
		SD_AUD: Auditability	1	1	2	2	3	4	5
	Class FM: Fault Mitigation	FM_PR: Fault Prevention	1	1	2	2	3	3	4
		FM_TO: Fault Tolerance	1	1	2	2	3	3	4
		FM_RE: Fault Removable	1	1	2	2	3	3	4
		FM_FO: Fault Forecasting	1	1	2	2	3	3	4

Service Quality Descriptor

The SQD is an data structure to exchange risk descriptions among CI operators.



Sharing options

- ❑ Information is shared with every partner
- ❑ Information is shared only with neighbours

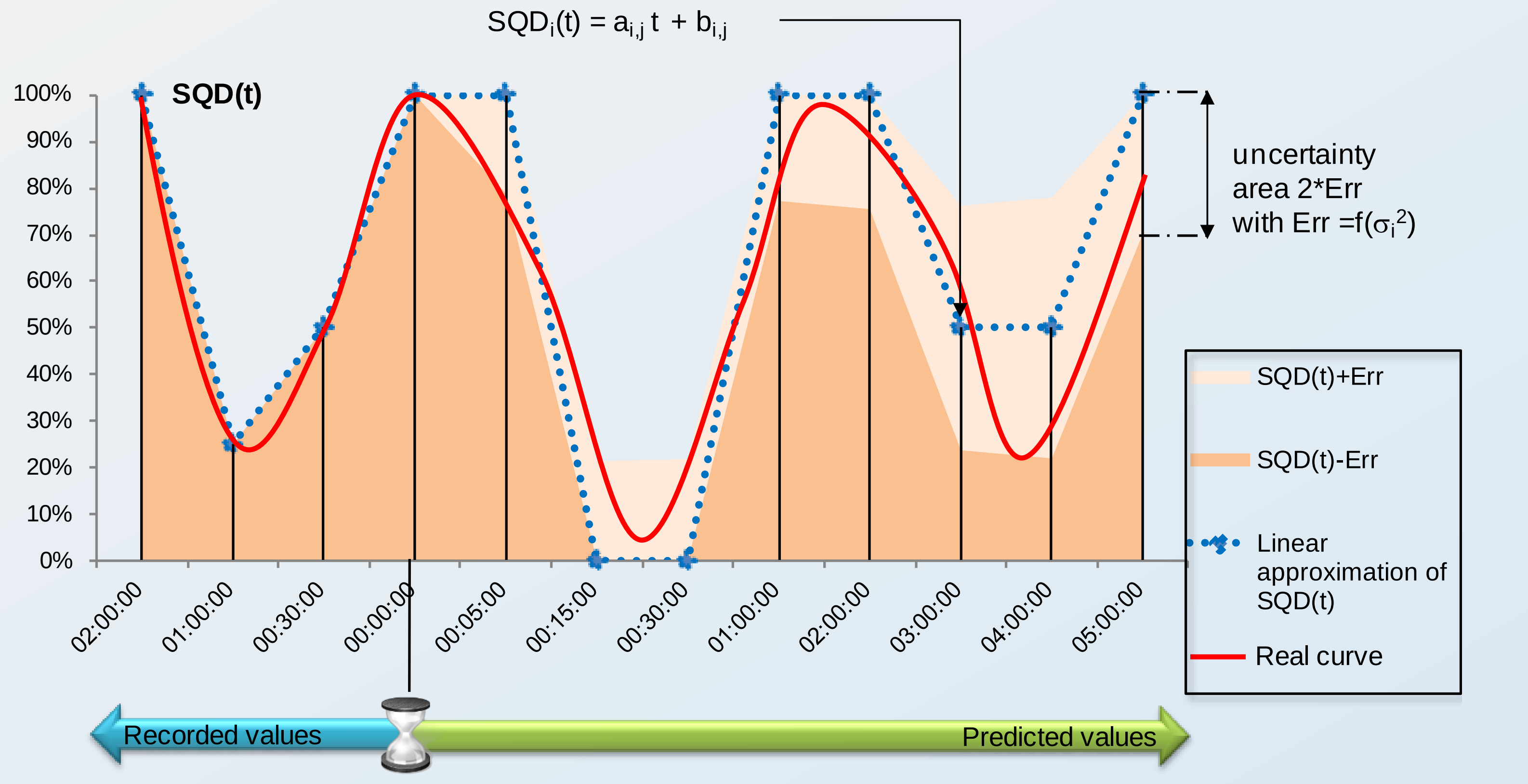
The SQD is one of three classes necessary to describe the risk level of a CI and it describes the state of the QoS provided by the CI (SQD class). The other ones are the externals threats occurring on the CI (TH class), the fault mitigation policy deployed in the CI (FM class). Some other information is shared as the ID of the CI, the origin of default, etc.

Value assignment to SQD

For each time t, each of the 10 parameters of SQD is the random variable taking the value 1 if the property is fulfilled and 0 if it is missing. Imagine the event space of all possible future event, and its probability of occurrence.

The i-th parameter is characterised by an estimation of the expected value, noted $SQD_i(t)$ as a function of time, and by an estimation of its variance $\sigma_i^2(t)$. This variance expresses errors from the model itself, the assessment error, and uncertainties of dependent services.

To simplify the description of $SQD_i(t)$, we replace it by a linear approximation for different segments of time, i.e. $SQD_i(t) = a_{i,j}\ t + b_{i,j,}$ for t between t_{j-1} and $t_{j,}$. Note that t_0=0 is considered current time. For the variance, a simple model with one single time slot could be enough: $\sigma_i^2(t) = c_i + d_i\ t$.



To summarise, the SQD is an xlm data structure containing for all 10 SQD parameters, the coefficients $t_{.}$, $a_{.}$, $b_{.}$, $c_{.}$, $d_{.}$, which allow to calculate for all upcoming points of time, the estimated expected value and standard deviation for 10 criteria: availability, reliability, maintainability,…

Conclusion

Within the FP7 ICT-SECURITY project MICIE and a Master in Information Systems Security Management at Luxembourg University, we intend to develop a real-time risk level dissemination and alerting system. To achieve this objective, the risk analysis has been deployed first at service layer level to take into account the heterogeneousness of involved CIs. It uses a specific ontology oriented service approach and focused on the notion of Quality of Service. This QoS has been modeled according to the notion of dependability and it will be assessed according to an approach similar to ISO 15408.

To be able to quickly compute the risk level, a simplified model of computation based on linear approximation has been proposed. This approach requires that interdependent CI share continuously for each offered service an xml structure describing its QoS. It contains 10 criteria and for each, an estimate of the expected value (and uncertainty of the estimate) for upcoming segments of time.

Our model needs further refinements, especially to consider modification of the CI over time and improved risk prediction techniques, and it needs validation in field.

Acknowledgement
The research leading to these results has received funding from the European Community's Seventh Framework Programme FP7/2007-2013 under grant agreement n° 225353 also referred as MICIE.

For more information:
http://www.itrust.lu/
http://www.micie.eu

European Commission
Information Society and Media