Risk prediction and information sharing with linked, but competing operators

MICIE Workshop

Roma

28th February, 2011

Dr. Carlo HARPES, itrust consulting

Risk prediction and information sharing with linked but competing operators

Agenda

Aim:

Design and implement a "MICIE alerting system" that identifies, in real time, the level of possible threats induced on a given Critical Infrastructure (CI) by "undesired" events happened in such CI and/or any other interdependent CI

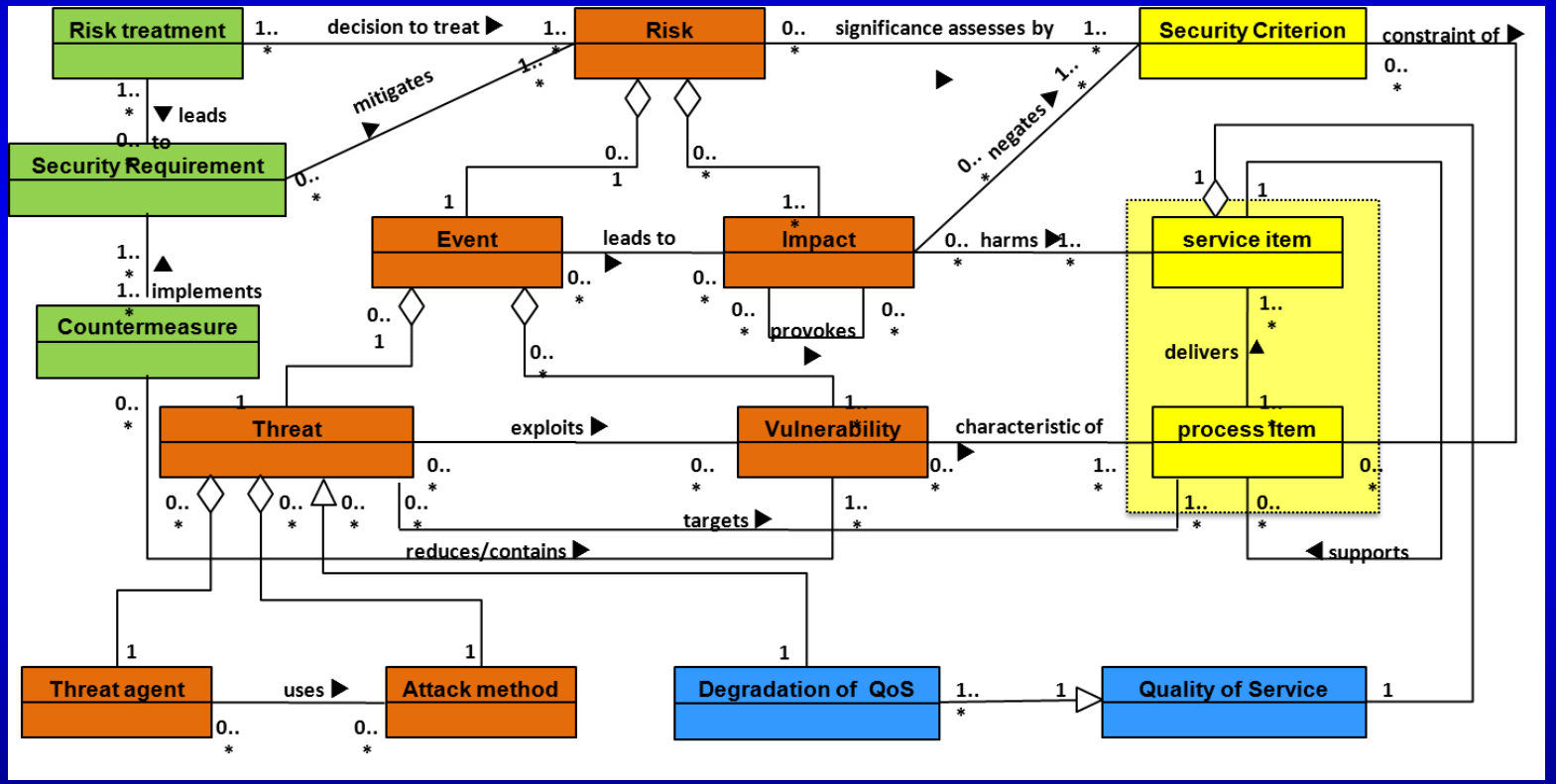
itrust's contributions:

