Selex ES | Israel Electric | Transelectrica | Lyse | itrust consulting | Multitel | Roma Tre | ENEA | CRAT | University of Surrey | Tudor | FCTUC

CockpitCI Project Overview

SCADA Cybersecurity Workshop

Bucharest,

16th September 2014

Antonio Graziano

CockpitCI Project Coordinator

Information Society

List of contents

- **Project introduction**
- **Technical solution**
- **Key concepts**
- **Concluding remarks**

The CockpitCI project

- Full name: "Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures"
- EU-FP7-SEC-2011-2.5-1 (285647)
- 12 partners from 8 countries
- 3 end-users: IEC, Lyse, Transelectrica
- 36 months project (start on 1st January 2012)

Partners on the map of Europe……

Partners on the map of Europe……

Partners on the map of Europe……

The CockpitCI project: partners role

Project Coordinator: **Antonio Graziano** (SELEX ES)

Scientific Coordinator: **Stefano Panzieri** (ROMA3)

WP LEADERS

Program Management
SELEX ES (Federico De Padova)

Modeling and Prediction of QoS …
ENEA (Michele Minichino)

Cyber Analysis and Detection
UC (Paolo Simoes)

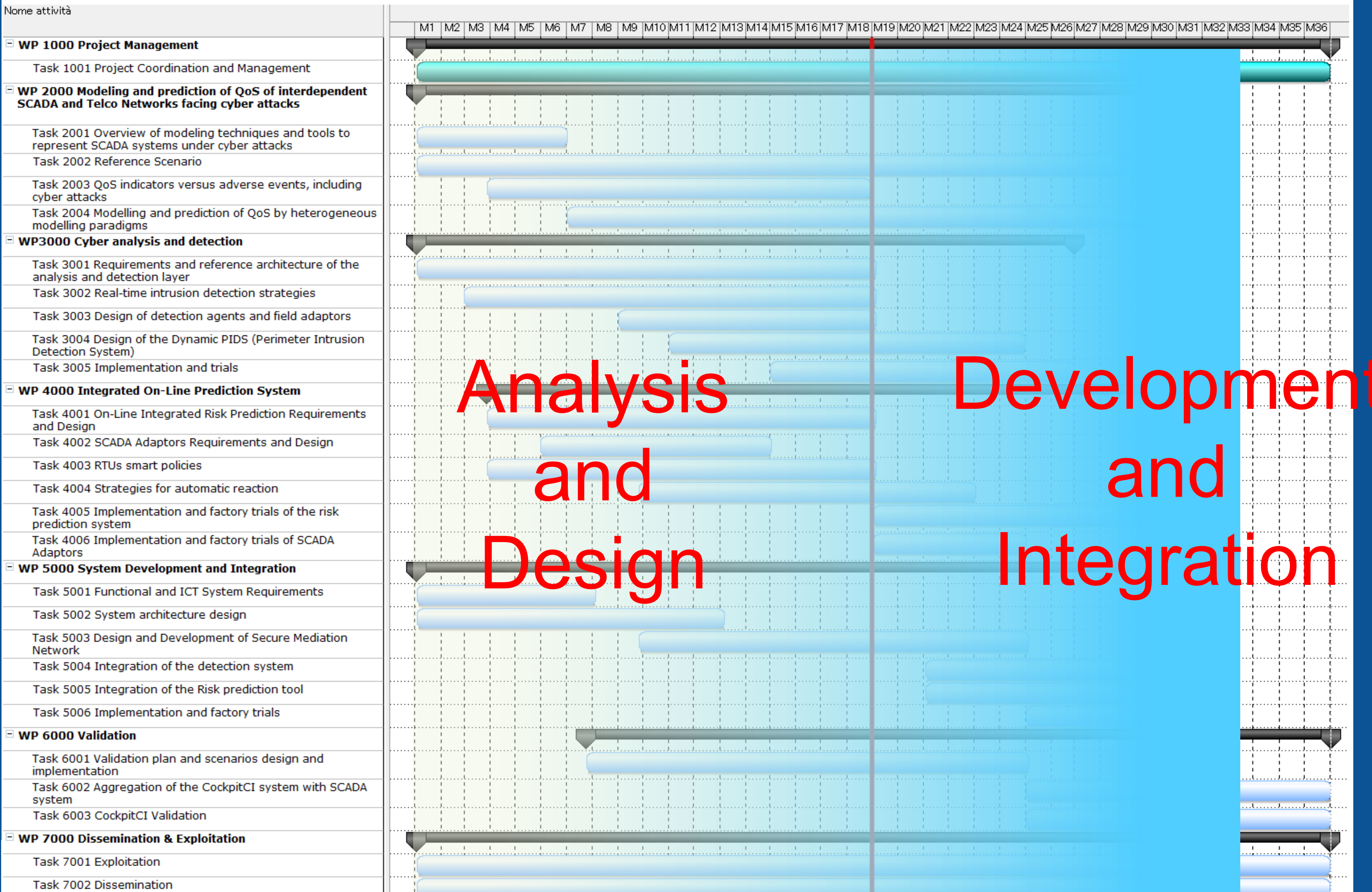
Integrated Risk Prediction
ROMA3 (Stefano Panzieri)

System development and Integration
SELEX ES (Antonio Graziano)

Validation
IEC (Leonid Lev)

Dissemination and Exploitation
itrust (Matthieu Aubigny)

The CockpitCI GANTT: where we are now

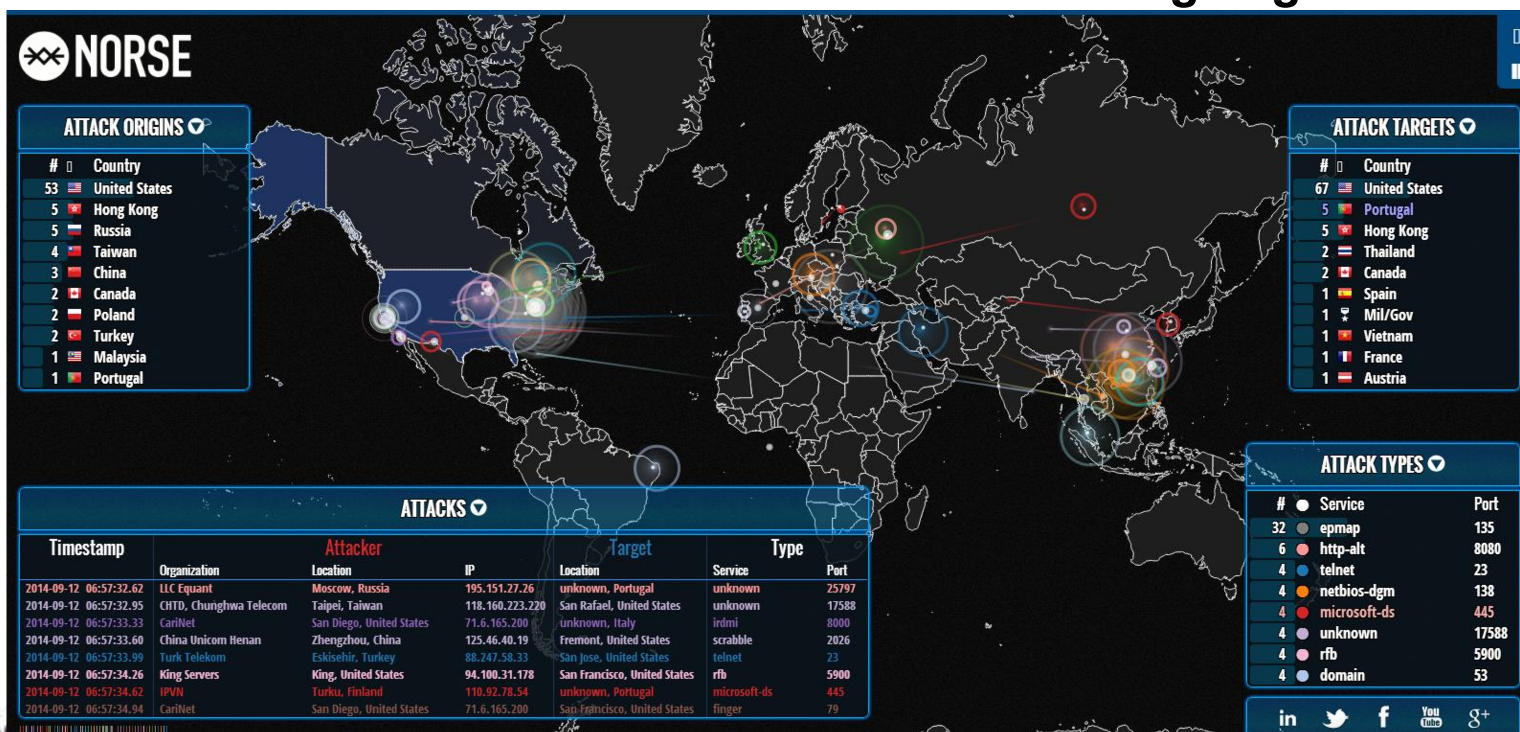


Cyber domain ….

The most challenging of all possible worlds ?

- A virtual domain created by man
- Where everything is possible (with a click)
- Continuously exposed
- Everything is on sale
  - bots, vulnerabilities, hacker kits,…

Attacks are going on all the time !



http://map.ipviking.com/

Cyber attacks to SCADA systems

Until 2010 ……. great attention but no evidence

Cyber attacks to SCADA systems

Until 2010 ……. great attention but no evidence

then Stuxnet

the first cyber attack against a SCADA system!

Cyber attacks to SCADA systems

Until 2010 ……. great attention but no evidence

then Stuxnet

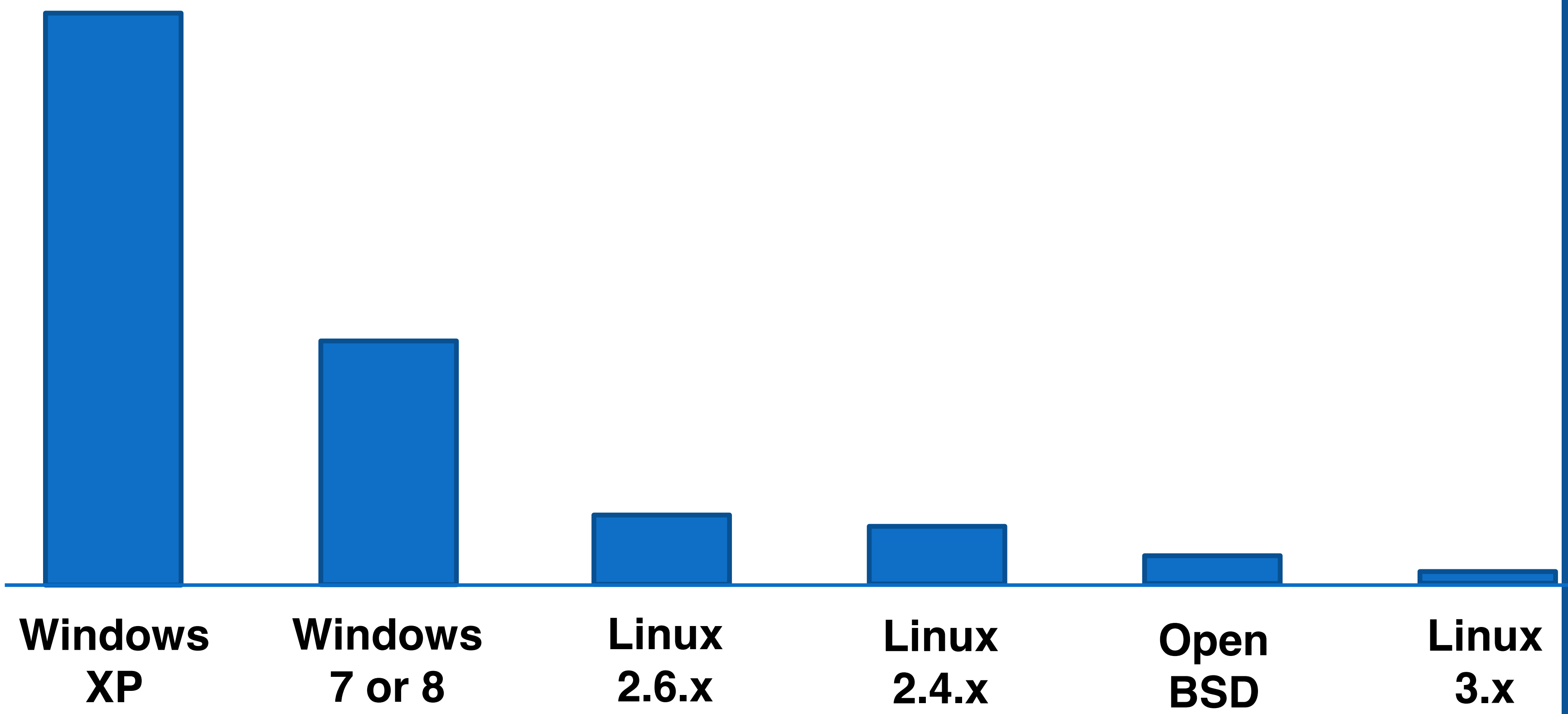
the first cyber attack against a SCADA system!

Cyber threats to SCADA systems *

Threats are just as sophisticated as needed !

*Extracted from: *Jart Armin & Raoul Chiesa, "Cyber Weapons in 2011: an F-16 just flew over a first world war battlefield"*, 2011.

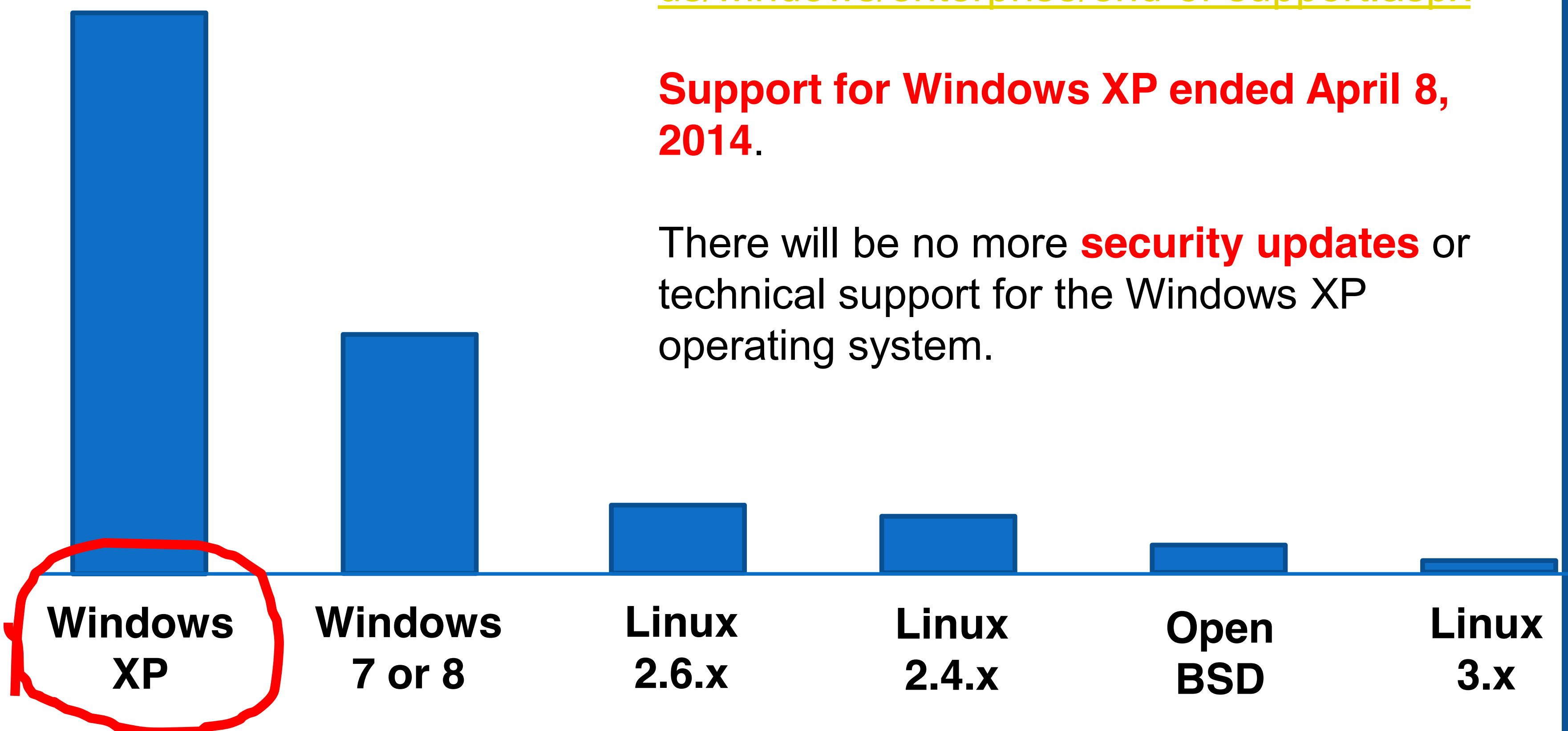
Top operating systems in Industrial Control Systems *



Cockpit CI

* Source: https://www.shodan.io
SHODAN is world's 1st search engine for Internet connected devices.

Top operating systems in Industrial Control Systems *



http://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

Support for Windows XP ended April 8, 2014.

There will be no more **security updates** or technical support for the Windows XP operating system.

* Source: https://www.shodan.io
SHODAN is world's 1st search engine for Internet connected devices.

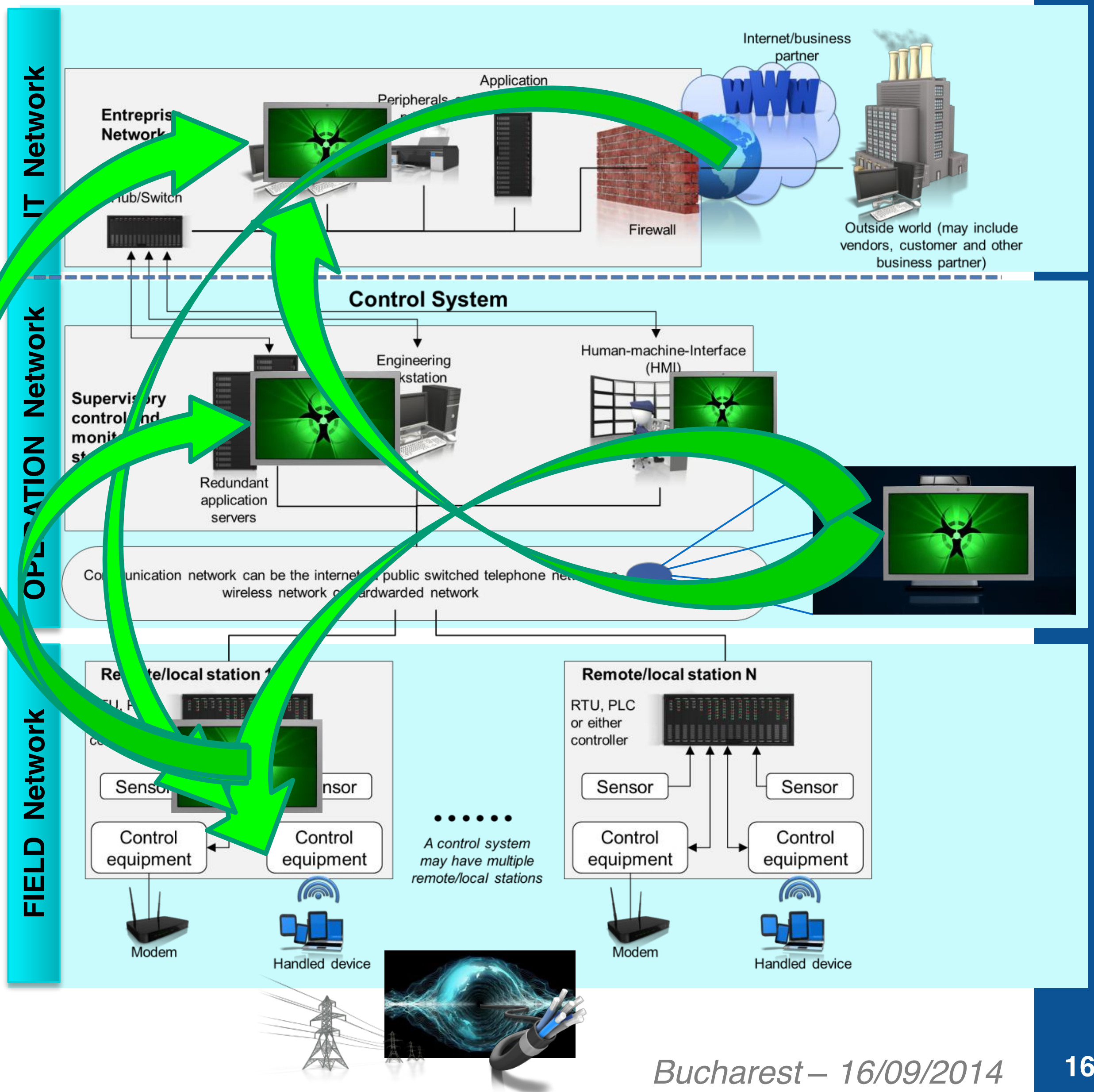
Cybersecurity in SCADA

FACT : Evolution from proprietary and closed architectures to open, standards-based solutions for ICS based infrastructure

CONSEQUENCE : Cyber-attacks can come from any part of the infrastructure:

1. **FIELD Network**
   as SCADA systems
2. **OPERATION Network**
   as Telco system or monitoring/management system
3. **IT Network**
   as enterprise devices and services

and can target any part of it



Cockpit CI

MICIE vision

By increasing cooperation among infrastructures one could:

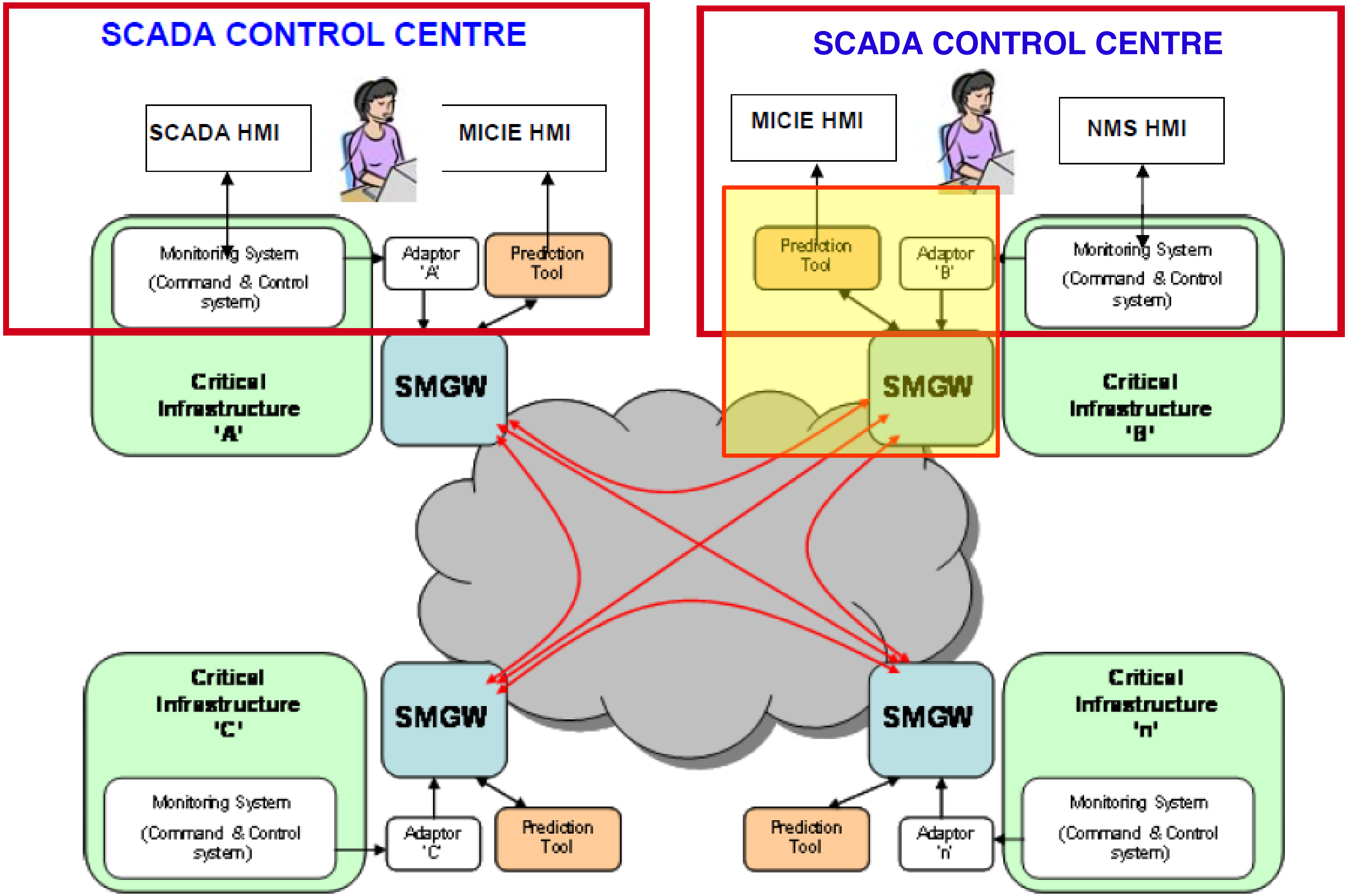
- **provide the operator with a better (global) situation awareness in the presence of adverse events (due to system failures or induced by cyber),**

  i.e. "information about the future evolution of their infrastructure with a wider perspective compared to previsions that can be generated by sector specific and isolated simulators";