- UniLux master thesis: "Risk Modeling and Simulation for Critical Information Infrastructure Protection".
  Risk ontology, service level descriptor, …
- How can the MICIE Gateway be used in a EU context?
  What data are operators willing to share?
- Specify security requirements (as ISO 15408 Protection Profile) for the MICIE gateway
- POC for data communication with Web Services
- Intrusion test on the Secure Mediation Gateway

Theoretic basis of risk assessment

Risk Ontology in CIP

An academic research on CIP allowed describing the ontology of risk in CIP at service layer level according to the degradation of QoS.

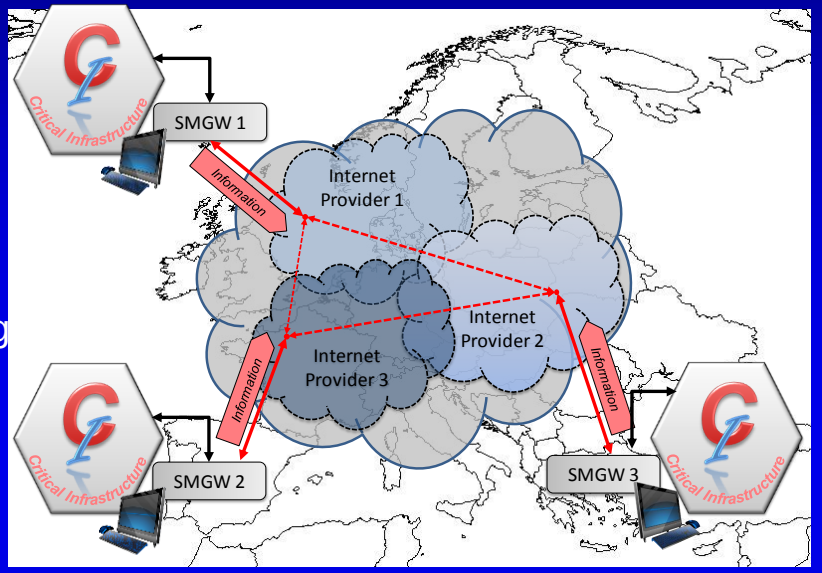


Model of Information Sharing in MICIE

MICIE Strategy

Aims of MICIE:

- Deployment of risk related information sharing among European CIs to predict risk level of CIs and avoid risk cascading phenomena
- Use of a specific interface called Secure Mediation GateWay (SMGW);
- Use of untrusted networks to provide communication channel between CIs (e.g Internet);
- High level of confidentiality, integrity, availability, and reliability.

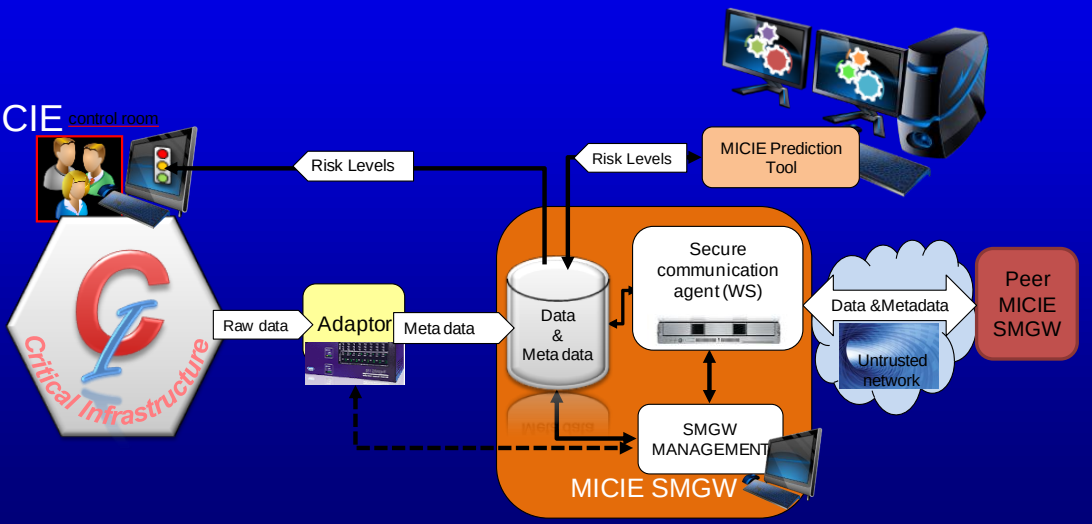


Interfaces:

- Between CI and Data Base
- Between peer SMGW
- Between Data Base and MICIE prediction tool

Technology choice

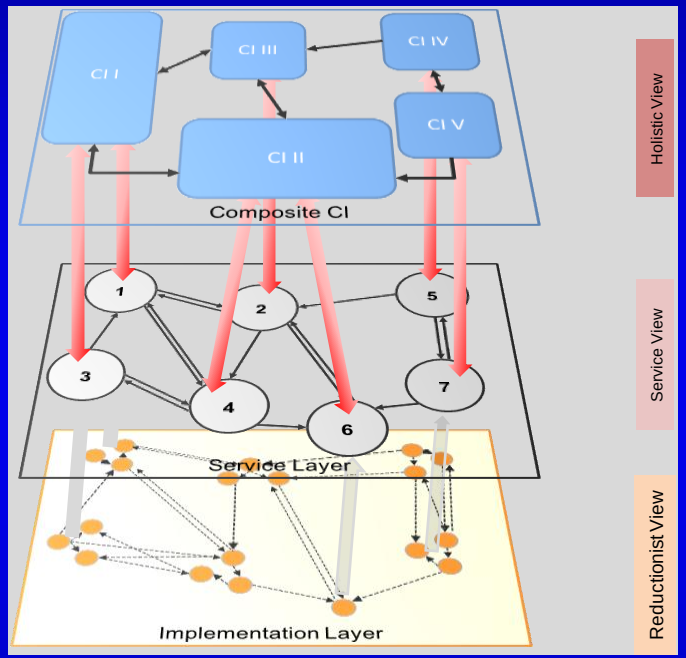
- Secure Web Service



Risk Ontology in composite CI system

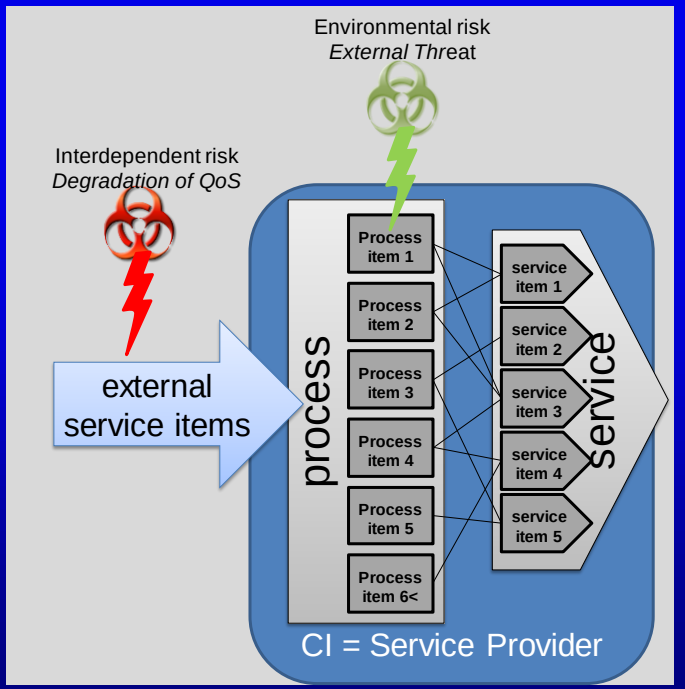
How to describe the risk ?

1) Risk assessment at service layer level



2) 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.



3) 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.

Information sharing system in CIP

Problematic

How ? What? To who ? When?