- **increase their level of service and predictive capability.**

FP7-ICT-SEC-2007.1.7
Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures

MICIE distributed architecture

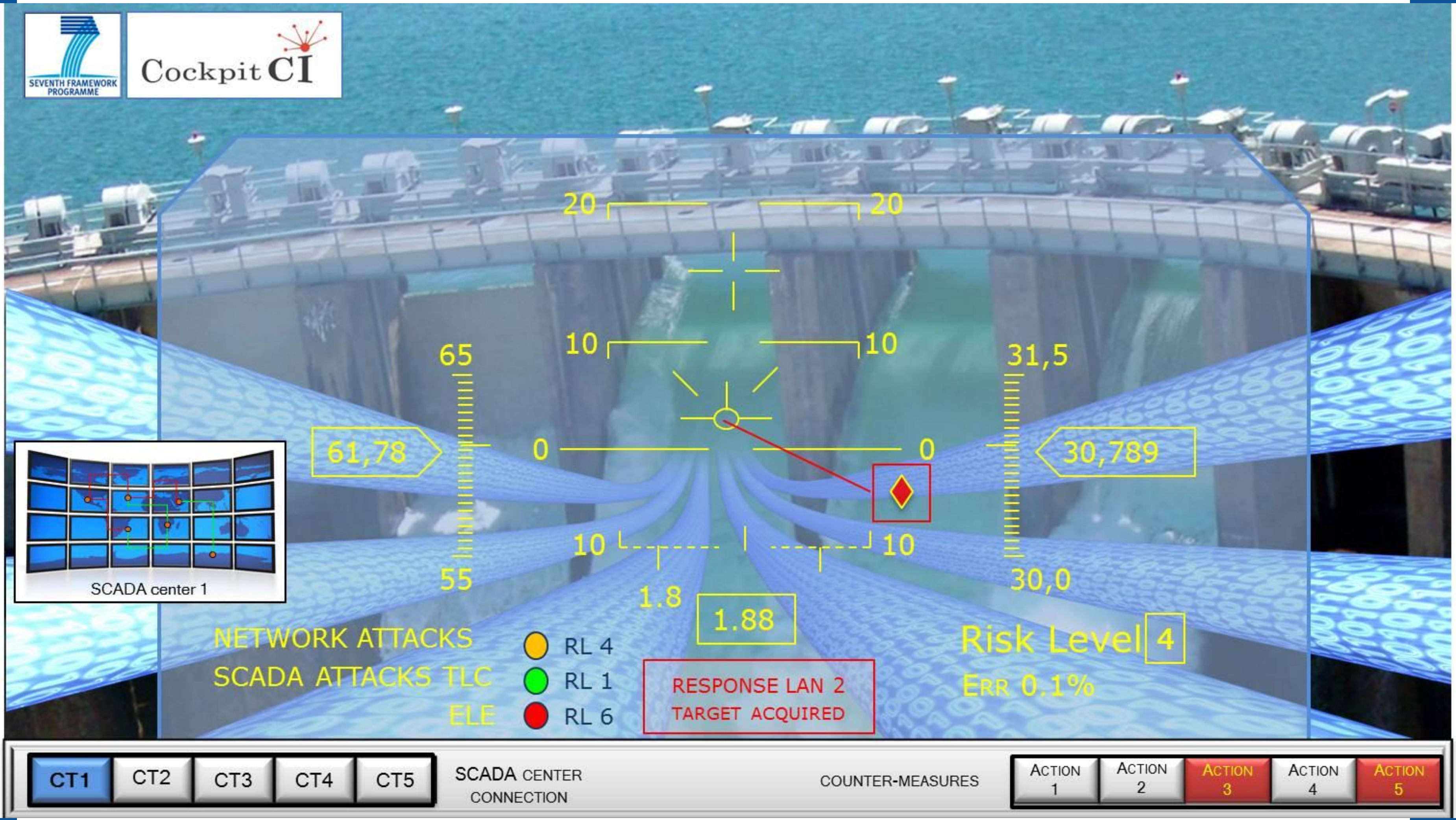


CockpitCI objectives……

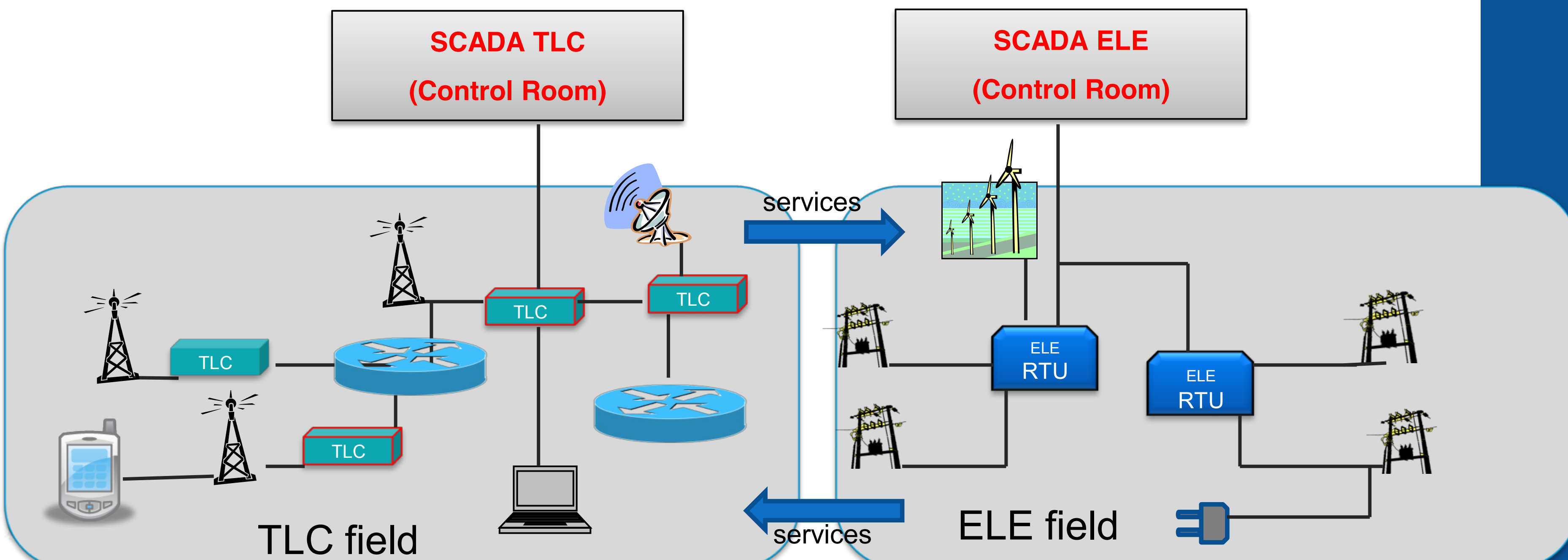
CockpitCI aims at:

- improving resilience and dependability of CIs by the **automatic detection of cyber threats** and the **sharing of near real-time information** about attacks among CI owners.
- identifying, in near real-time, the **CI functionalities impacted by cyber-attacks** and **assessing the relevant degradation** of CI delivered services.
- classifying the associated risk level, **broadcasting alerts** at different security levels and **activating strategies of containment** of the possible consequences of cyber-attacks.
- leveraging **the ability of field equipment, in coordination with the central control level, to counteract cyber-attacks** by deploying preservation and shielding strategies able to guarantee the required safety.

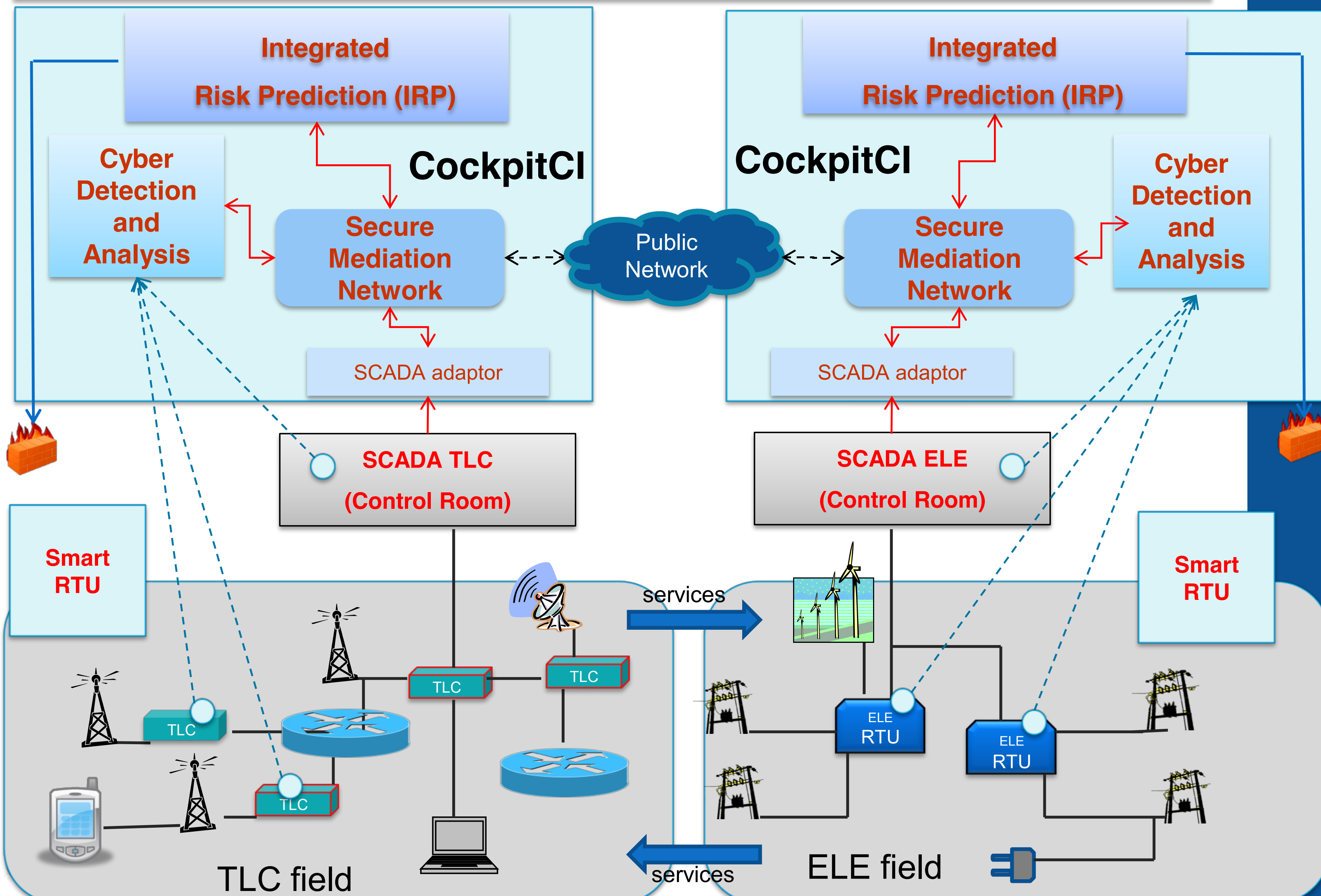
VISION


SEVENTH FRAMEWORK PROGRAMME
Cockpit CI
20
20
10
10
65
31,5
61,78
0
0
30,789
10
10
55
30,0
1.8
1.88
SCADA center 1
NETWORK ATTACKS
SCADA ATTACKS TLC
ELE
RL 4
RL 1
RL 6
RESPONSE LAN 2
TARGET ACQUIRED
Risk Level 4
ERR 0.1%
CT1
CT2
CT3
CT4
CT5
SCADA CENTER CONNECTION
COUNTER-MEASURES
ACTION 1
ACTION 2
ACTION 3
ACTION 4
ACTION 5

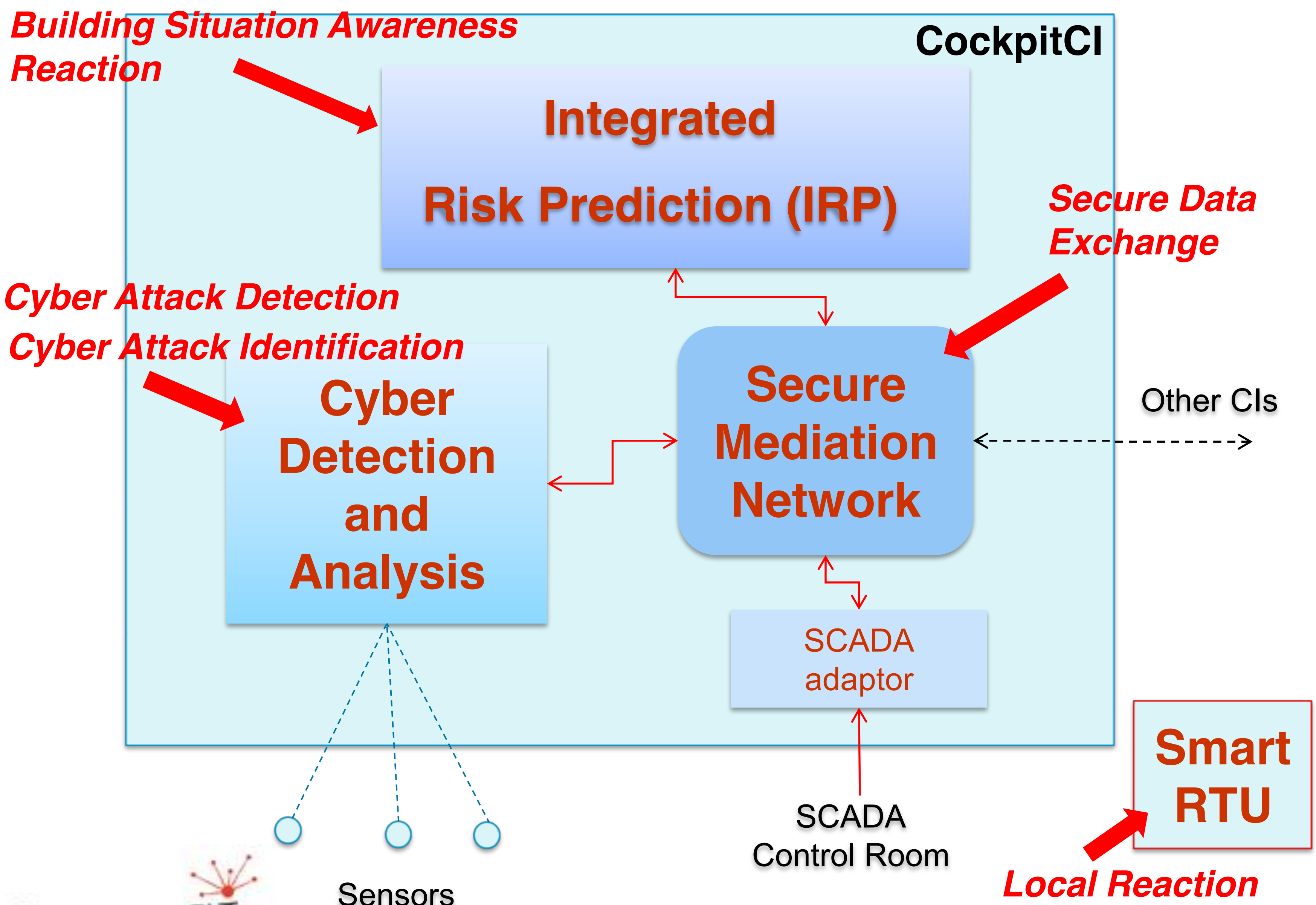
CockpitCI operational context



CockpitCI operational context



CockpitCI schematic architecture



Key concepts

- Situation Awareness
- Intrusion tolerance
- No interference with SCADA system

Situation Awareness

- What vulnerabilities exist in the system ?
- Which attacks are going on ?
- Will the attack be successful ?
- What happens if the attack is successful ? What is the impact in terms of QoS ?
- What is the impact if the attack is successful on an interdependent infrastructure ?

Intrusion tolerance

- Understand how much of the infrastructure can be kept in operation safely in adverse situations;
- Maintain at least partial operation rather than go to total shutdown;
- Assess and mitigate the influence of a cyber attack on the operation of a critical infrastructure controlled by a vulnerable SCADA control centre over a vulnerable communication network.

CockpitCI: basic solution

Monitoring and decision support

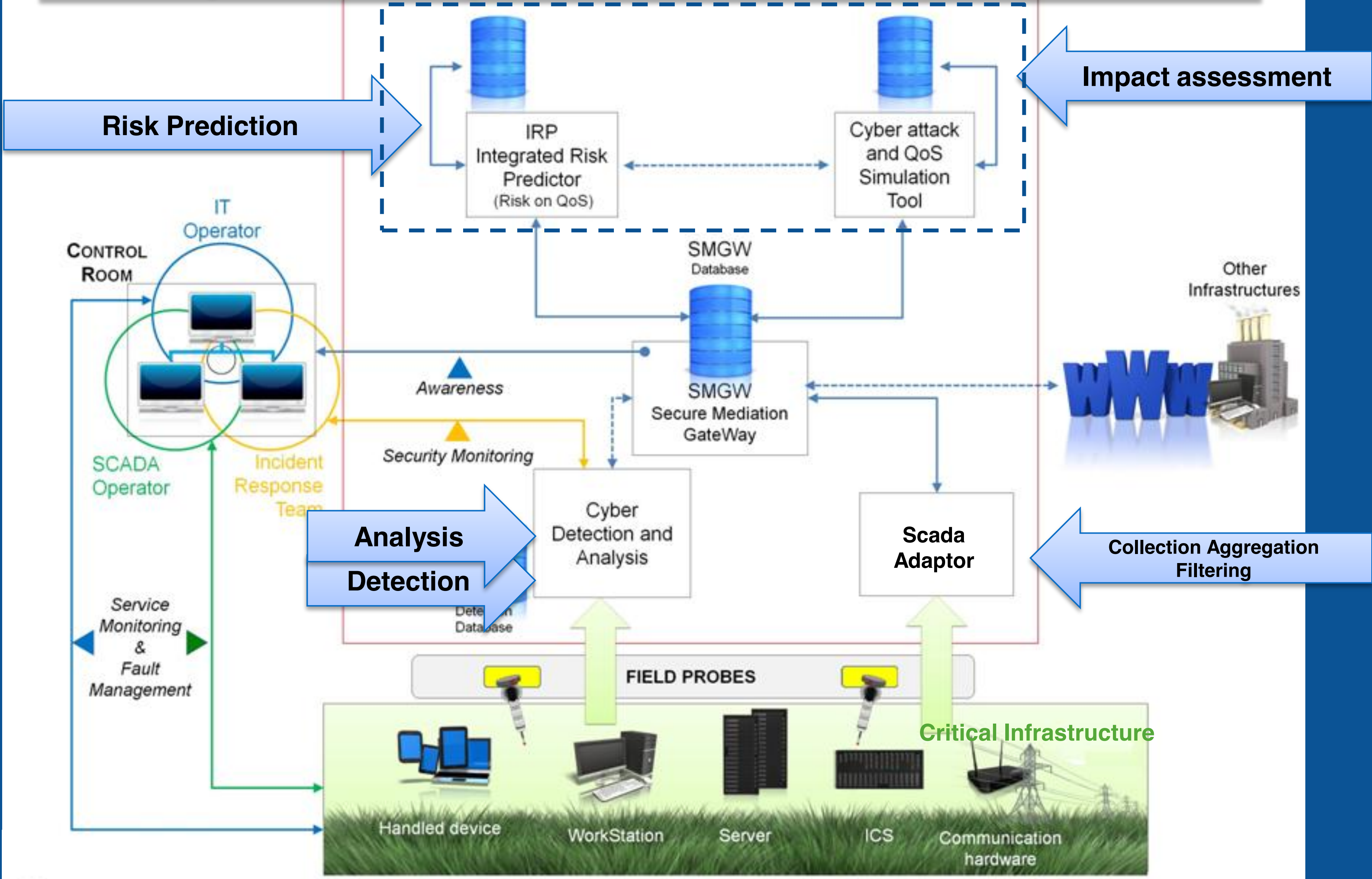
- Passive
- Not invasive
- Invisible
- legacy compliant
- patching as needed

CockpitCI: advanced solution

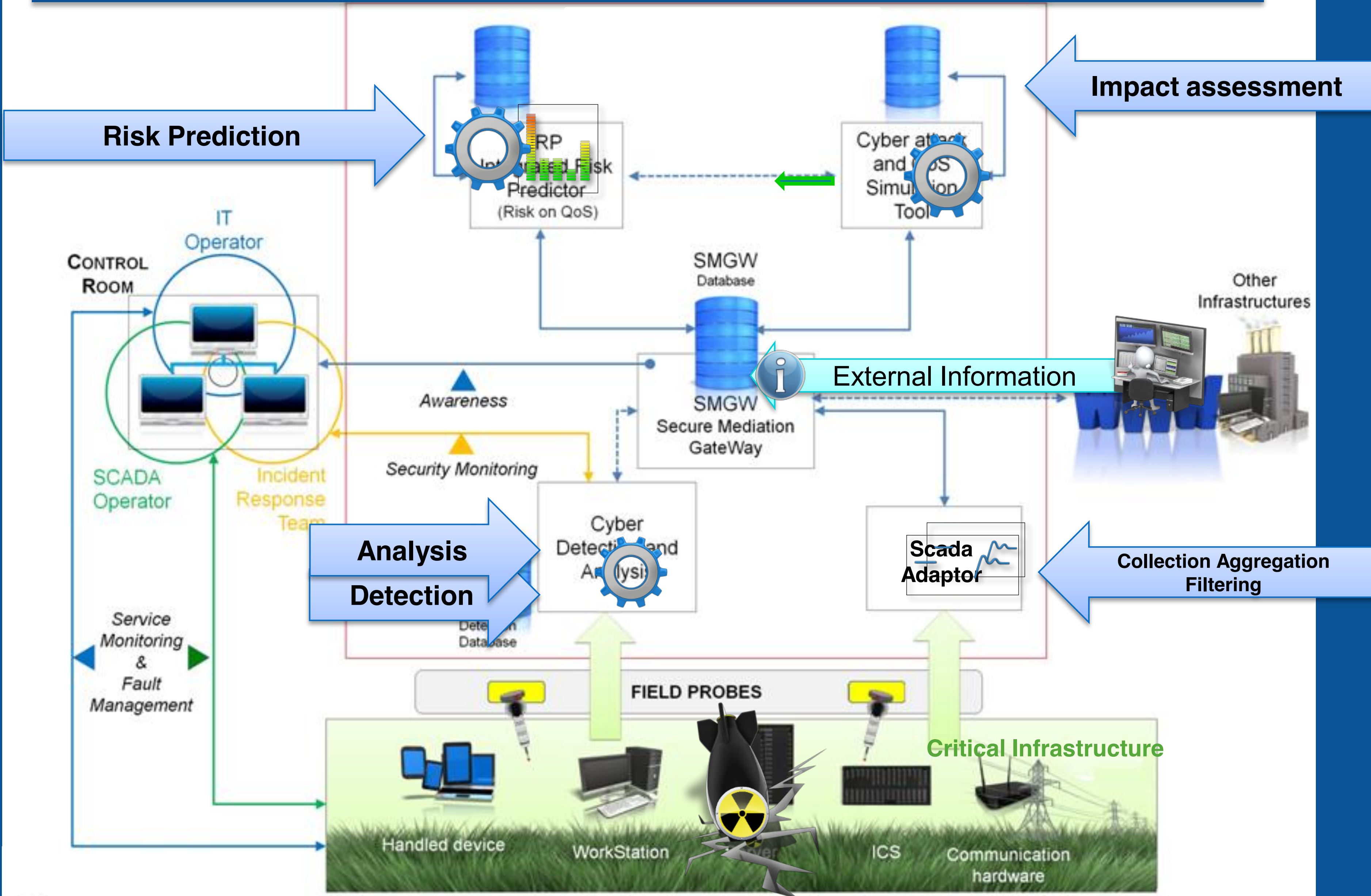
Beyond decision support to include automatic reaction mechanisms, e.g.:

- The Risk Predictor triggering reconfiguration of a firewall;
- The Risk Predictor raising and broadcasting the level of the alert;
- Smart RTUs refusing to execute an “abnormal sequence of commands”;
- Local sets of RTUs coordinating in autonomy in case of isolation from SCADA control centre.