- Through the MICIE gateway
- Information at Service Layer
- Every partner or neighbour
- Regularly and/or at demand

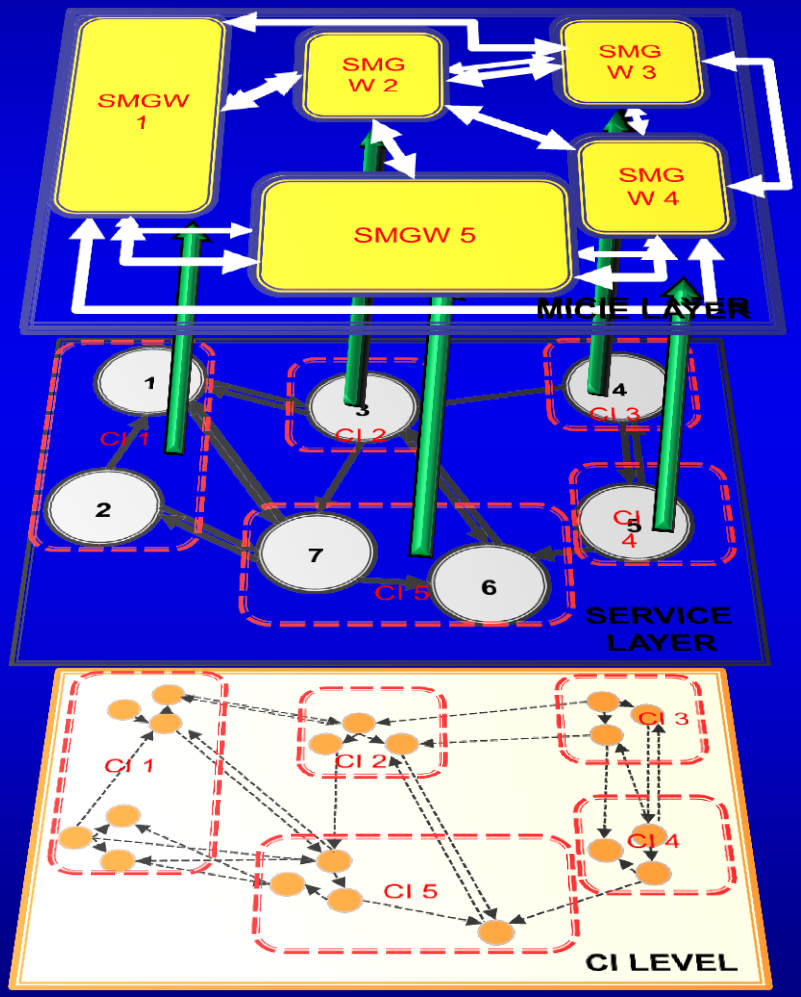
How to choose the sharing options ?

- Data flow
- Information Confidentiality
- Information Access
- Type of information data