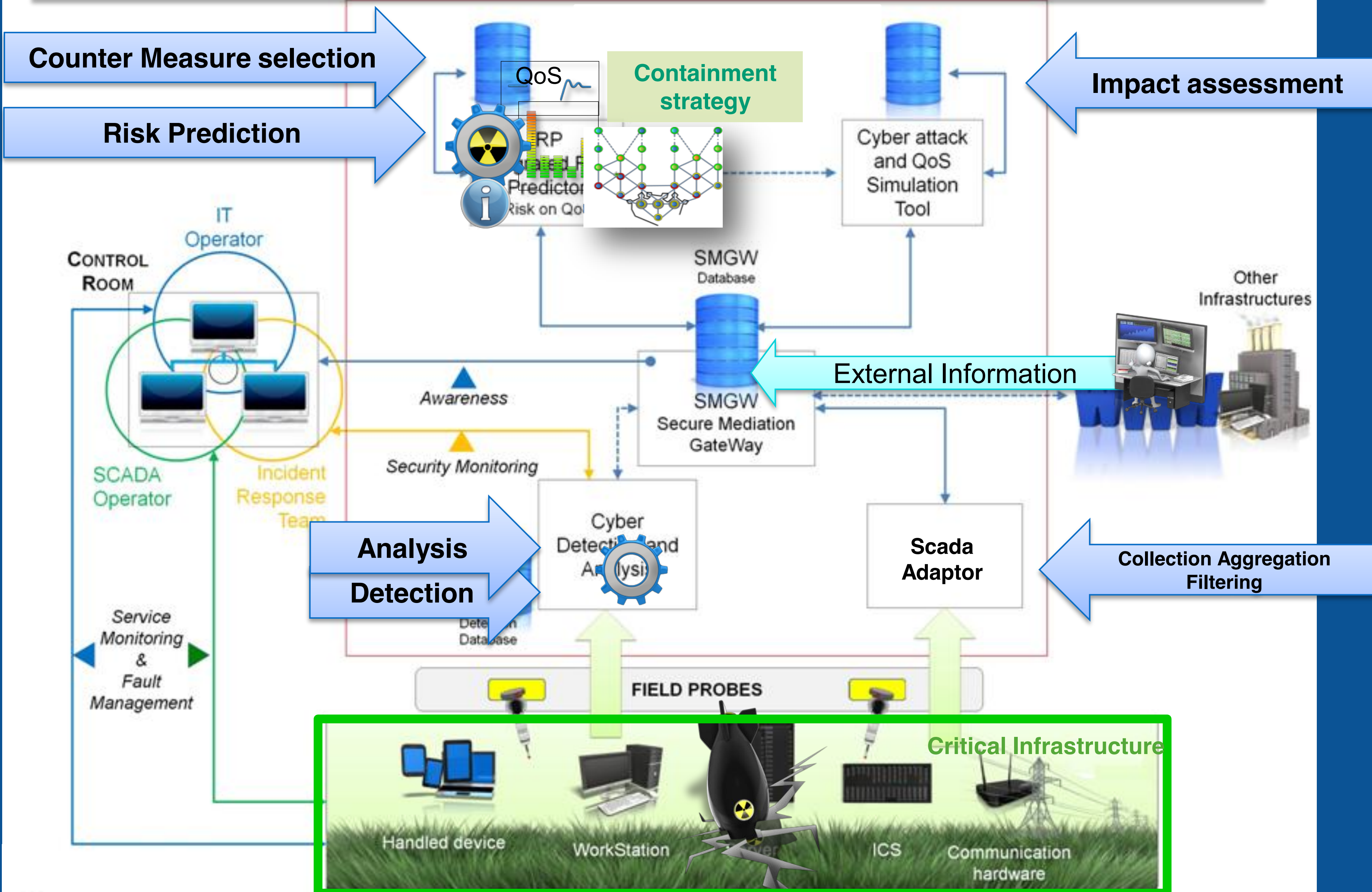
CockpitCI simple schema with functions



CockpitCI in operation: Monitoring mode



CockpitCI in operation: Monitoring & reaction mode



Main results

- state-of-the-art cyber detection capabilities (SCADA specific, zero-day potential)
- cyber modeling + QoS modeling ➔ cyber impact on QoS
- integrated solution (from cyber detection to risk prediction (and reaction))
- hybrid test bed remotely accessible for design and test
- Impact evaluations on QoS in specific situations:
  - no cyber attack
  - in presence of cyber attack
  - in presence of cyber attack and CockpitCI tool

Concluding remarks

- **CockpitCI is investigating and proposing an innovative solution in order to address issues such as:**
  - Increase the level of situation awareness;
  - Keep infrastructures in operation (at least partially) in adverse situations;
- **Cyber threat is often not at the top of the list;**
- **Cyber threat is not virtual;**
- **CockpitCI adds an extra layer of defense.**

Follow on

- **Cyber detection :**
  - Highlight on cyber detection architectures, techniques and tools
  - which attacks can be detected and how ?

- **Modelling**
  - Scenario characteristics
  - Models and where can they be deployed

- **Integrated Risk Predictor:**
  - which outputs (cyber impact, service impact, risk level, CM) are produced and how ?
  - Smart reaction: when and how

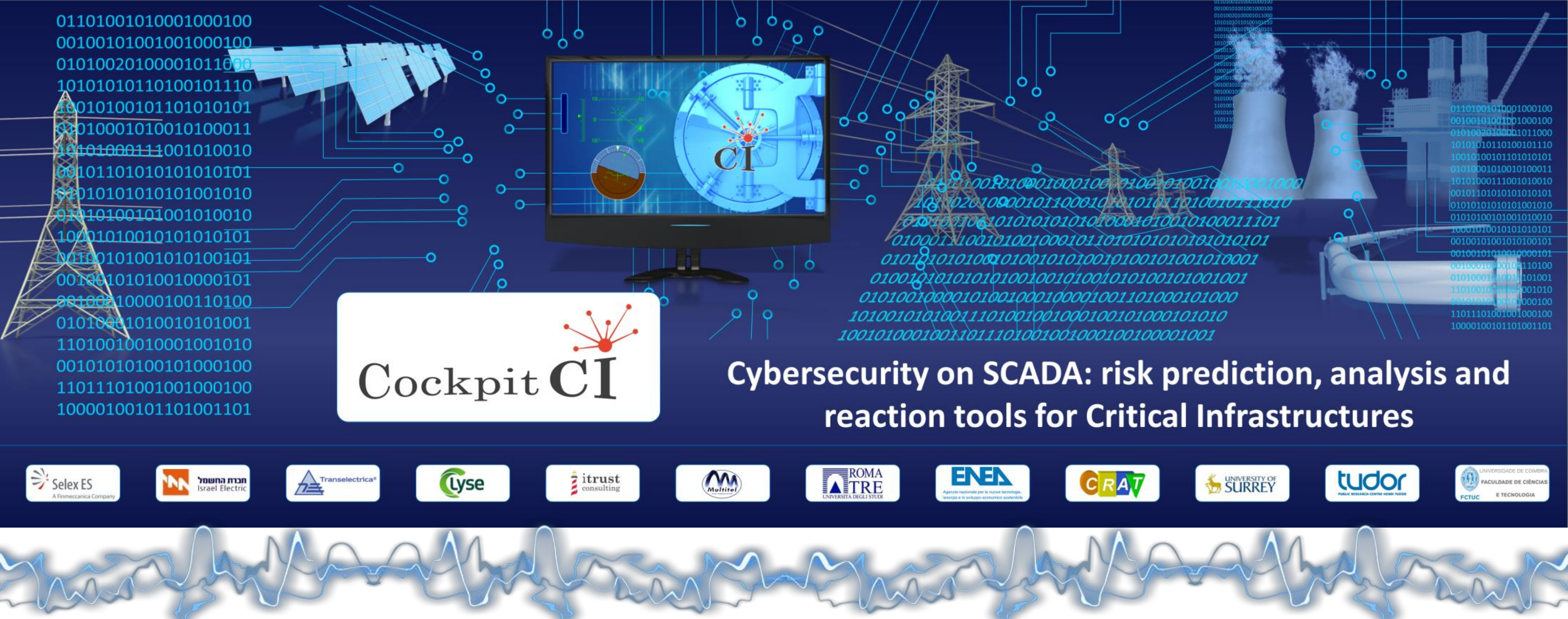
- **Validation**
  - Hybrid TestBed: what is it and why.

Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Thank you for your attention

Information Society



Improving cyber-security awareness on Industrial Control Systems: the CockpitCI approach

FCTUC FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

4th CockpitCI Workshop (Bucharest 16.09.2014)

Tiago Cruz
University of Coimbra

Information Society

Presentation Outline

- *Introduction*
- *Cyber Analysis and Detection in the CockpitCI solution*
- *Reference architecture*
- *Event analysis and correlation*
- *Detection Agents and Field Adaptors*
- *PIDS Architecture: integration*
- *Conclusions*

Introduction

ICS and SCADA

In the last few years, Industrial Control Systems (ICS), such as SCADA (Supervisory Control and Data Acquisition) systems, have evolved towards open architectures and standard technologies:

- Initially, ICS systems were isolated by nature (the *airgap* principle), being limited to the process network – in those times, security was guaranteed by both obscurity and isolation (a bad practice, anyway).

- Protocols were proprietary and its documentation was undisclosed, creating a false sense of security.

- Only manufacturers and attackers knew of failures and vulnerabilities, with both parts having no interest in their divulgation.

This move, together with the use of ICT technologies and the increasing adoption of open, documented protocols, exposed serious weaknesses in SCADA architectures.

ICS vs. ICT

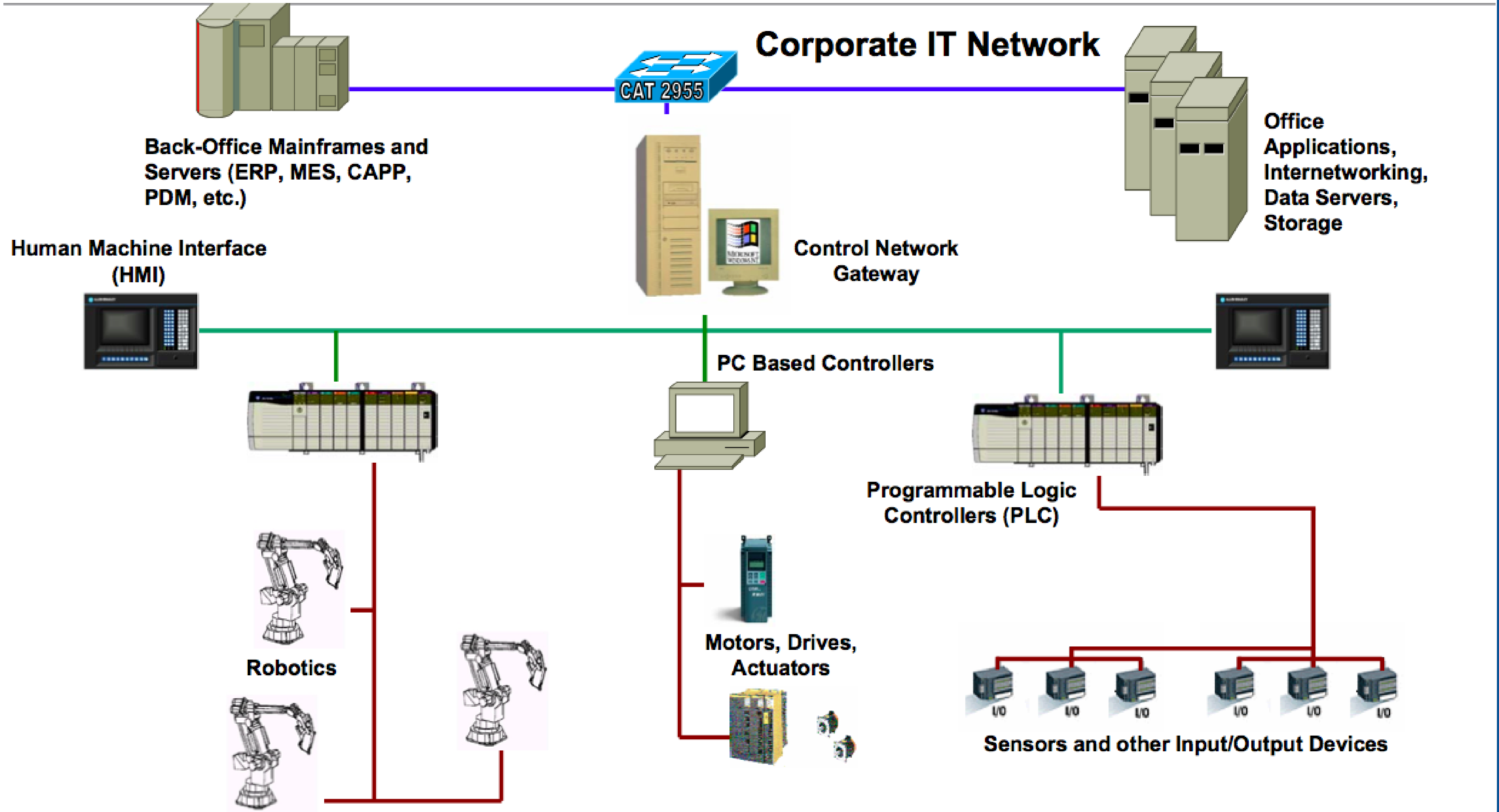
Up to a certain extent, SCADA architectures are becoming increasingly similar to ICT systems:

- Widely available, low-cost Internet Protocol (IP) devices are replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents.

- ICS are adopting ICT solutions to promote corporate connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols.

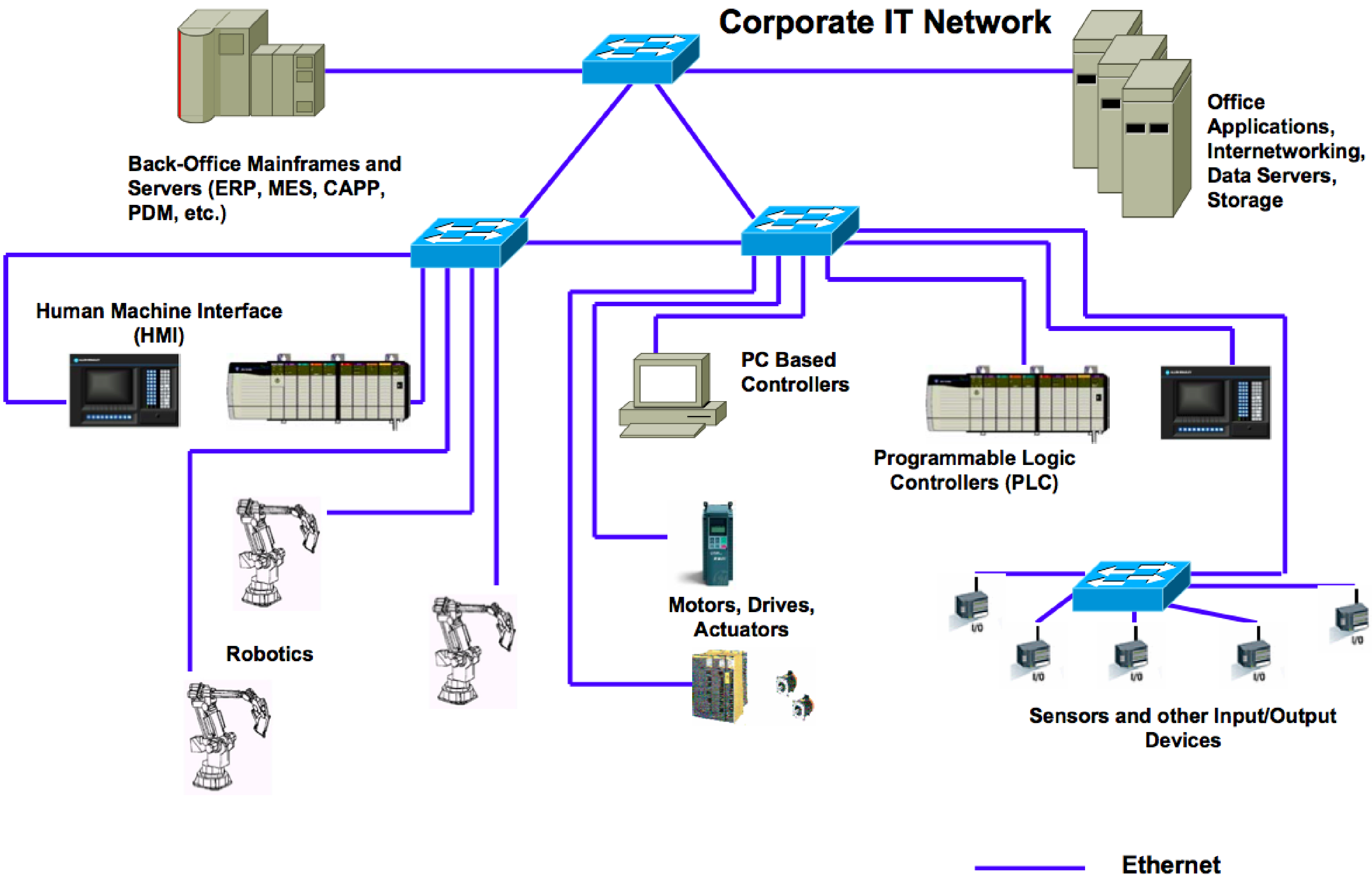
While this integration introduced new ICT capabilities, it provided significantly less isolation for the ICS, from the outside world.

A legacy SCADA network



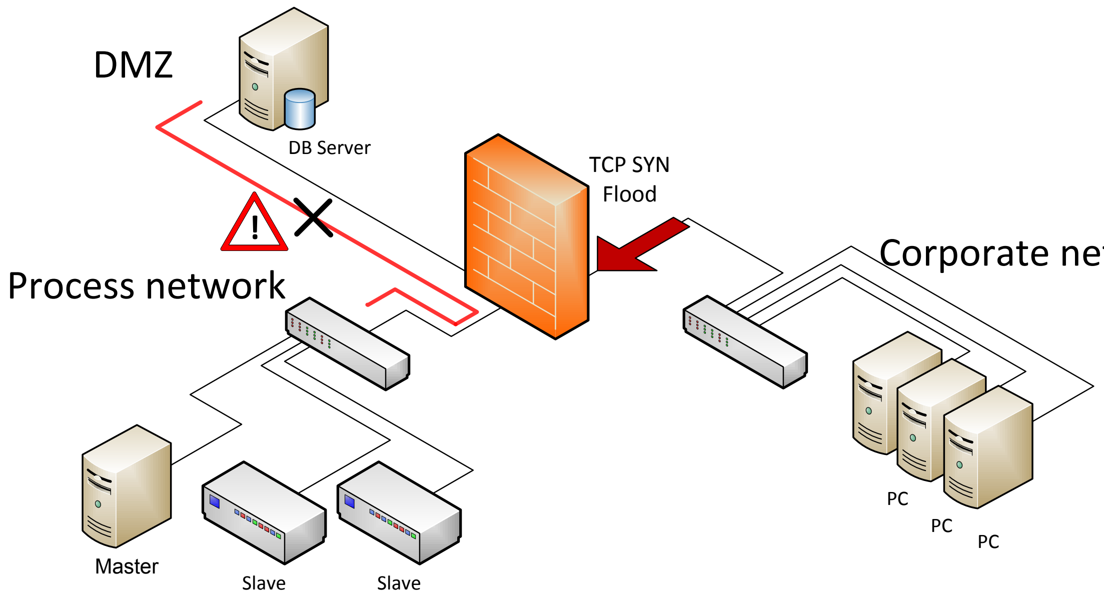
MES: Manufacturing Execution Systems
PDM: Process Data Management
MRO: Maintenance Repair and Overhaul
CAPP: Computer Assisted Process Planning

A modern SCADA network



ICS vs. ICT: *One size fits all ?*

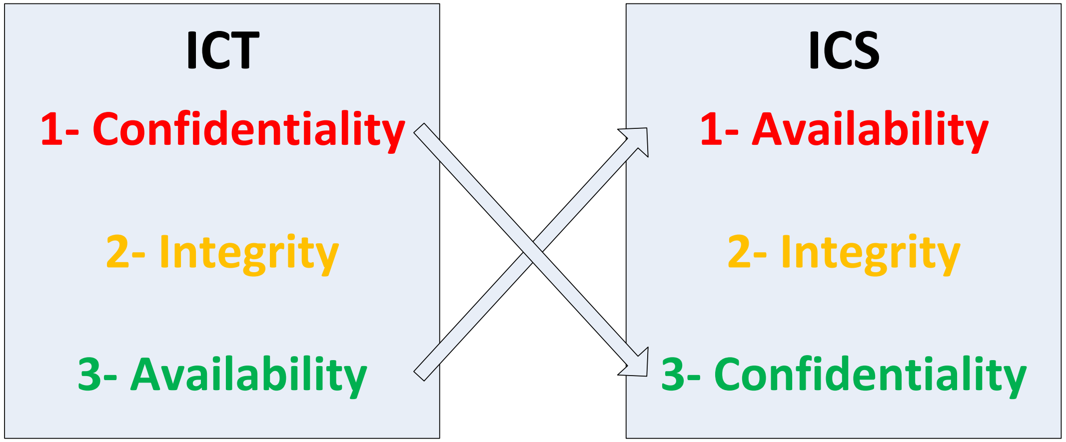
Many of the protection measures used in standard ICT security frameworks (firewalls, IDSs and other) can be adapted for the process control and SCADA environments.



This has the drawback of introducing some security risks, mainly because there are some assumptions regarding ICT networks that not always are equally true in ICS environments.

Cyber-awareness in ICS: why ?

ICS systems have a different set of priorities, when compared with ICT infrastructures.



This situation calls for a domain-specific approach to cyber threat handling in ICS systems, designed to address its specific characteristics.

ICS-oriented cyber-awareness constitutes one of the core contributions of the CockpitCI project and it's the main guiding principle for oriented developments.

The CockpitCI project

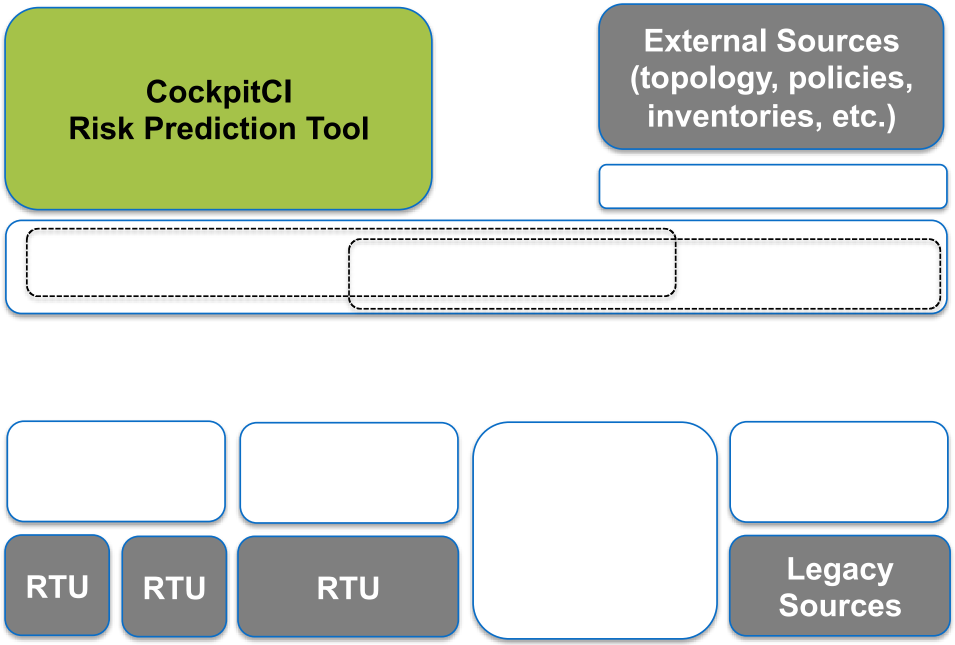
Past projects (particularly the MICIE project) have proved that increasing cooperation among infrastructures' owners by sharing information leads to better previsions.

However such an integration is not enough in order to quickly and effectively react to all adverse events that may occur over the System of Systems and, in particular, to face cyber attacks.

To overcome this limitation, the CockpitCI project aims **provide cyber threat awareness to ICS systems**, leveraging the legacy from MICIE and adding a contextual approach to cyber threat management.

The CockpitCI Cyber-analysis and detection layer

The CockpitCI project includes a cyber analysis and detection layer that must work as a soft real-time Distributed Monitoring System and Perimeter Intrusion Detection System (PIDS).



It must be able to develop and deploy smart detection agents to monitor the potential cyber threats according to the types of networks (SCADA, IP…) and corresponding devices.

Reference architecture

A generic probing architecture

The proposed cyber detection and analysis architecture builds on a distributed infrastructure that aggregates several probing and monitoring points, working together on close coordination, along three security zones:

IT Network, **Operations Network,** **Field Network**.

This multi-zone topology provides a contextual approach to the problem of probe placement. It has two purposes:

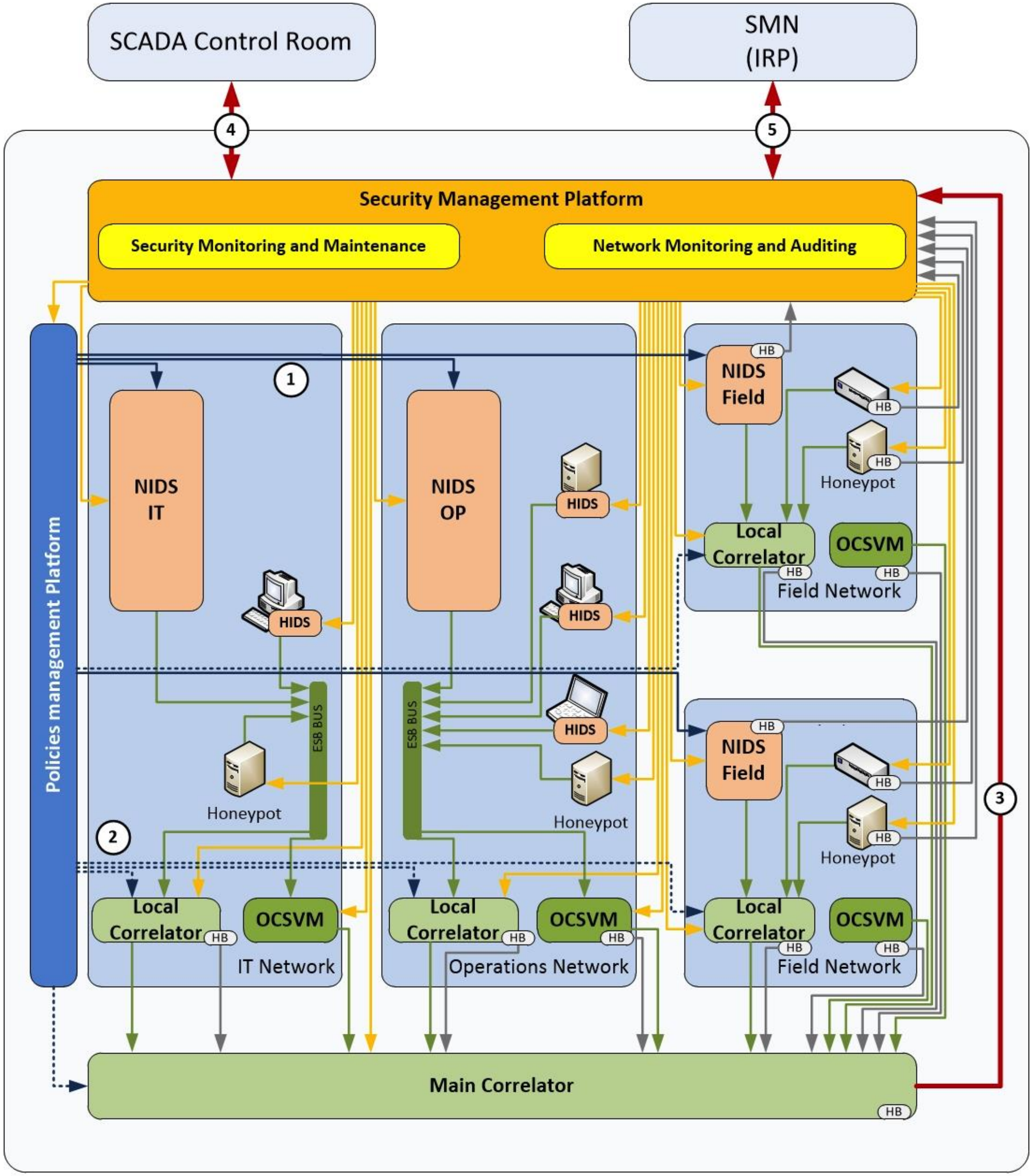
- To separate different infrastructure contexts for which different detection, analysis/inference strategies might apply.
- To provide well-defined security perimeters between each zone, which are critical to provide mediation mechanisms which may inspect and control information flows between each one.

CockpitCI Cyber Analysis and Detection

Legend:

HB – Heart Beat Mechanism
NIDS – Network Intrusion Detection System
HIDS – Host Intrusion Detection System
OCSVM – One Class Support Vector Machines
ESB – Enterprise Service Bus

1. Detection Policies
2. Correlation Policies
3. Anomaly and Security Event Detection
4. Management Information and alarms
5. Processed events and IRP results



Cockpit CI

Event analysis and correlation

Event analysis and correlation

CockpitCI analysis architecture

Objective: provide automatic intrusion detection and alarm generation for SCADA system protection

• In this perspective, two different solutions are used for implementing the analysis layer for automatic intrusion detection:

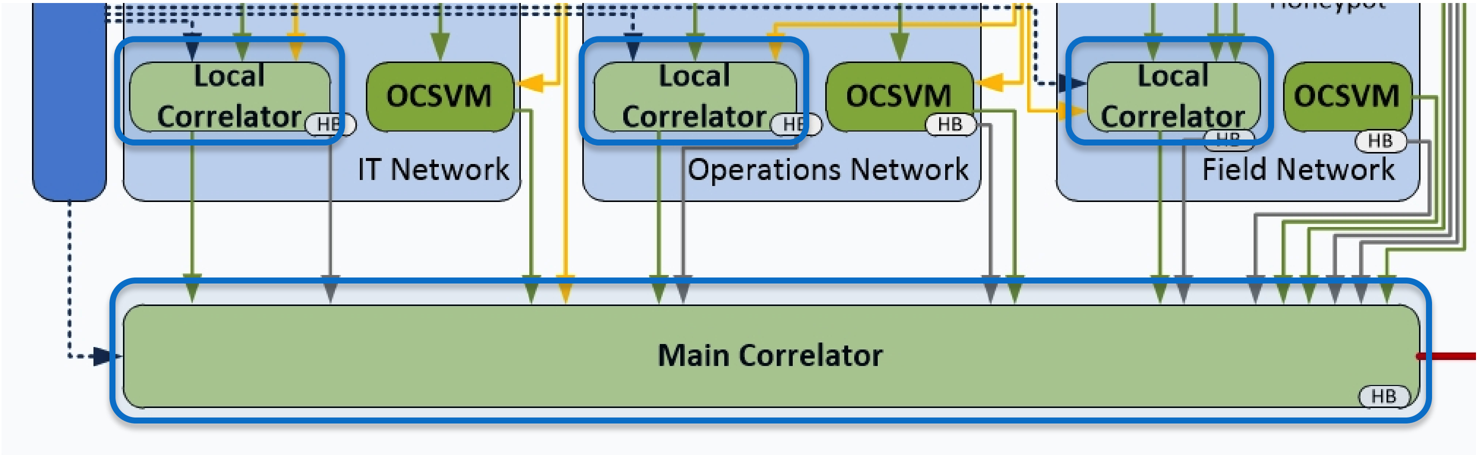
- **Rule-based correlation techniques**.
- Use of **machine-learning** for anomaly detection.

• Being impossible to perform security analysis tasks within a realtime processing timeframe, this architecture opts instead for a “soft-realtime” approach.

• Attacks, rather than being instantaneous events, are comprised by a series of operations executed within a finite time window – nevertheless, effective reaction must necessarily depend on a careful analysis on the threat.

Two-level correlation

A two-level correlation approach implicitly incorporates contextual knowledge about the network topology, while improving scalability:

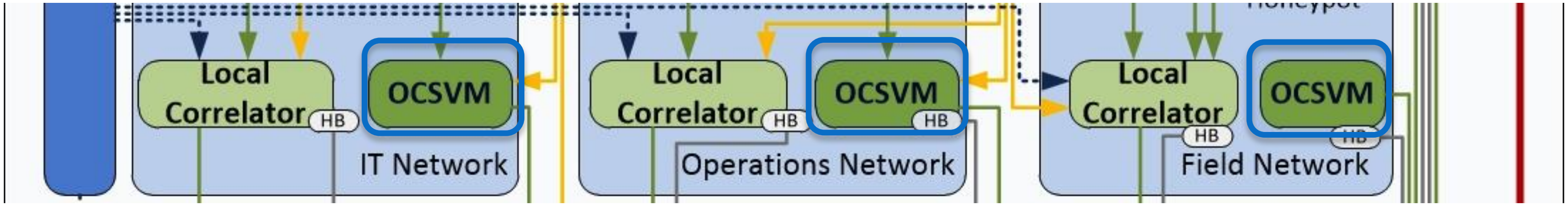


- **The local correlator** collects the events from the sensors or agents and performs the processing of alerts. Local correlator configuration is customized accordingly to the nature of its network zone.

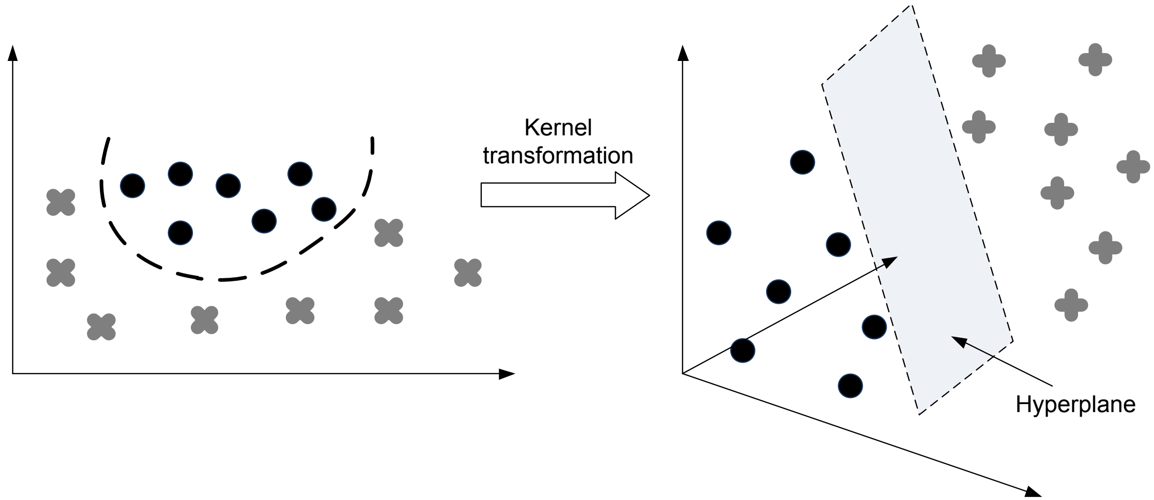
- **The main correlator** is primarily focused in Multi-Step and Attack Focus Recognition. By having a “global view” of the infrastructure, it is able to detect network traversal attacks, a specific type of Multi-Step attacks.

Anomaly detection via machine learning (OCSVM)

OCSVM (One-Class Support Vector Machine)



- Extension of SVM for the case of unlabelled data
- SVM: two-class classification algorithm and requires labelled data. Uses a Kernel function to map the data into a space where it is linearly seperable

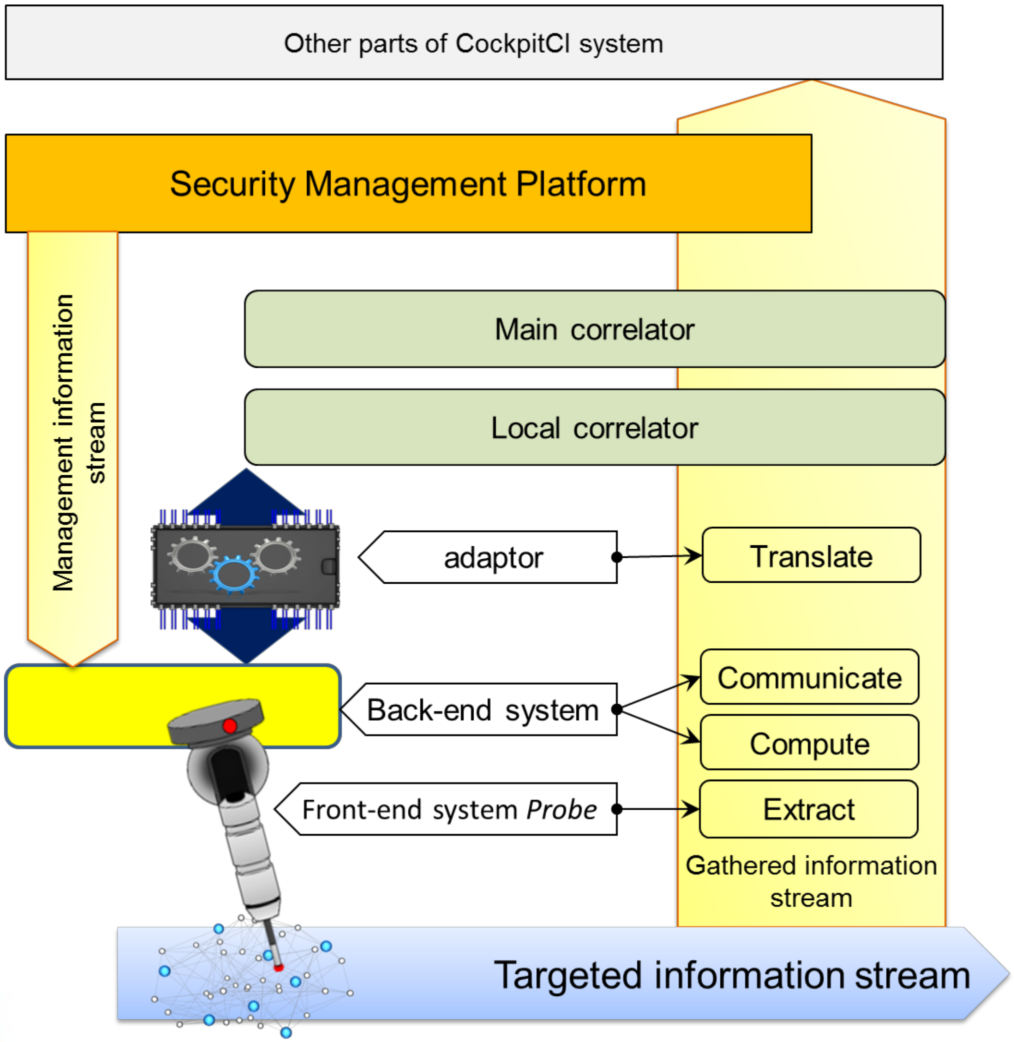


Operation of OCSVM has two phases: Training and Testing

Detection Agents and Field Adaptors

The generic detection and analysis workflow

Focus on the lowest level of the CockpitCI system



List of detection agents

Name	Short Description	Scope
Network Intrusion Detection System	Monitor the traffic on a network segment or perimeter	**IT / OP / Field**
Host Intrusion Detection System	Monitor a specific host system	**IT / OP**
Honeypot (conventional and SCADA-specific)	Provide a decoy components to detect cyber-attempts (A SCADA Honeypot was developed by the project.)	**IT / OP / Field**
Update Checker	Assess component vulnerability	**IT / OP**
Exec Checker	Control exec code in traffic	**IT / OP**
Configuration Checker	Monitor the integrity of system configuration	**IT / OP**
Behaviour Checker	Monitor the behaviour (such as T° , system load…)	**IT / OP / Field**
Output traffic control	Control the integrity of components by examining generated network traffic	**IT / OP**

Cockpit CI

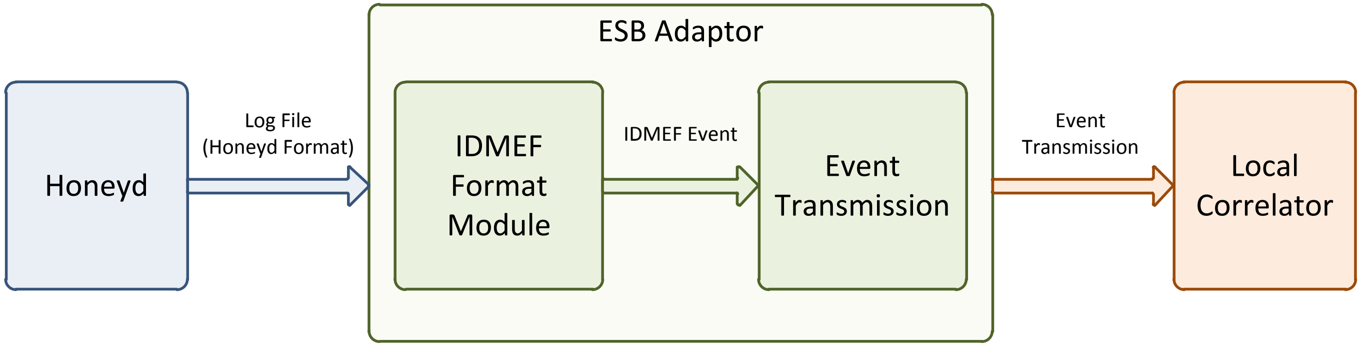
PIDS Architecture: integration

PIDS Architecture: integration

Detection layer component integration

An ESB (Event Service Bus) provides interfacing between detection and analysis. It is based on a Message Oriented Middleware framework .

“Gluing” together the disparate components that constitute the cyber analysis and detection layer, also providing a shared interface for event streaming and delivery.



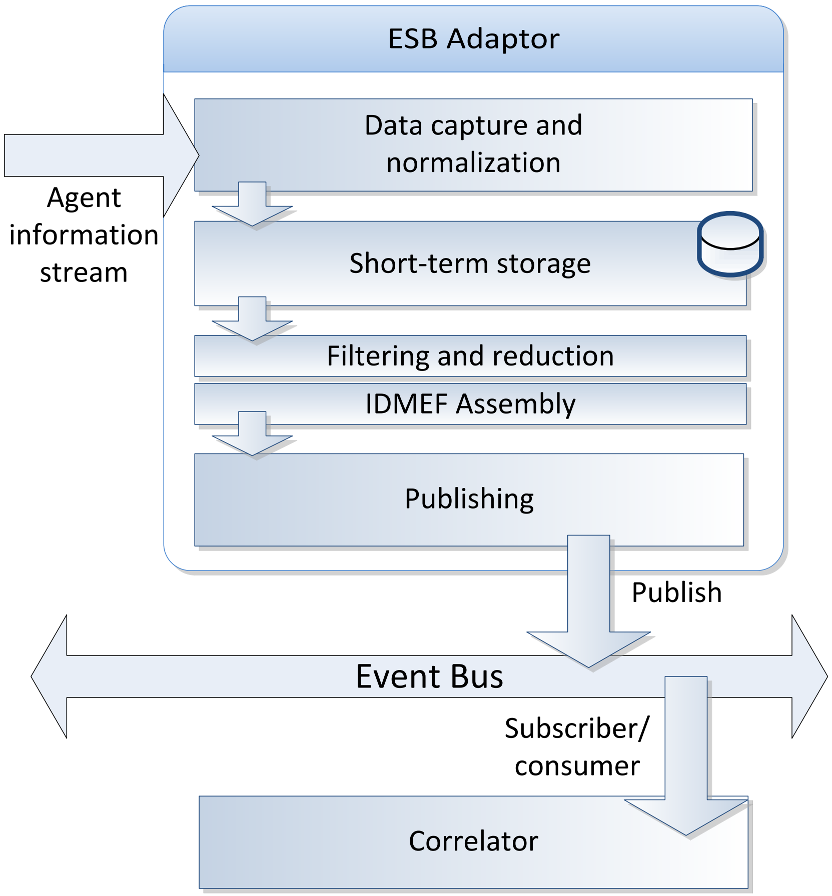
The eventing interface between each component and the ESB is responsible for parsing and filtering events, also being able to store them on a local short-term database, used for event filtering and aggregation.

There is also an adaptor to provide the management API for each component.