Broadcasting option

Information is shared with every partner

Information is shared only with neighbours

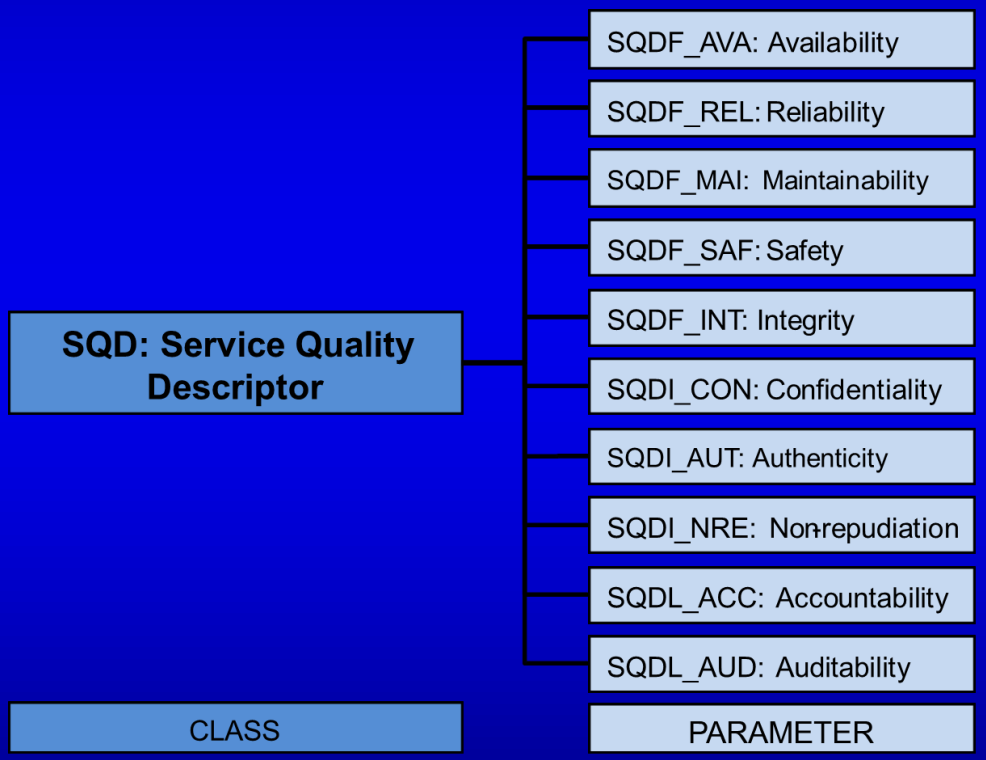


Information sharing system in CIP

What to share ?

The Service Quality Descriptor (SQD)

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



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).

The whole of parameters is called SRD (Service Risk Descriptor).

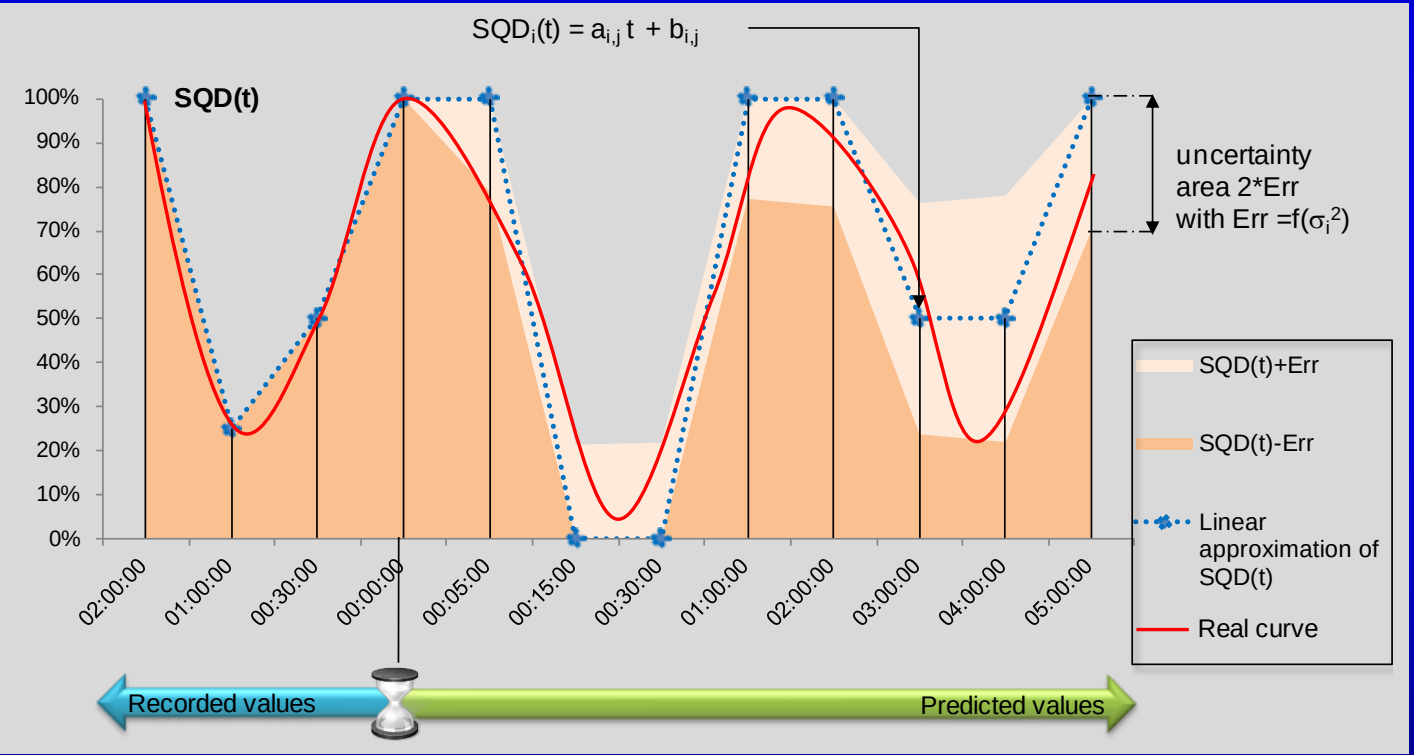
Some other information is shared as the ID of the CI, the origin of default, etc.

Information sharing system in CIP

Value assignement 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.

Each parameters is characterised by an estimation of the expected value and by an estimation of its variance. For the computation a linear approximation is chosen.

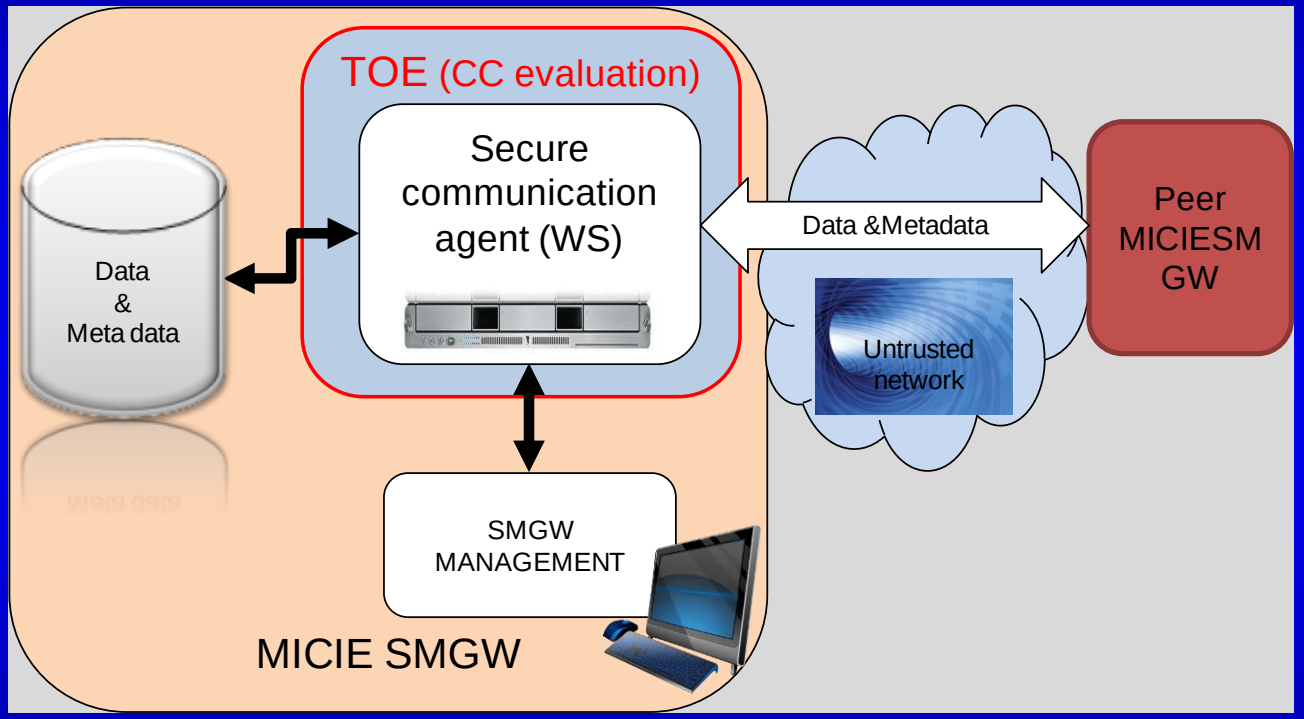


The SQD is an xlm data structure containing for all 10 SQD parameters, for different upcoming time intervals, the coefficients of an linear approximation of the expected value and and of the standard deviation of the parameters.