Detection layer component integration

ESB + queuing:

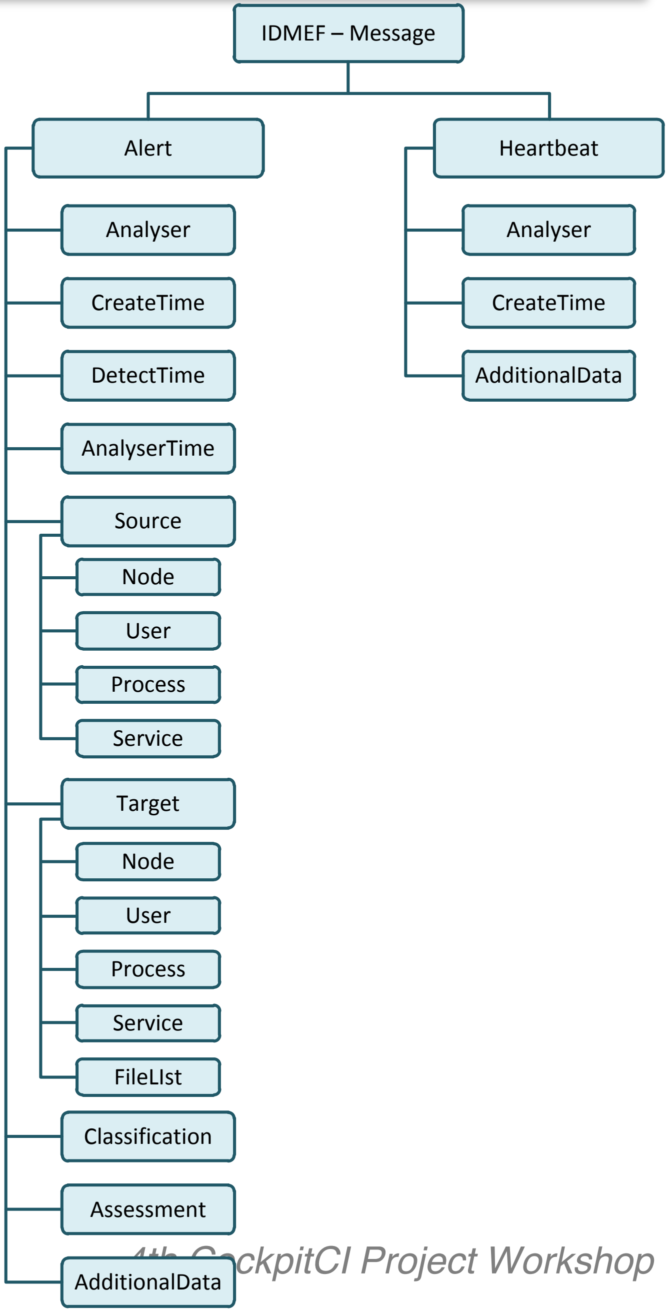
- Provides temporal (sequence) integrity
- Provides scalability for multi-provider, multi-consumer topologies
- Provides backlog management for disconnection events
- Eases integration



Message format - IDMEF

Why IDMEF ?

- One of the informal standards for security events (RFC4765).
- It is XML-based.
- It's extensible and simple to parse. Its processing is a low-overhead task.
- Neutral message format.



Conclusions and next developments

The Cyber Detection and Analysis Layer departs from the conventional ICT IDS paradigm to offer a complete solution to deal with ICS cyber-security.

It is not a solution exclusively designed for the SCADA scope, going one step further to cover the complete ICS cyber security scope. Also, it was designed to scale and be flexible enough to meet the needs of ICS infrastructures, while providing consolidated management and orchestration features.

It integrates a wealth of detection agents with diverse capabilities (such as stealthiness), including completely new techniques, but also known approaches introduced for the first time in such contexts.

It is able to detect both **known** and **rogue threats**, thanks to the use of contextual and topological analysis and processing strategies based on machine learning and rule-based techniques.

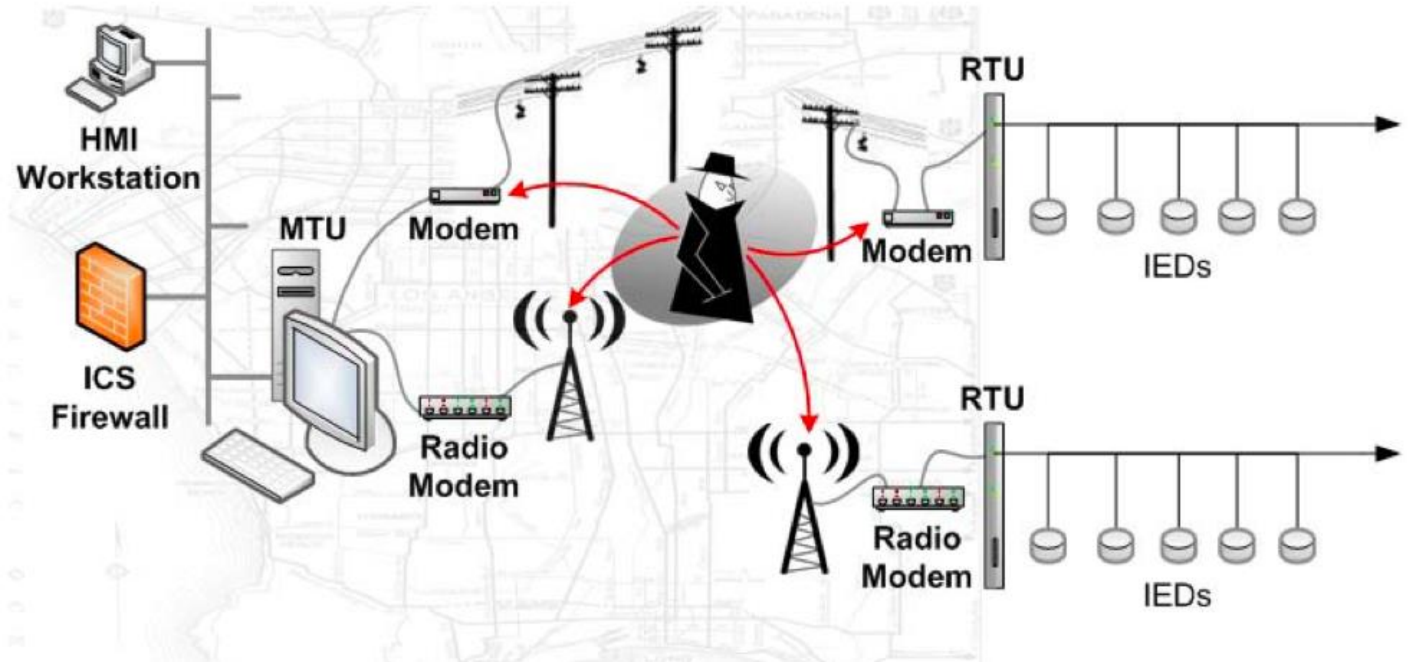
Cockpit CI

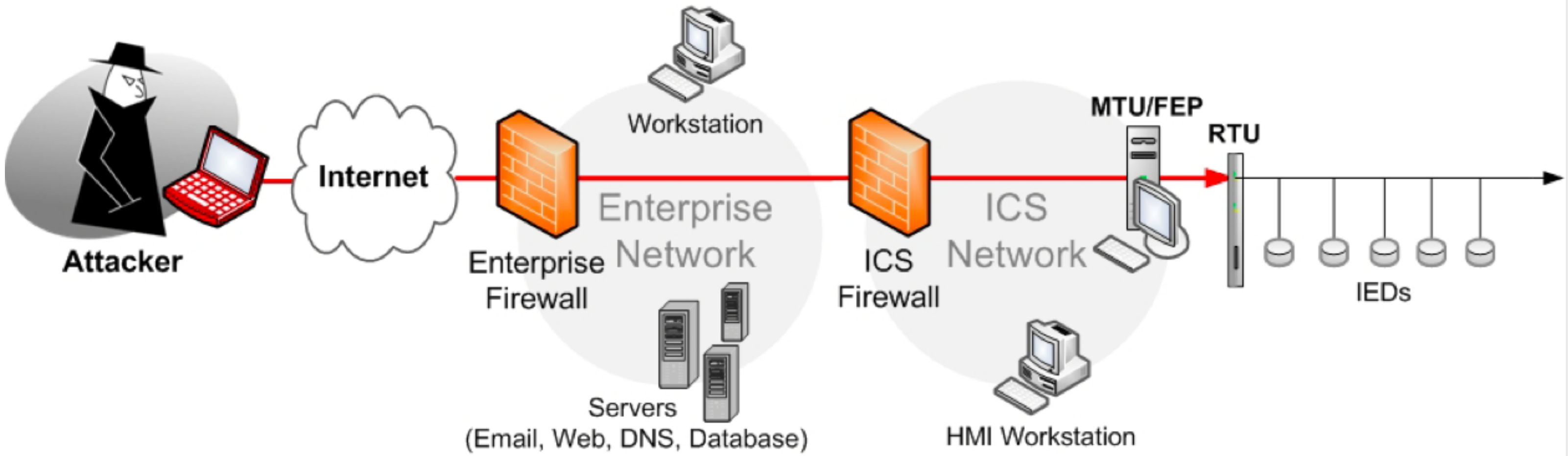
Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Thank you for your attention

We all see where this is going…

Attack scenarios





Doomsday at the distance of one click ? Almost…

Estonia suffered a series of cyber attacks that began 27 April 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn.

The **South Florida blackout**, in 2008, left almost 4 million customers without electricity. Some experts blame this event on a cyber-attack.

In 2010, **Stuxnet**, a trojan designed to attack Siemens Step7 HMI software and S7 PLCs temporarily set back **Iran's nuclear program** . It almost ruined one-fifth of the Iranian nuclear centrifuge by spinning out of control while simultaneously replaying recorded system values to fake normal system behaviour during the attack.

2007

CIA: Cyberattack caused multiple-city blackout

By Tom Espiner
Special to CNET News.com

A cyberattack has caused a power blackout in multiple cities outside the United States, the CIA has warned.

The SANS Institute, a computer-security training body, reported the CIA's disclosure on Friday. CIA senior analyst Tom Donahue told a SANS Institute conference on Wednesday in New Orleans that the CIA had evidence of successful cyberattacks against critical national infrastructures outside the United States.

"We have information that cyberattacks have been used to disrupt power equipment in several regions outside the U.S.," Donahue said. "In at least one case, the disruption caused a power outage affecting multiple cities."

Donahue added that the CIA does not know who executed the attacks or why but that all of the attacks involved "intrusions through the Internet."

Related Stories

China accused of cyberattacks on New Zealand
September 13, 2007

Homeland Security IT chief blamed for cyberwoes

2013

Napolitano Warns Downed Power Grid Is Inevitable Due To Cyber Attack

Written by: Tara Dodrill Alternative Energy September 9, 2013 0

A major cyber attack will one day disrupt life as we know it in the United States.

So says former Department of Homeland Security Secretary Janet Napolitano, who made the comments during her finals days in the post.

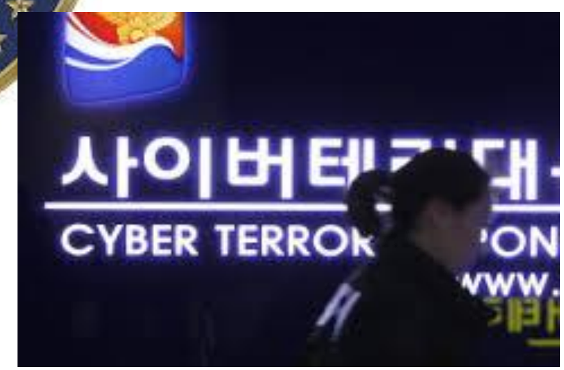
image credit abcnews.go.com

The then-Obama administration official stated during a speech that it was a matter of "when" not "if" the power grid would go down due to a cyber attack. Many feel that smart grid technology and an increase in the installation of smart meters will make the power grid even more susceptible to hackers.

Janet Napolitano described her time heading the Department of Homeland Security as successful because no terror attacks occurred during her tenure.

Cyberwarfare

C^5I (command, control, communications, computers, combat systems, and intelligence) units are being set-up everywhere.



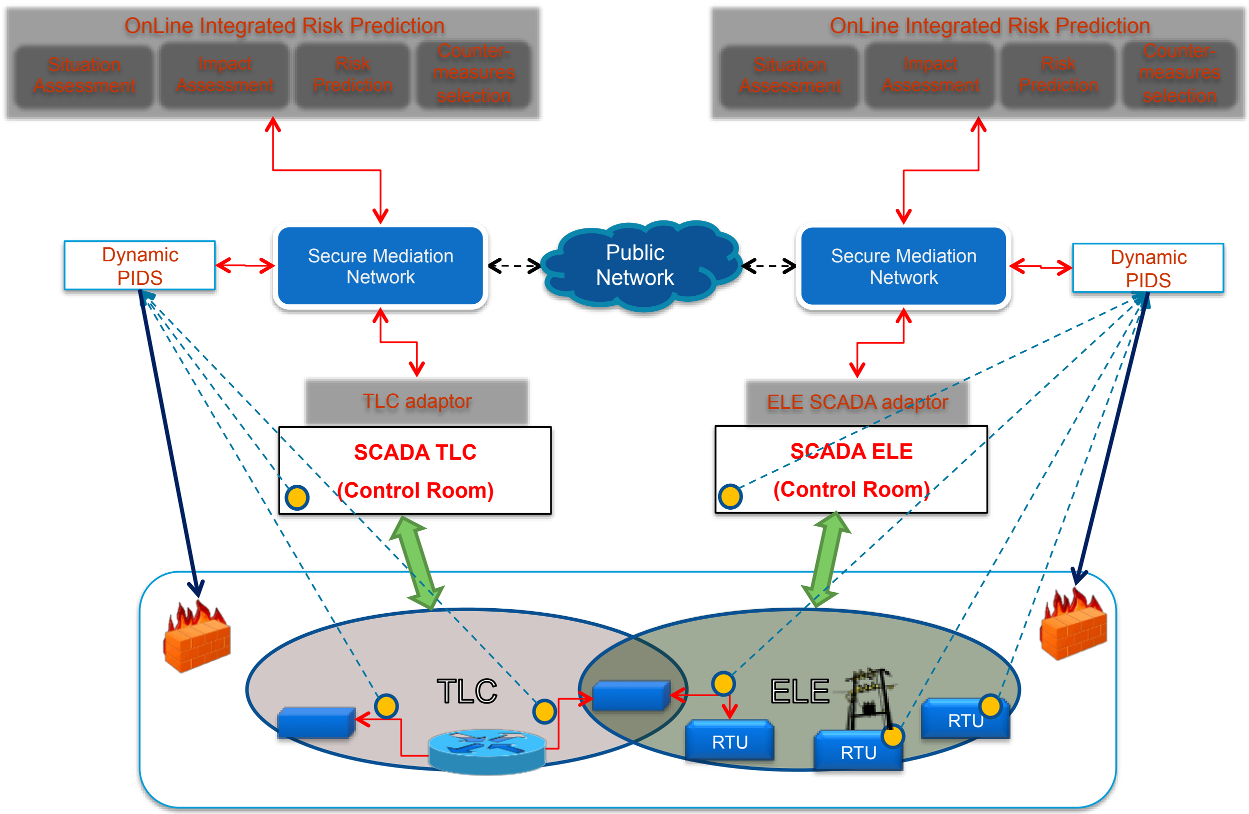
Tactically speaking, C^5I capabilities are an operational force multiplier.

Cyberwarfare

Cockpit CI

The CockpitCI Cyber-analysis and detection layer

For each CI, there is a Perimeter IDS that receives information from detection agents.



Each each field network demarcates an area where autonomous response capabilities, might be deployed and available).

Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Integrated Detection Mechanism

4th CockpitCI Workshop (Bucharest 16.09.2014)

Leandros Maglaras & Jianmin Jiang

University of Surrey

Information Society

Scada systems - Cyber attacks

Cyber-attacks can come from any part of the infrastructure:

1. **FIELD Network** as SCADA systems
2. **OPERATION Network** as Telco system or monitoring management system
3. **IT Network** as enterprise devices and services

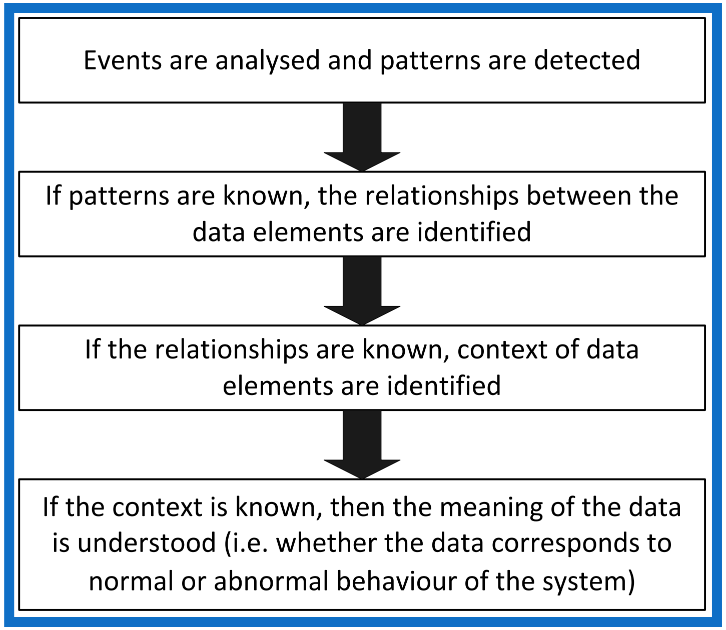
Kinds of **cyber attacks:**

1. Denial of Service (**DoS**)
2. Accidental or malicious infections by **worms**
3. **Spoofing** attacks/**Man-In-The-Middle** attacks
4. **Authentication violation**

Cockpit CI

Network monitoring
Detection and classification

- **Feature extraction**
- **Per packet – per flow analysis**
- **Parameter calibration**
- **Performance evaluation metrics (TP, TN, FP,…)**
- **Machine learning algorithms**
  a. Naïve Bayes
  b. Clustering
  c. Markov chains
  d. **Support Vector Machines**



Threat identification by **machine learning**

Cockpit CI

OCSVM for SCADA systems

- **OCSVM** does not require any **signatures** of data to build the detection model
- **OCSVM** is capable of detection both known and unknown (**novel**) attacks
- In practice training data, taken from **SCADA** environment, could include **noise** samples - **OCSVM** detection approach is robust to noise samples
- Algorithm **configuration** can be controlled by the user to regulate the percentage of anomalies expected
- **OCSVM** detectors can operate **fast** enough for online detection
- **OCSVM** is capable of handling **multiple** attributed data (many features)

IT- OCSVM : Integrated detection mechanism

- **Pre-processing** of raw input data, feed the OCSVM module
- Selection of the most appropriate **features** for training of the OCSVM
- Creation of **cluster of OCSVM** models trained on discrete datasets
- **Testing** of the traffic dataset that contain malicious attacks
- **Ensemble of Classifiers** (voting)
- **Social analysis** based on network traces
- **Fusion** of the information gathered OCSVMs
- Creation of **IDMEF** files that describe the nature of the alert, in terms of importance, the position in the system, time.

Features

Central OCSVM

A/A	Network Data feature	Type of feature
1	Packet size	Content based
2	Rate	Time based
3	Num_packets_dst	Time based
4	Num_packets_src_dst	Time based
5	Num_ARP_packets	Time based

$$Packet_{scaled} = \frac{packet\ size}{Max\ packet\ size}$$

$$Rate_{scaled} = \frac{Time\ difference}{Max\ time\ difference}$$

$$\text{Num\_packets\_dst} = \sum_{k=1}^{10} \mathrm{a} * 0.1, \text{ where } \begin{cases} a = 1\ if\ destination\_packet(i-k) = destination\_packet(i) \\ a = 0\ if\ destination\_packet(i-k) <> destination\_packet(i) \end{cases}$$

$$Num\_packets\_src\_dst = \sum_{k=1}^{10} \mathrm{a} * 0.1, \text{where} \begin{cases} a = 1\ if\ destination\_packet(i-k) = destination\_packet(i)\ and\ source\_packet(i-k) = source\_packet(i) \\ a = 0\ if\ destination\_packet(i-k) <> destination\_packet(i)\ or\ source\_packet(i-k) <> source\_packet(i) \end{cases}$$

$$\text{Num\_ARP\_packets} = \sum_{k=1}^{10} \mathrm{a} * 0.1, \text{ where } \begin{cases} a = 1\ if\ packet\_protocol\left(i-k\right) = ARP \\ a = 0\ if\ packet\_protocol\left(i-k\right) <> ARP \end{cases}$$

Cockpit CI

Cluster of OCSVMs

frame.number	frame.time_epoch	source	destination
5	1399045733	50:b7:c3:8d:7a:5d	ff:ff:ff:ff:ff:ff
6	1399045733	30:f9:ed:c0:34:33	ff:ff:ff:ff:ff:ff
7	1399045733	172.27.224.32	172.27.224.3
8	1399045733	172.27.224.32	172.27.224.3
9	1399045733	30:f9:ed:c0:34:33	ff:ff:ff:ff:ff:ff
10	1399045733	172.27.224.3	172.27.224.32
12	1399045733	172.27.224.32	172.27.224.3
13	1399045733	172.27.224.3	172.27.224.32
14	1399045733	172.27.224.32	172.27.224.3
15	1399045733	172.27.224.3	172.27.224.32
16	1399045733	172.27.224.32	172.27.224.3
17	1399045733	172.27.224.3	172.27.224.32
18	1399045734	172.27.224.32	172.27.224.3
19	1399045734	172.27.224.3	172.27.224.32
22	1399045734	172.27.224.32	172.27.224.3
23	1399045734	172.27.224.3	172.27.224.32
24	1399045734	10.3.3.28	230.0.0.1
25	1399045734	10.3.3.28	230.0.0.1
26	1399045734	172.27.224.32	172.27.224.3
27	1399045734	30:f9:ed:c0:34:33	ff:ff:ff:ff:ff:ff
28	1399045734	172.27.224.3	172.27.224.32
30	1399045734	172.27.224.32	172.27.224.3
31	1399045734	172.27.224.33	172.27.224.3
32	1399045734	172.27.224.3	172.27.224.33
33	1399045734	30:f9:ed:c0:34:33	ff:ff:ff:ff:ff:ff

Central OCSVM

frame.num	frame.time_epoch	destination	frame.protocols	frame.len
7	1399045733	172.27.224.3	eth:ip:tcp	60
8	1399045733	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
12	1399045733	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
14	1399045733	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
16	1399045733	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
18	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
22	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
26	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
30	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
41	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
43	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
45	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
47	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
49	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
51	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
54	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
56	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68
61	1399045734	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
70	1399045734	172.27.224.3	eth:ip:tcp	60
71	1399045735	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
74	1399045735	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
76	1399045735	172.27.224.3	eth:ip:tcp:mbtcp:modbus	66
78	1399045735	172.27.224.3	eth:ip:tcp:mbtcp:modbus	68