Secure Information Sharing in MICIE project 1/3

A Protection Profile for Secure Information Sharing Among CIs

TOE : The target of evaluation is the interface with the external environment of the operator: the Secure Communication Agent (SCA) based on Web services



Usage and major security features of the TOE:

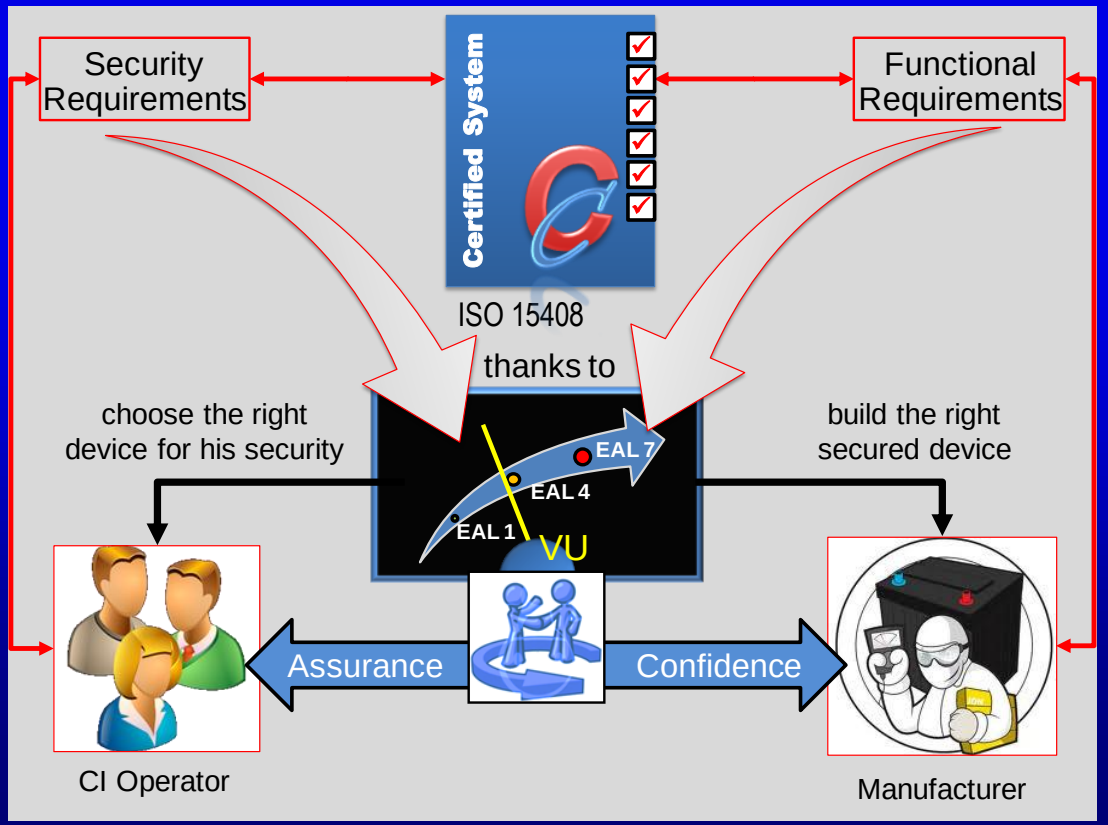
- Collect risk related information from, and broadcast to peer CI operator via open networks.
- Ensure confidentiality, integrity, availability or risk related information.

Secure Information Sharing in MICIE project 2/3

Benefits of the ISO 15408 approach

The standardised approach allows:

- ❑ Choosing security objectives and assumption to cover identified treats.
- ❑ Designing Security Functional Requirements to cover objectives.
- ❑ Certifying that the SMGW is secure if operated in the conditions it has been designed for.
- ❑ Providing confidence to manufactures that the device is secure enough.
- ❑ Fostering operators' trust in the security of a given device.