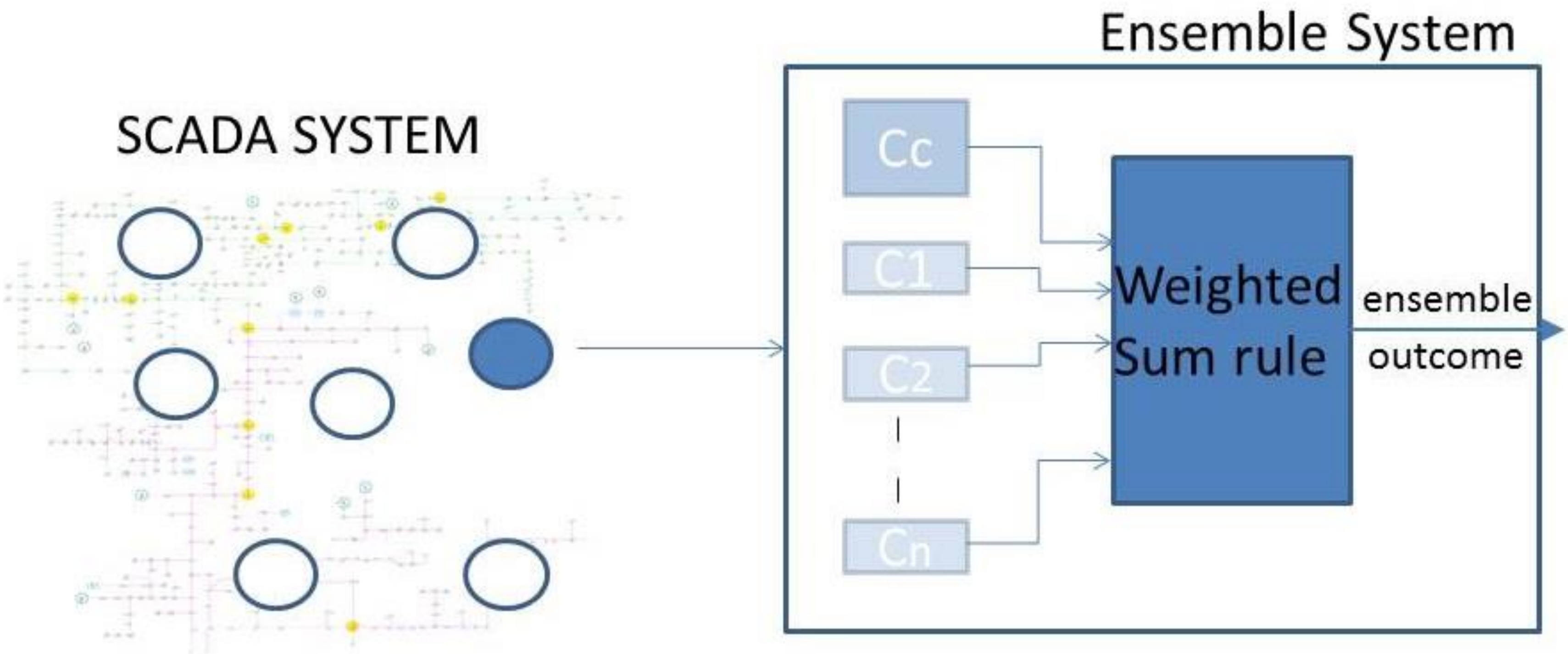
Split OCSVM

frame.number	frame.time_epoch	destination	frame.protocols	frame.len
2	1399047346	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
5	1399047346	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
6	1399047346	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
8	1399047346	172.27.224.33	eth:ip:icmp:data	98
10	1399047346	172.27.224.32	eth:ip:tcp:mbtcp:modbus	66
17	1399047346	172.27.224.32	eth:ip:tcp:mbtcp:modbus	66
19	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
23	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
25	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
27	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
29	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	66
47	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	66
49	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
53	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
55	1399047347	172.27.224.33	eth:ip:icmp:data	98
57	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
59	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64
61	1399047347	172.27.224.32	eth:ip:tcp:mbtcp:modbus	66
72	1399047348	172.27.224.32	eth:ip:tcp:mbtcp:modbus	66
74	1399047348	172.27.224.32	eth:ip:tcp:mbtcp:modbus	64

Split OCSVM

Cockpit CI

Ensemble system



Cc – Central OCSVM

$C_{1\text{-}n}$ – Split OCSVM

IT-OCSVM

IT-OCSVM in operation

$$q_e(i,j) = \sum_{n=1}^{N} w_i d_t(i,j)$$

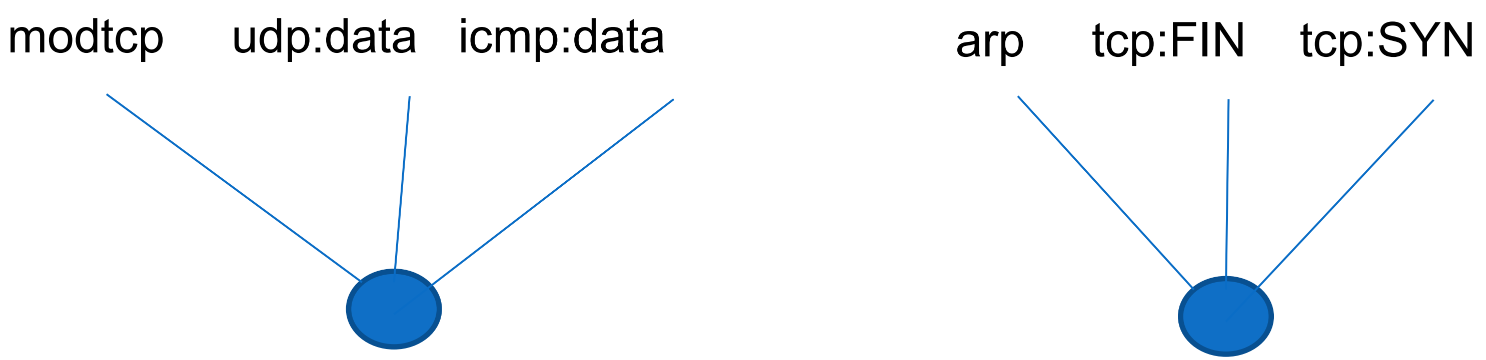
Social metrics

Spearman's correlation coefficient – based on used protocol

$$p = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)}$$

The final output is a number that indicates whether there is a differentiation in the way that each source behaves during the training and the testing period

$$q_s(i,j) = \frac{q_e(i,j)}{p_j}, \forall\ q_e(i,j)\ with\ source\ node\ j$$



Most used protocols used by a node during normal (left) and abnormal (right) operation

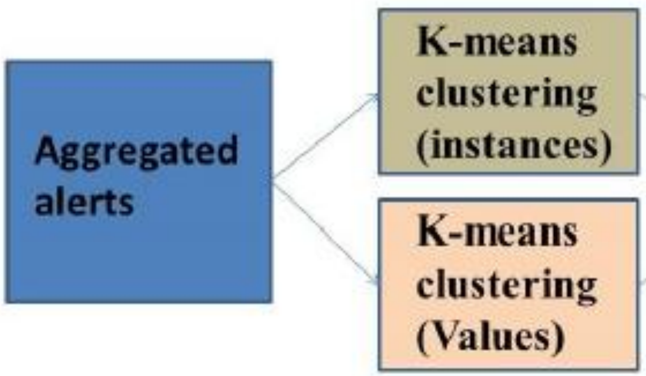
Fusion of alarms

1st Stage : Aggregation :

$$qa_j = \sum_i q_s(i,j), \quad qb_j = \sum_i 1, \forall\ q_s(i,j)\ with\ source\ node\ j$$

2nd Stage : Clustering - Categorization

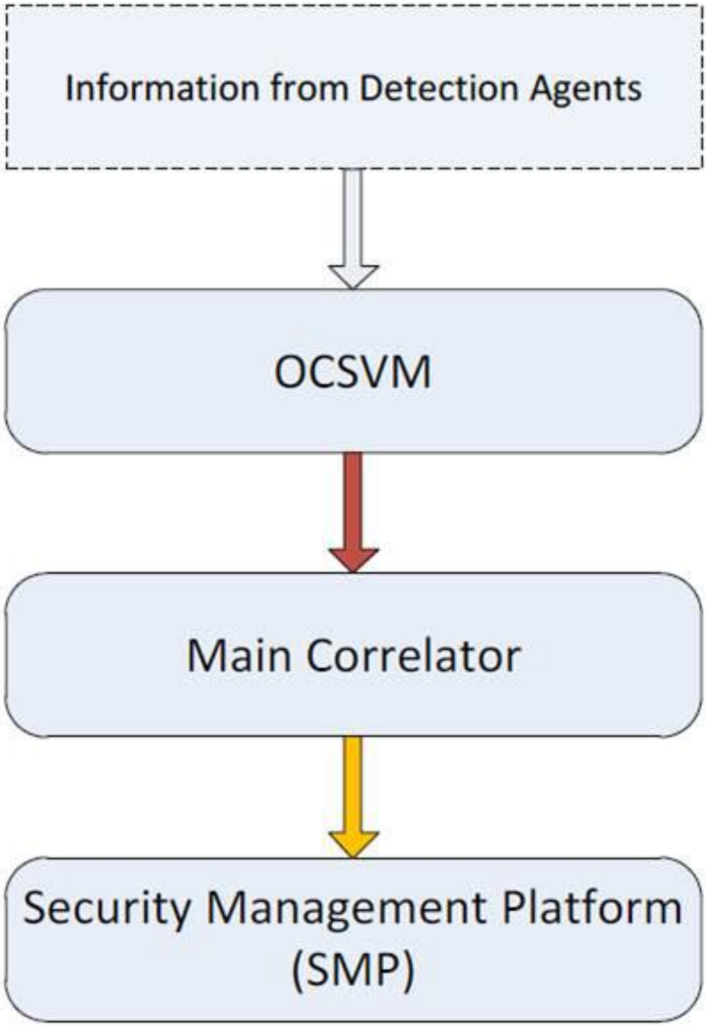
$$SSE = \sum_{k=1}^{K} \sum_{j=1}^{N_k} ||qa_j - \mu_k||^2$$



K-means (instances)	K-means (Value)	Final classification
Severe	Severe	Severe
Severe	Possible	Medium
Possible	Severe	Medium
Possible	Possible	Possible

Cockpit CI

Communication - Integration




```
<?xml version="1.0" encoding="UTF-8"?>
- <idmef:IDMEF-Message version="1.0" xmlns:idmef="http://iana.org/idmef">
  - <idmef:Alert>
    - <idmef:Analyzer analyzerid="test">
      - <idmef:Node category="unknown">
          <idmef:location>IT Network</idmef:location>
          <idmef:name>OCSVM</idmef:name>
        </idmef:Node>
      </idmef:Analyzer>
      <idmef:CreateTime ntpstamp="0x1130fdd3.0xa0000000">2014-08-19T16:19:43+01:00</idmef:CreateTime>
    - <idmef:Source>
      - <idmef:Node>
        - <idmef:Address category="ipv4-addr">
            <idmef:address>172.27.224.32</idmef:address>
          </idmef:Address>
        </idmef:Node>
      </idmef:Source>
    - <idmef:Target>
      - <idmef:Node>
        - <idmef:Address category="ipv4-addr">
            <idmef:address>172.27.224.3</idmef:address>
          </idmef:Address>
        </idmef:Node>
      </idmef:Target>
      <idmef:Classification text="SEVERE ALARM"/>
    </idmef:Alert>
</idmef:IDMEF-Message>
```


IDMEF messages produced by IT-OCSVM

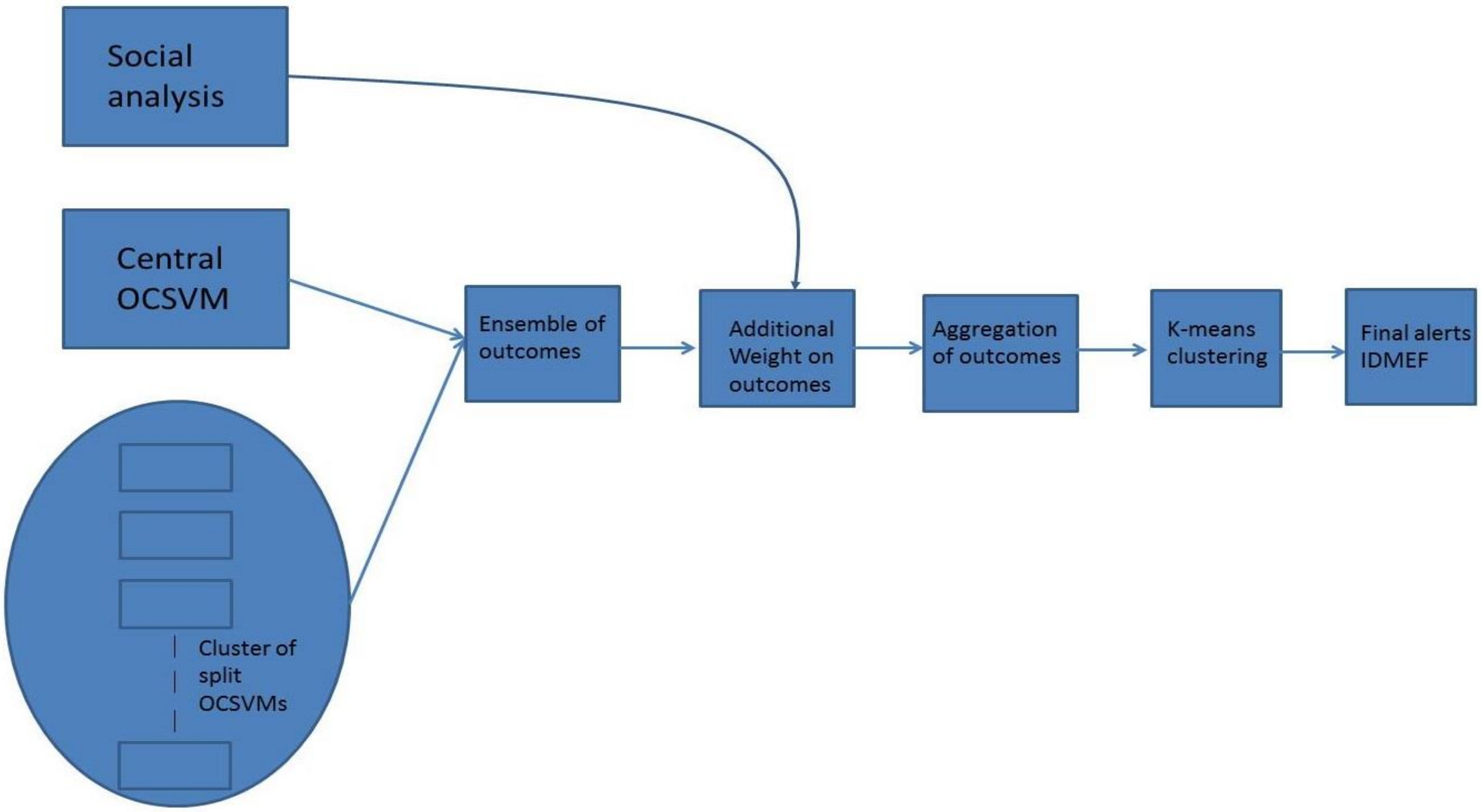
IDMEF files inform about source, destination, time and classification of the event


```
172.27.224.32,eth:ip:tcp:mbtcp:modbus,eth:ip:tcp, , ,
172.27.224.3,eth:ip:tcp:mbtcp:modbus,eth:ip:icmp:data, , ,
172.27.224.33,eth:ip:icmp:data, , , ,
10.3.3.28,eth:ip:udp:data, , , ,
d0:7e:28:8e:40:9b,eth:llc:stp, , , ,
```


Sources file created by IT-OCSVM

Cockpit CI

Architecture of the detection mechanism



Cockpit CI

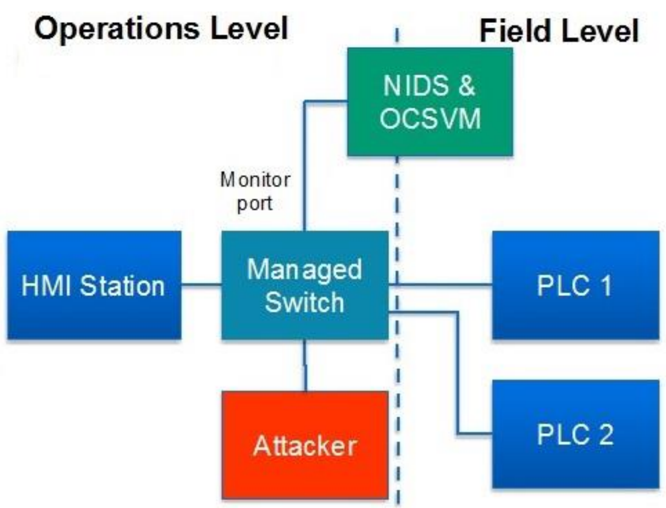
Nature of the trial

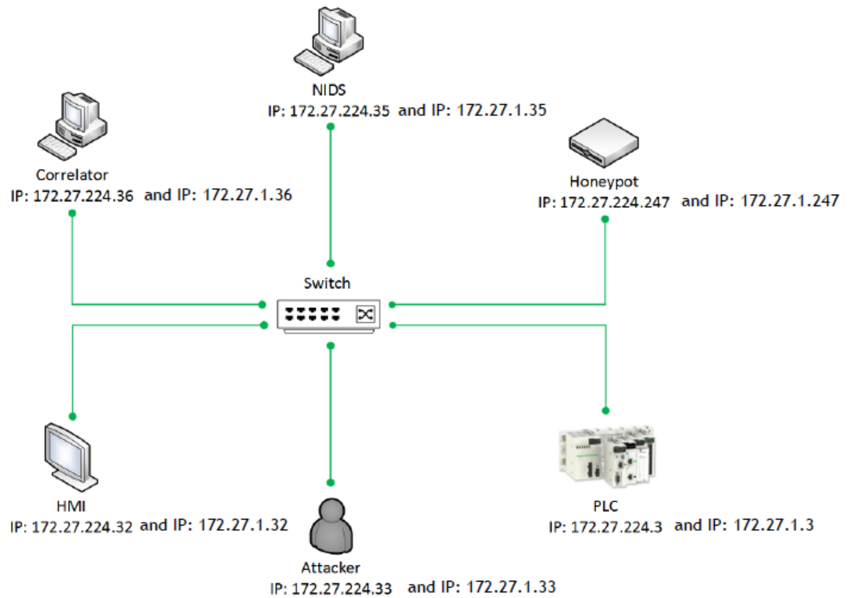
A. **Network scan attack**

B. **ARP spoofing - MITM attack**

C. **DoS attack**

Frame number	Frame time_epoch	Source	Destination	Frame.protocols	Frame.len	Col.info





Transformed datasets

Central OCSVM

```
1 1: 0.18661229987018105 2: 0.05179558011049724 3: 0.0 4: 0.0 5: 0.1
1 1: 4.6638485967466064E-4 2: 0.05041436464088398 3: 0.1 4: 0.1 5: 0.1
1 1: 5.011205741489403E-4 2: 0.04765193370165746 3: 0.2 4: 0.2 5: 0.1
1 1: 0.07182604724705569 2: 0.04143646408839779 3: 0.0 4: 0.0 5: 0.1
1 1: 0.0067294657508171 2: 0.04143646408839779 3: 0.0 4: 0.0 5: 0.1
1 1: 0.04598406510677064 2: 0.04143646408839779 3: 0.2 4: 0.2 5: 0.1
1 1: 0.03813842506418002 2: 0.04143646408839779 3: 0.0 4: 0.0 5: 0.2
1 1: 0.14369331420862086 2: 0.04558011049723757 3: 0.2 4: 0.2 5: 0.2
1 1: 0.021966402690674756 2: 0.04419889502762431 3: 0.1 4: 0.1 5: 0.2
1 1: 0.03862565135253925 2: 0.04558011049723757 3: 0.2 4: 0.2 5: 0.2
1 1: 0.014140214648189736 2: 0.04419889502762431 3: 0.0 4: 0.0 5: 0.2
```

Split OCSVM

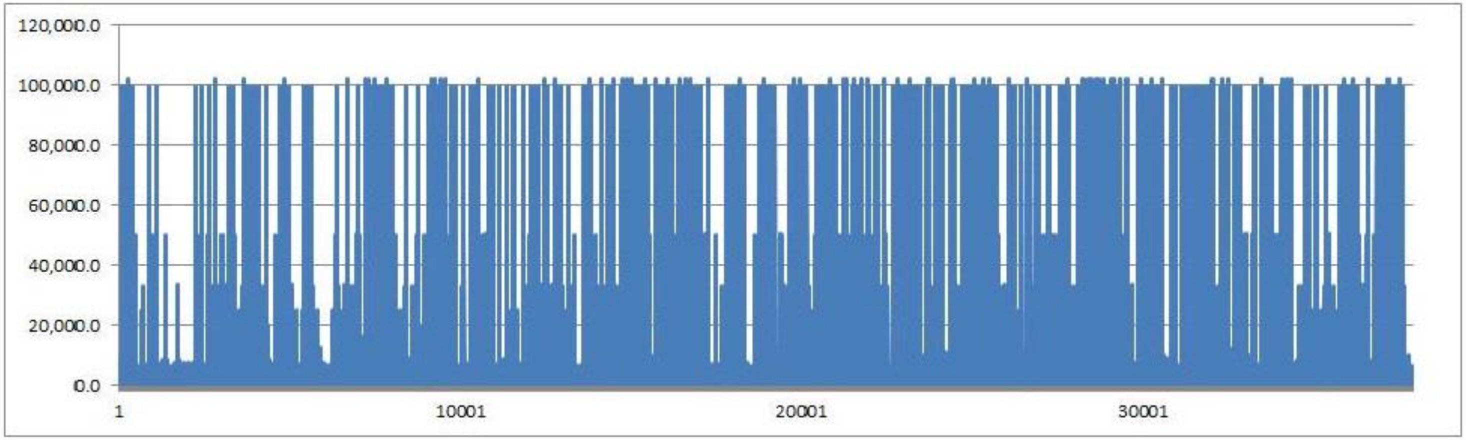
```
1 1: -4.618338530824944 2: 0.6122448979591837 3: 0.0
1 1: -4.747598641215887 2: 0.6122448979591837 3: 0.0
1 1: -4.22820822378137 2: 0.6122448979591837 3: 0.0
1 1: -4.47037156022453 2: 0.6122448979591837 3: 0.0
1 1: -4.282215789767468 2: 0.6122448979591837 3: 0.0
1 1: -4.585233406666963 2: 0.6122448979591837 3: 0.0
1 1: -4.539874534291136 2: 0.6122448979591837 3: 0.0
1 1: -4.565755053271114 2: 0.6122448979591837 3: 0.0
1 1: -4.703581812231512 2: 0.6122448979591837 3: 0.0
1 1: -4.22820822378137 2: 0.6122448979591837 3: 0.0
```

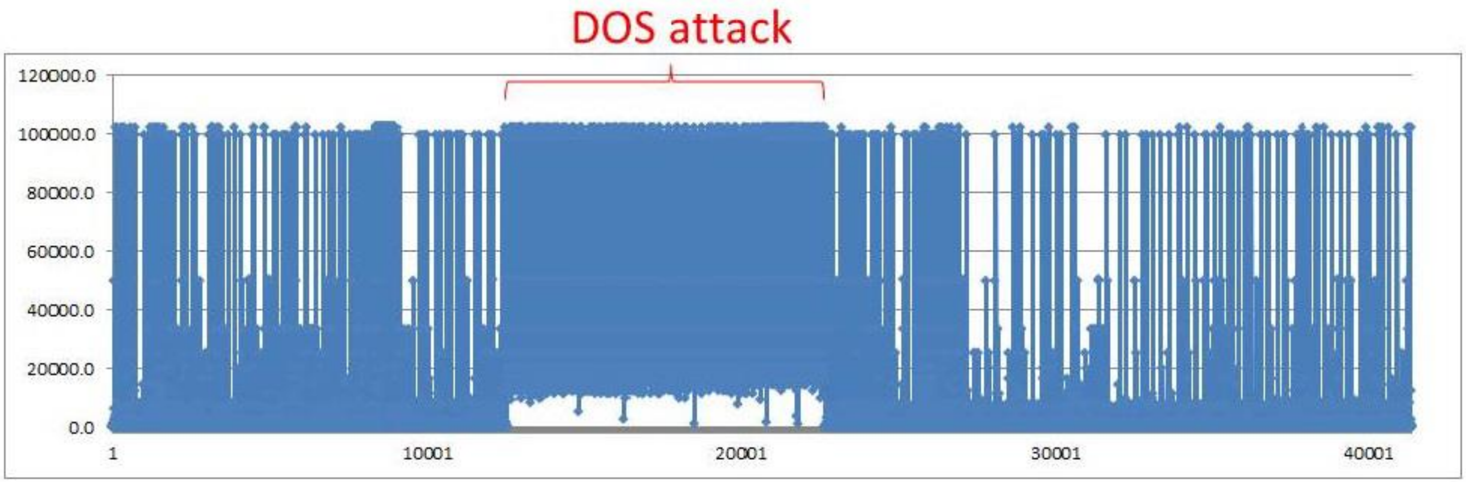
Testing data consists of normal data and attack data and the composition of the data sets are as follows:

- **Testing set-A**’ : 1- 5000 Normal data records
- **Testing set-B**’ : 5000- 10000- Normal data records + Arp spoofing attack + Network scan attack
- **Testing set-C**’ : 10000 – 25000 Normal data records + Dos attack + Network scan attack
- **Testing set-D**’ : 25000- 41000 Normal data records + MITM attack

Cockpit CI

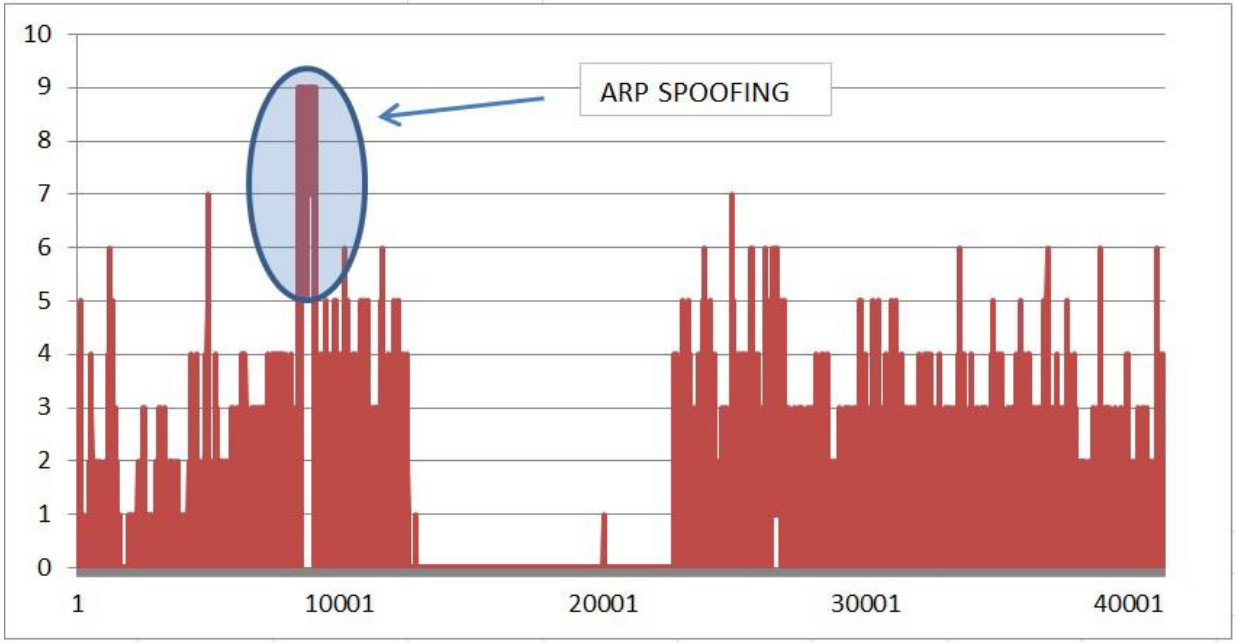
Rate of packets

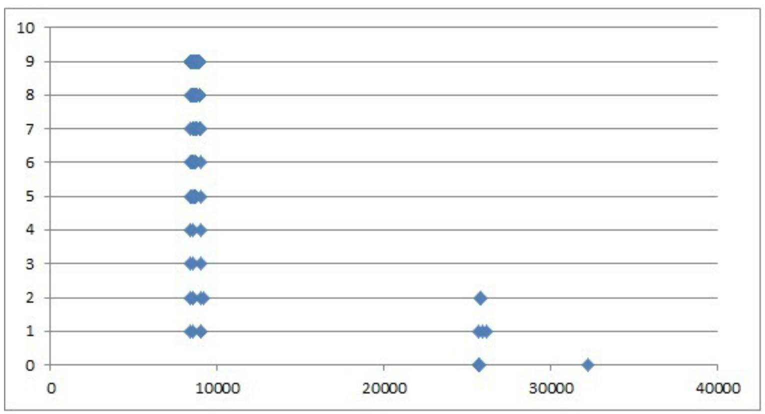


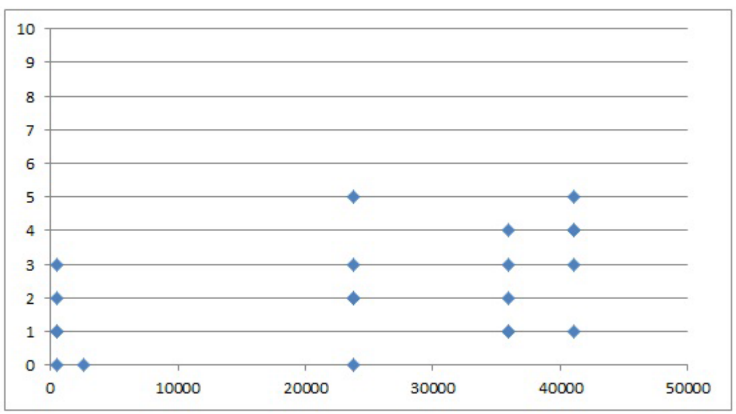


Cockpit CI

ARP spoofing (overall – split datasets)







Cockpit CI

Precision -accuracy

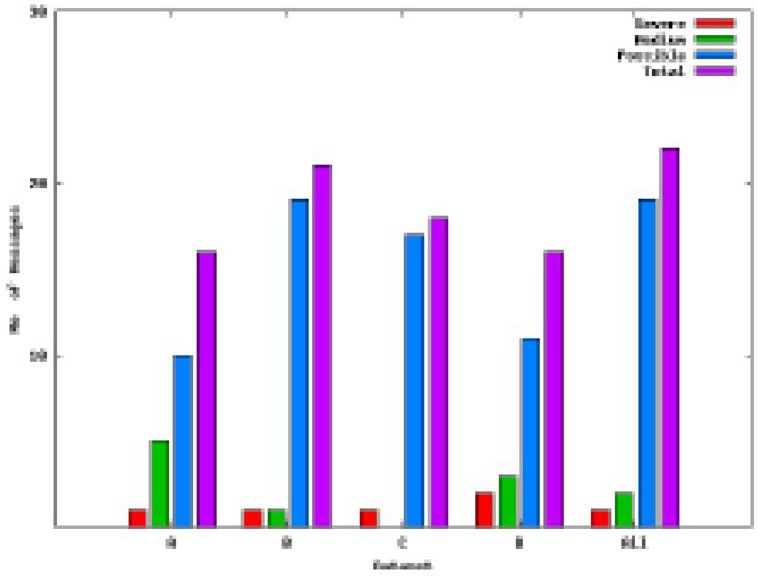
$$Detection\ accuracy = \frac{True\ positives + True\ neganives}{Sample\ size} \times 100\%$$

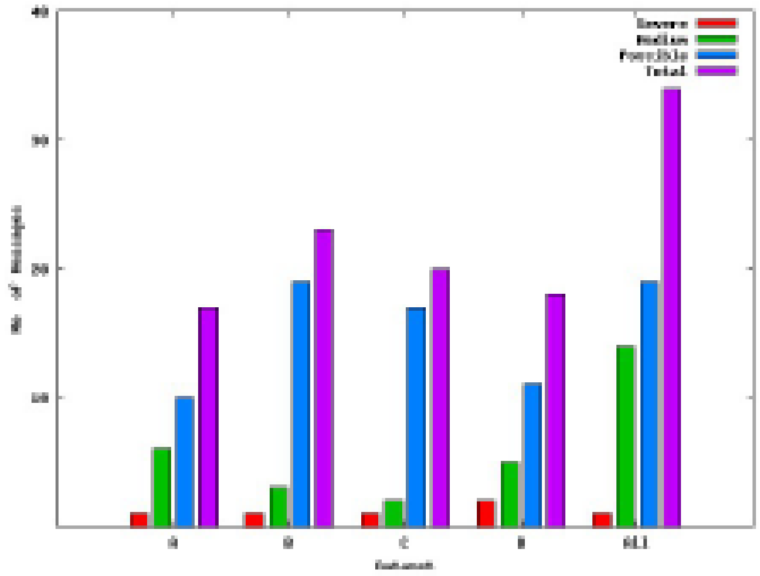
$$Flase\ alarm\ rate = \frac{Flase\ positives}{True\ neganives + Flase\ positives} \times 100\%$$

	DA	FAR
Testing Data set A	98.81%	1.18%
Testing Data set B	94.6%	3.25%
Testing Data set C	95.20%	1.51%
Testing Data set D	96.37%	2.3%
FULL Testing Data set	96.3%	2.5%

Cockpit CI

Impact of the fusion mechanism





Dataset	*Initial alarms*	*Aggregated alarms*
A	129	16
B	658	21
C	9273	18
D	203	16
All	10507	22

Aggregated alarms produced by IT-OCSVM are significantly decreased compared to the initial alarms

IT-OCSVM categorizes aggregated alarms.

Cockpit CI

- Integrated detection mechanism
- Based on OCSVM, Social network analysis
- Automatic Creation of a cluster of split OCSVMs
- Ensemble, aggregation, k-means clustering

Conclusions – Discussion

Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

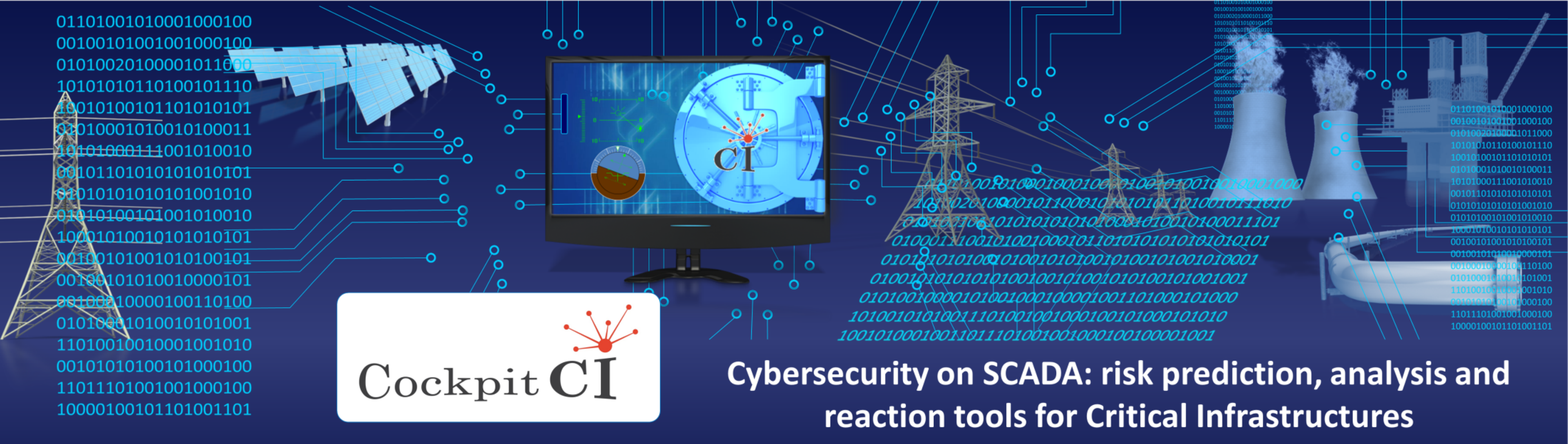
Any question ?

Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Thank you for your attention

Information Society



Software vulnerability and malware analysis engines

4th CockpitCI Workshop (16.09.2014 Bucharest)

M. Aubigny
itrust consulting

Information Society

Introduction: Detection strategy background

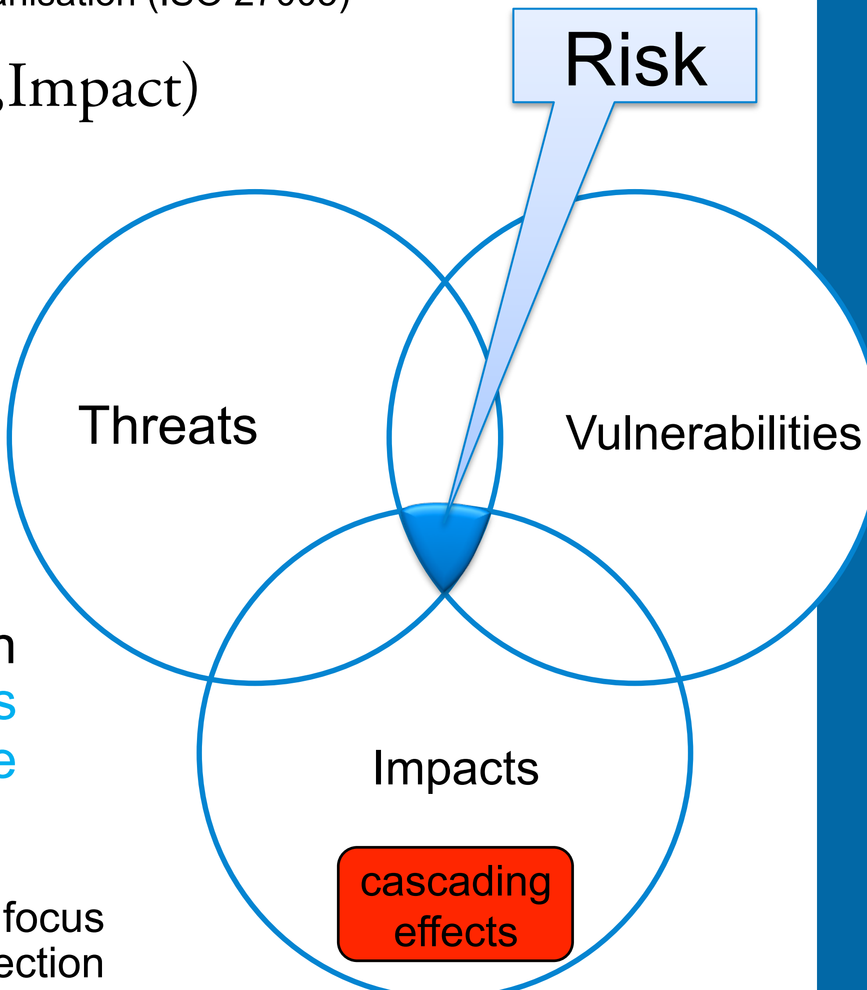
Risk Management

Risk is associated with the potential that threats will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation (ISO 27005)

$$Risk_{CI}=F_{Assets}(Threats,Vulnerability,Impact)$$

To manage the risk, for example by predicting the risk level of an organisation, we should know both threat and vulnerability levels of the organisation.

The detection tools included in CockpitCI should target both threats and vulnerabilities in the entire organisation.



NB: The simulation and prediction tools will focus on the potential impacts according to detection input and threat evolution to assess the QoS.

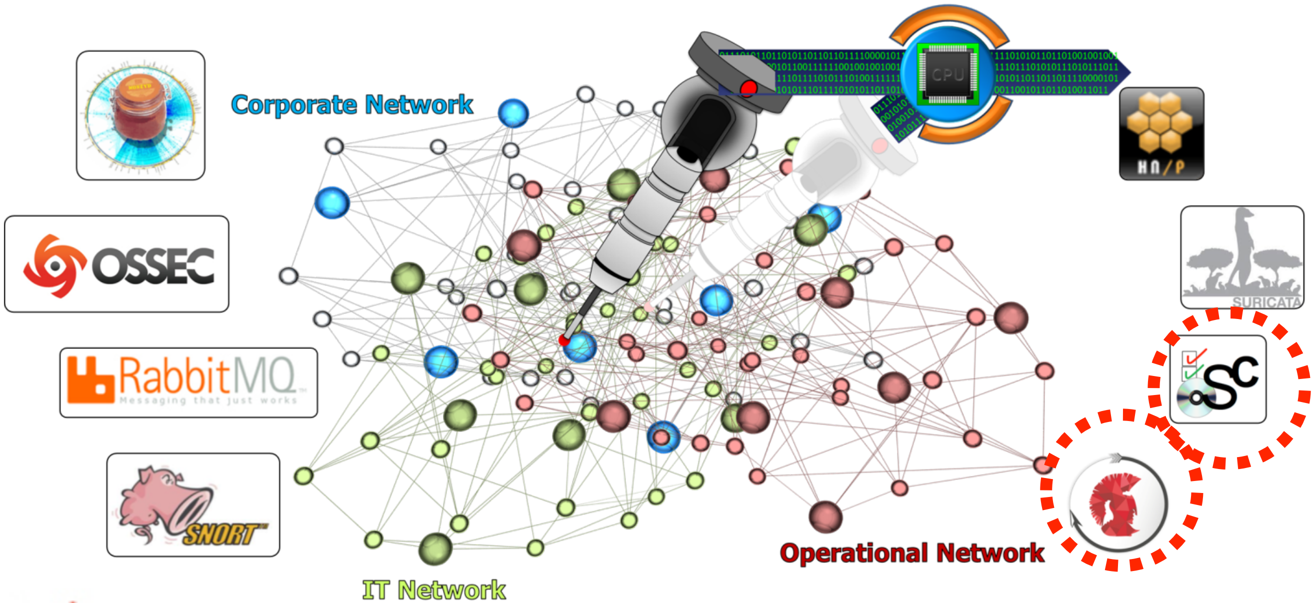
Introduction: what's up in CockpitCI?

Detection framework overview

The CockpitCI detection framework is a multi-layered detection solution (deployed on the 3 types of networks: ICS, Telco, Corporated) that enables different types of detection tools to assess vulnerabilities and threats: Honeypot, HIDS & NIDS, Specific SCADA tools.

We want to speak about 2 tools developed by itrust in the project framework:

- **Software checker**: a vulnerability assessment solution;
- **AVCaesar**: a specific antivirus solution.



Software checker: **it's time to check your vulnerability**

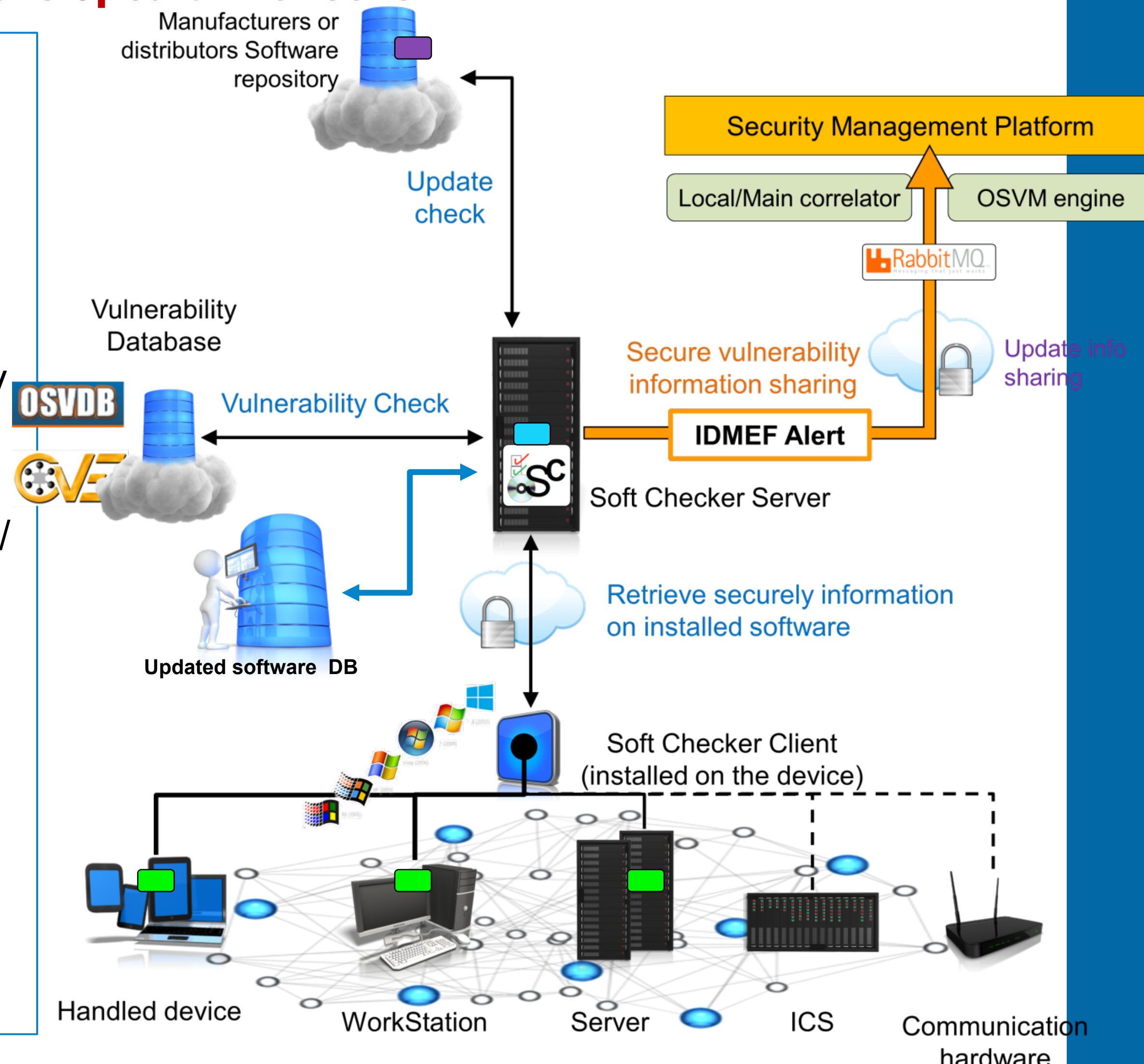
Software checker: it's time to check your vulnerability

Software checker overview

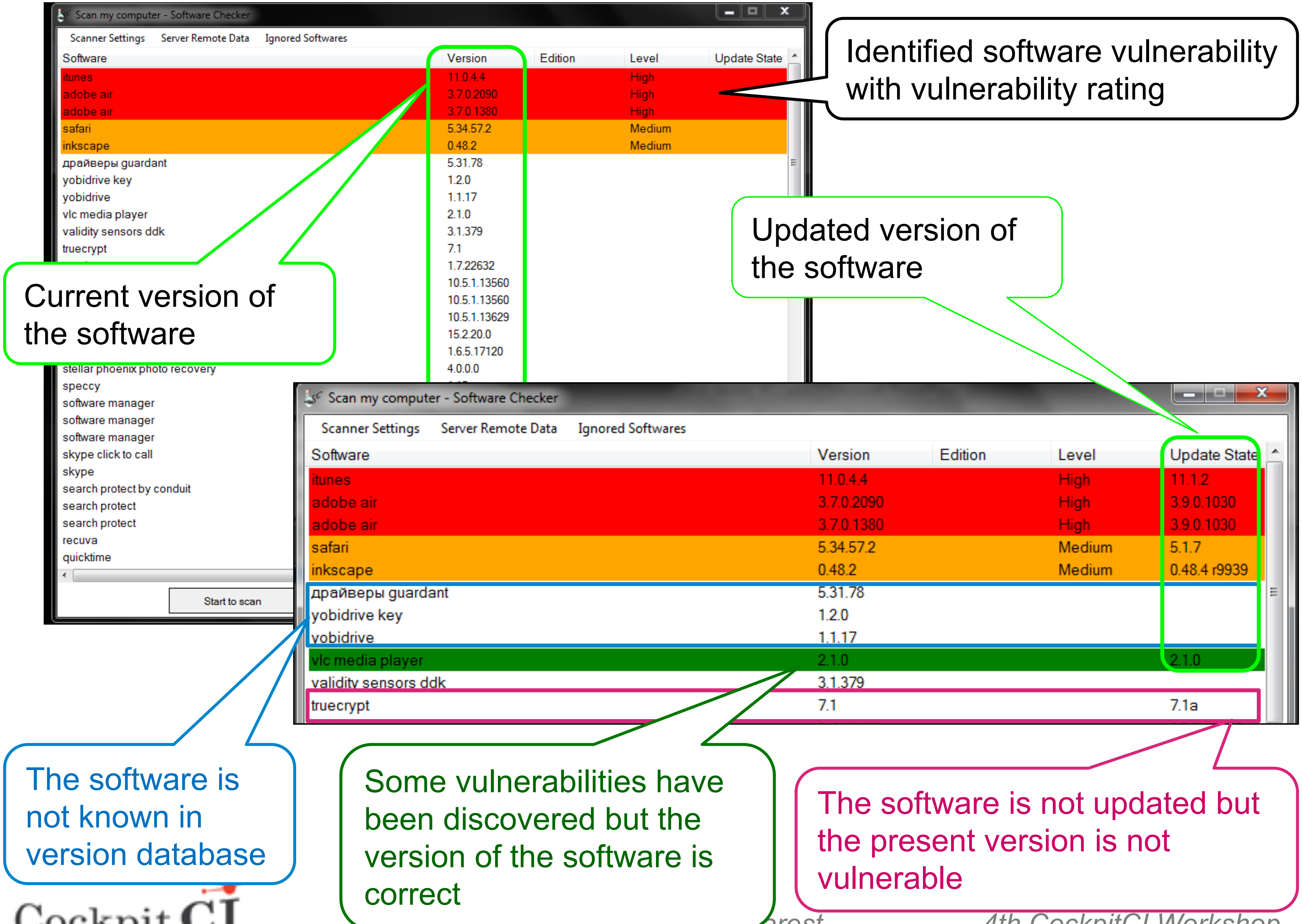
As it is often difficult to efficiently and securely manage the security of all installed software, we have developed SW Checker.