Secure Information Sharing in MICIE project 3/3

Protection Profile for MICIE secure gateway

TOE Description: The SCA based on Web services and its interfaces:

1. with the unsecured network (internet) to communicate with peer SMGW;
2. with the Data Base used by the prediction tool and the CIs data adaptor;
3. with the SMGW management system (policy, audit, supervision…).

Assets - Two classes

- Shared information, like risk related data to share and general information about the CI topology.
- The ToE and its configuration itself.

Threats – 8 in three types

- Threats on communication, i.e. interception of admin. command or of messages.
- Threats on keys management
- Threats on security policies and their security contexts

Assumptions – only two:

- Administrator non hostile,
- protected physical access to TOE

Security Objectives [SO] – 17 SO in three types

- **SO for services** delivered by the TOE: Management of the TOE, Confidentiality and integrity of data exchanges and of data topology
- **SO for the TOE**: identification and authentication of users or administrators, management of security policy, detect replay messages, use appropriate cryptography and protect keys.
- **SO for the operational environment**: trusted administrator, secure environment administration, protection of physical access., secure keys generation.

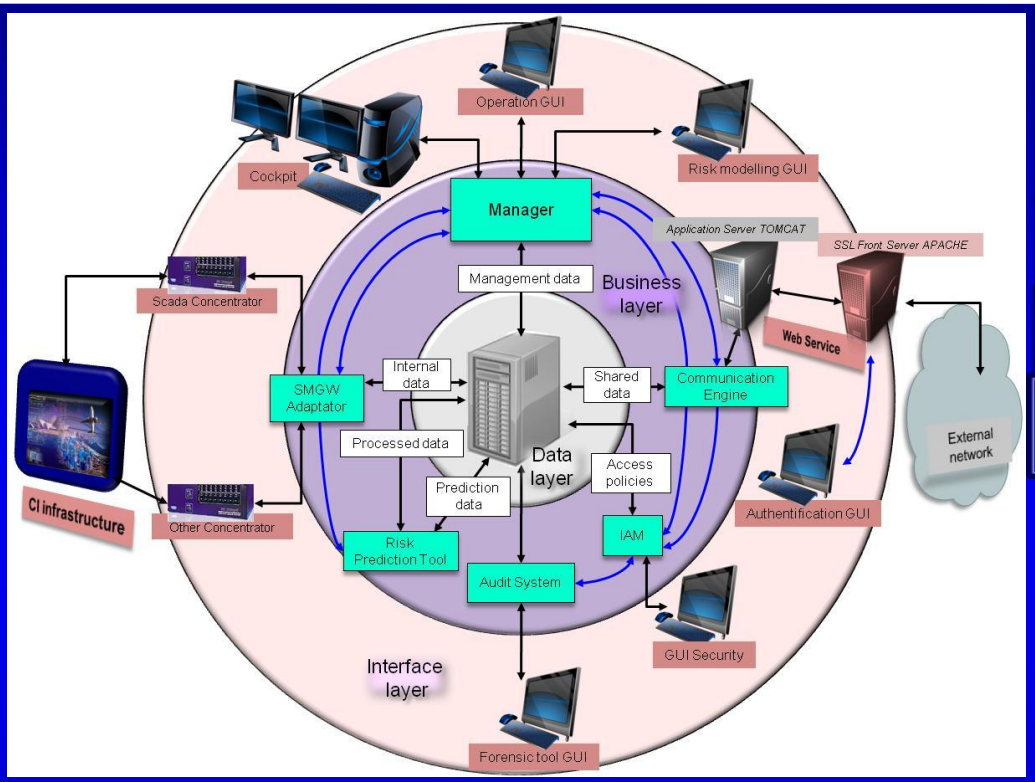
40 Functional Requirements: to reach the identified SO:

Secure Information Sharing in MICIE project 1/3

Protection Profile for MICIE secure gateway

POC:

Web service based



Intrusion test:

- **No vulnerability**
- **Source pending…**
- **Recommendations for proper use.**

[Rec 1] Setup a firewall to filter the traffic towards the server system.

[Rec 2] Hide services not useful on external interface.

[Rec 3] Update openSSH and Apache httpd.

[Rec 4] Define a policy for the update of the server and the services.

Thank you for your attention

Dr. Carlo HARPES, itrust consulting