In CockpitCI

- **Regularly** retrieve information on software deployed on platform: *for example as soon as a component is connected to the network.*
- **Regularly** verify the vulnerability state of software
- Provide an IDMEF Alert in case of detected vulnerability to Local/ Main correlator and SMP.
- Check in option the **last** update version of software and inform the SMP to plan update deployment.
- Provide a central database of **trusted** links for updates.



Results of the vulnerability assessment (laptop interface)

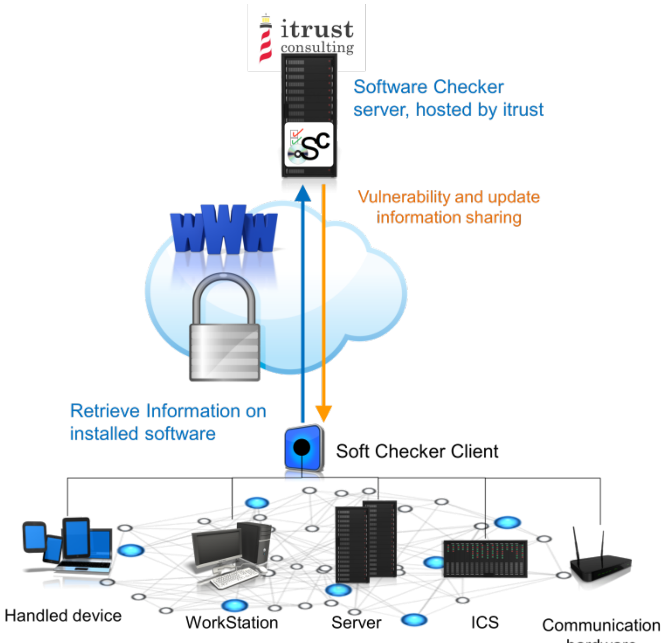


Other deployment design: As a service or as an appliance

As a service

Light version

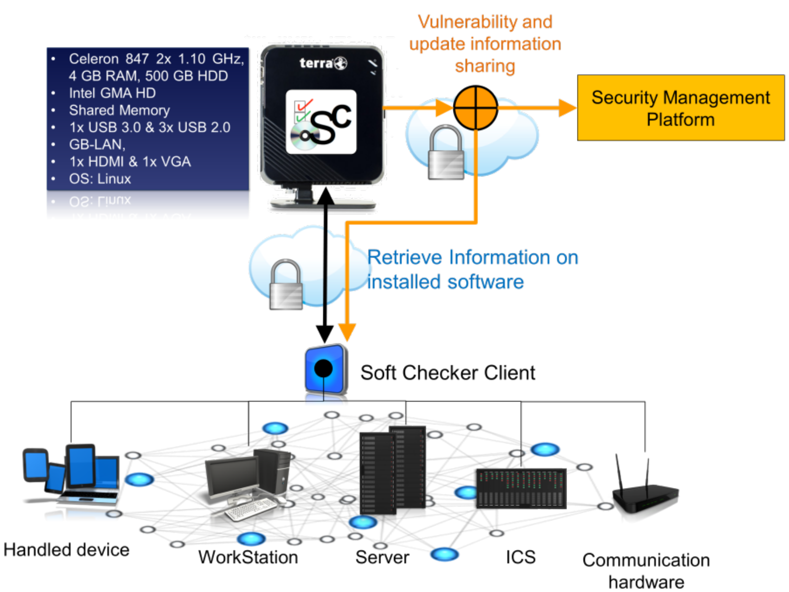
- Clients are deployed on local devices.
- Operation of the server is managed by itrust.
- No connection with Security Management Platform



As an appliance

AllInOne version

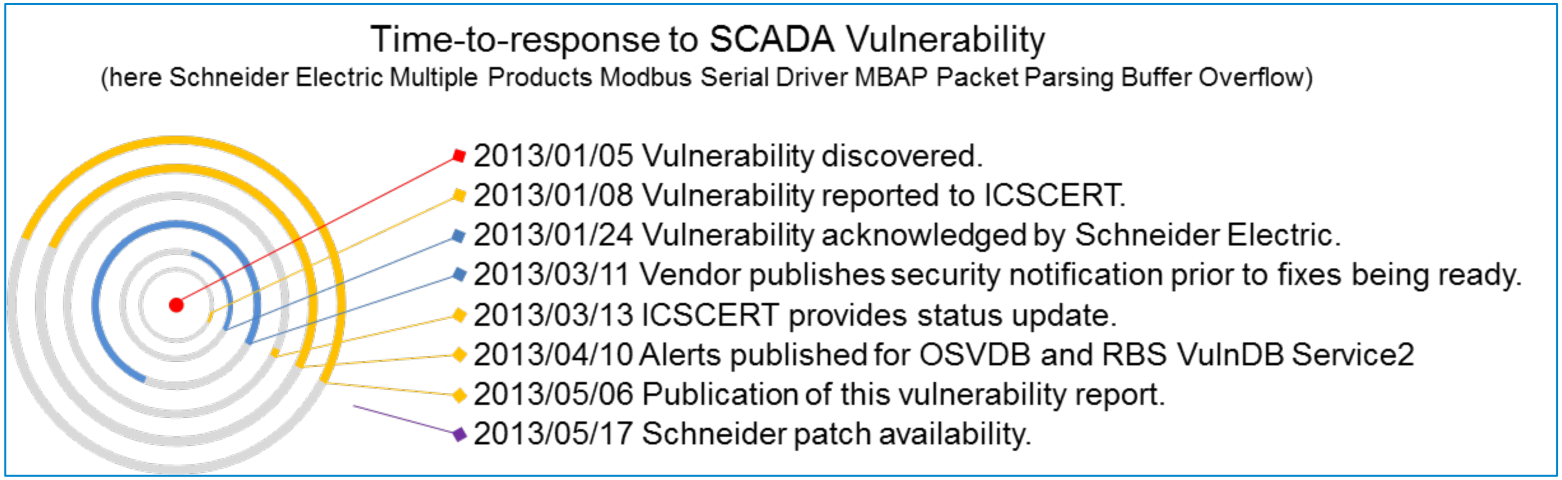
- Clients are deployed on local devices.
- Server deployed and maintained by itrust but operated by the owner.
- Communication with customer's security platform or directly with deployed devices



Major outcomes and future works

Major outcomes

- As the vulnerability database contains multiple open sources, it avoids manufacturer's latency on security vulnerabilities of their own products and warns CI owners of the level of software vulnerability.



- If an unknown software is discovered and not referenced in the database, it could be sent to a malware analysis service for deep analysis.
- Free trial available upon request (info@itrust.lu).

Future issues

- Develop client for Linux OS, OS X, embedded OS.
- Develop a non-client supported version to test SCADA systems without being invasive.
- Deploy the system on the IEC HTB for validation (on-going).

AVCaesar: Declare total war on malware

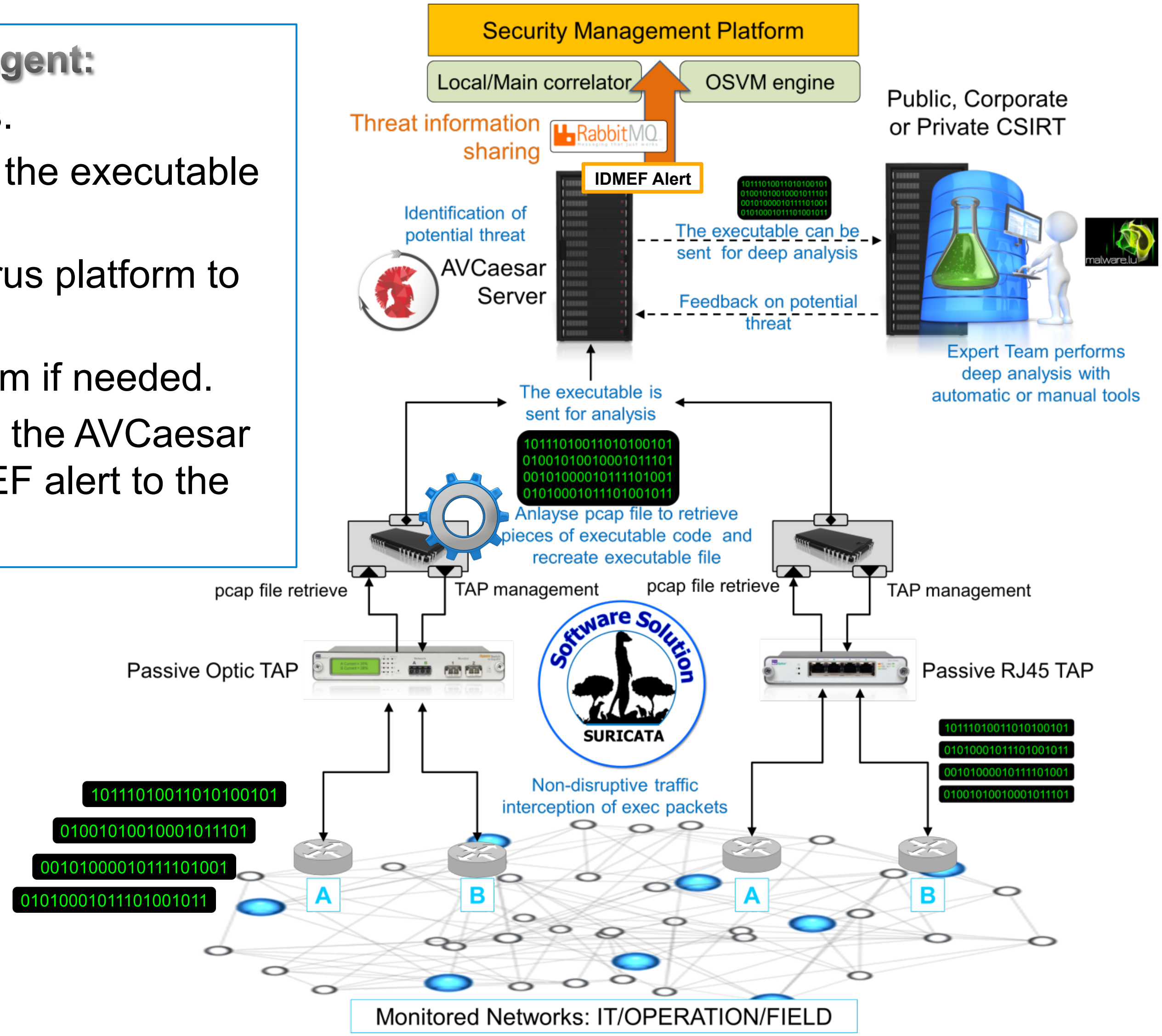
Overview

As more than one antivirus is better, we developed AVCaesar 10 in 1

Aim of the detection agent:

- Capture exec packets.
- Analyse and recreate the executable file.
- Send to a multi-antivirus platform to analyse criticality.
- Send to an expert team if needed.
- If a threat is detected, the AVCaesar server sends an IDMEF alert to the SMP.

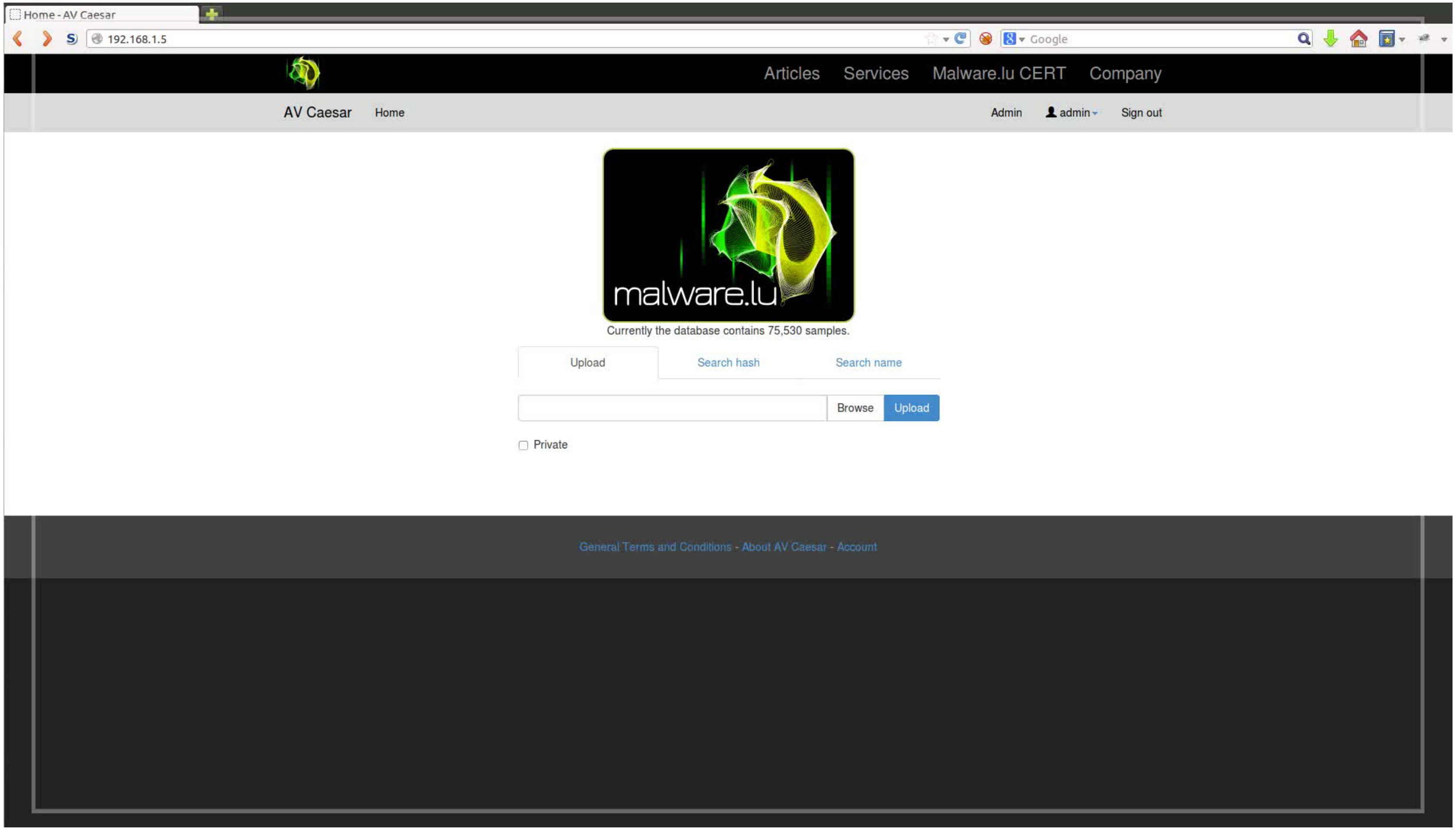
NB: All connections use secure protocol.



Cockpit CI

AVCaesar demonstration

Quick video showing a malware analysis by AVCaesar multi-antivirus

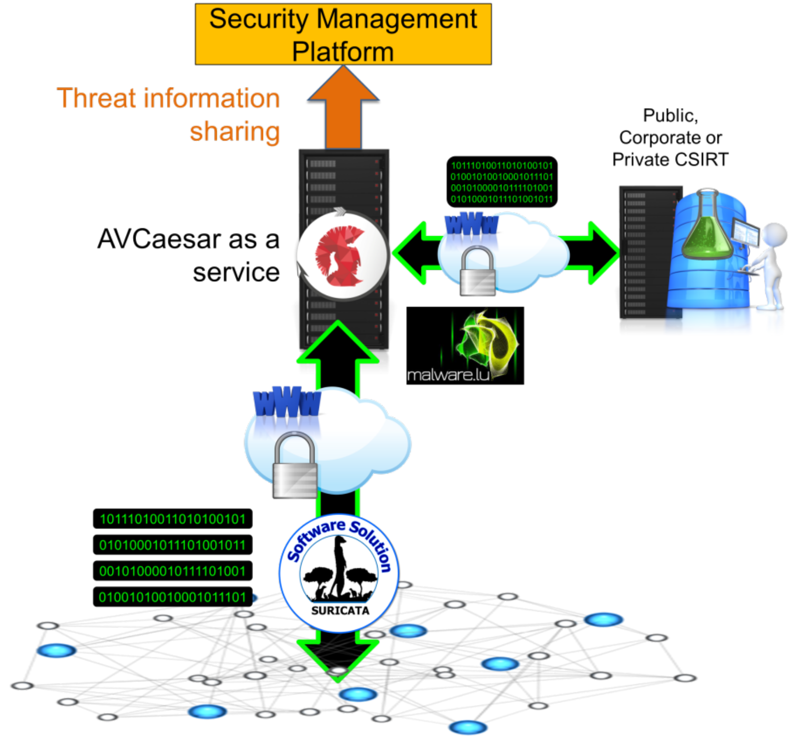


Deployment design: As a service or as an appliance

As a service

Web Service solution

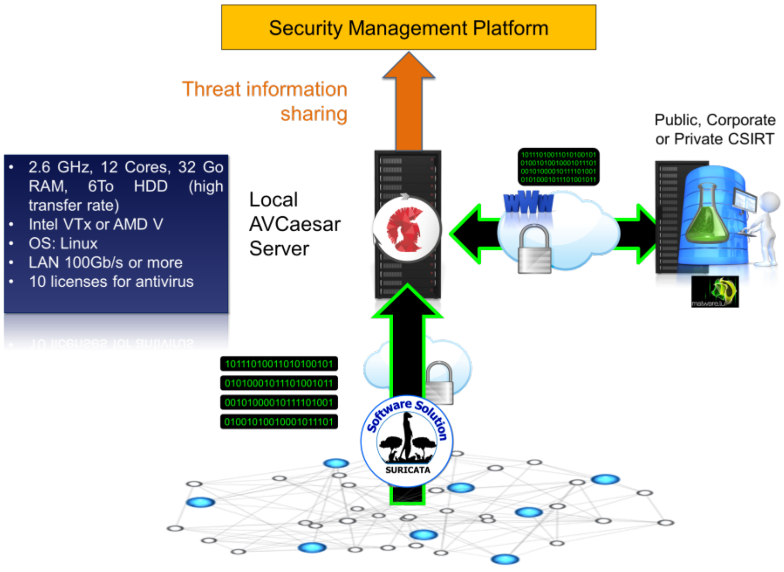
- Registration on the CERT Malware.lu.
- Service options: Daily, monthly or yearly subscription.
- Service operated by malware.lu: a brand of itrust.



As an appliance

Private server solution

- Server hosted by user but deployed and maintained by malware.lu.
- Communication with security platform enabled.
- Communication with CERT enabled.



Major outcomes and future works

Major outcomes:

- This antivirus enables 10 antiviruses simultaneously in real-time.
- The malware.lu database currently contains 4,948,599 samples.
- The antivirus could be deployed as a web-service (reachable by request) or as a dedicated component of the CI's network.
- The antivirus engine is connected either on-line or off-line with an updated database of malware (open database *malware.lu*).
- The web-service is part of a CSIRT service which shares cyber-alerts and receives cyber detection notifications.
- The system is now deployed as a service since 30th October 2013 and available for free trial here: www.itrust.lu.
- The system has been tested by governmental and European organisations.
- Able to share information to the SMP in IDMEF alert.

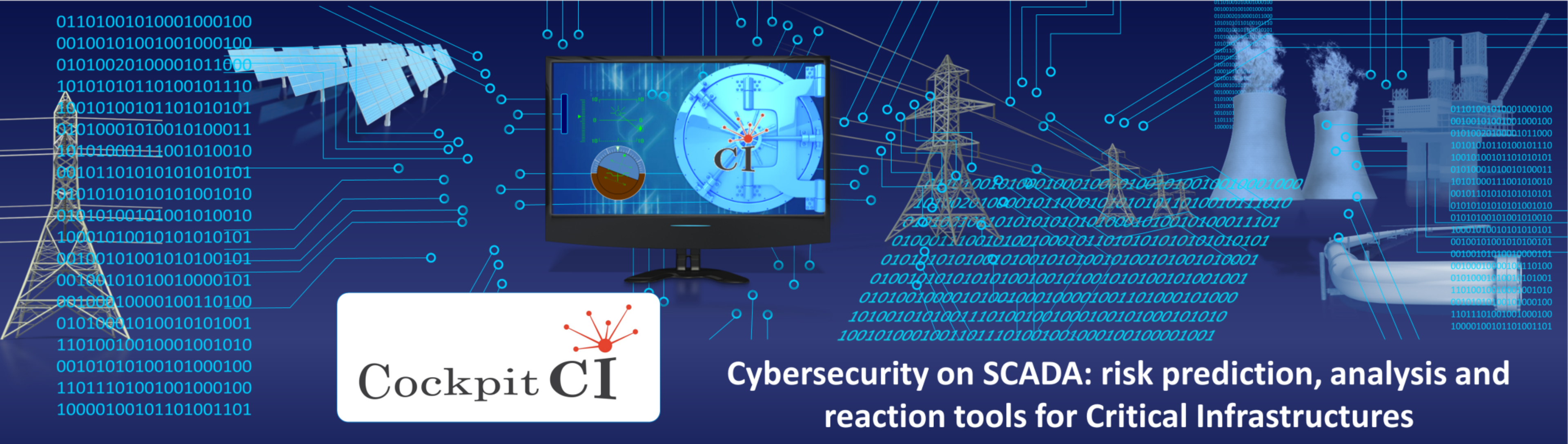
Future issues:

- Deploy the system on the Hybrid-test bed (on-going).
- Deploy in union with other detection tools like SW Checker or NIDS/IDS.

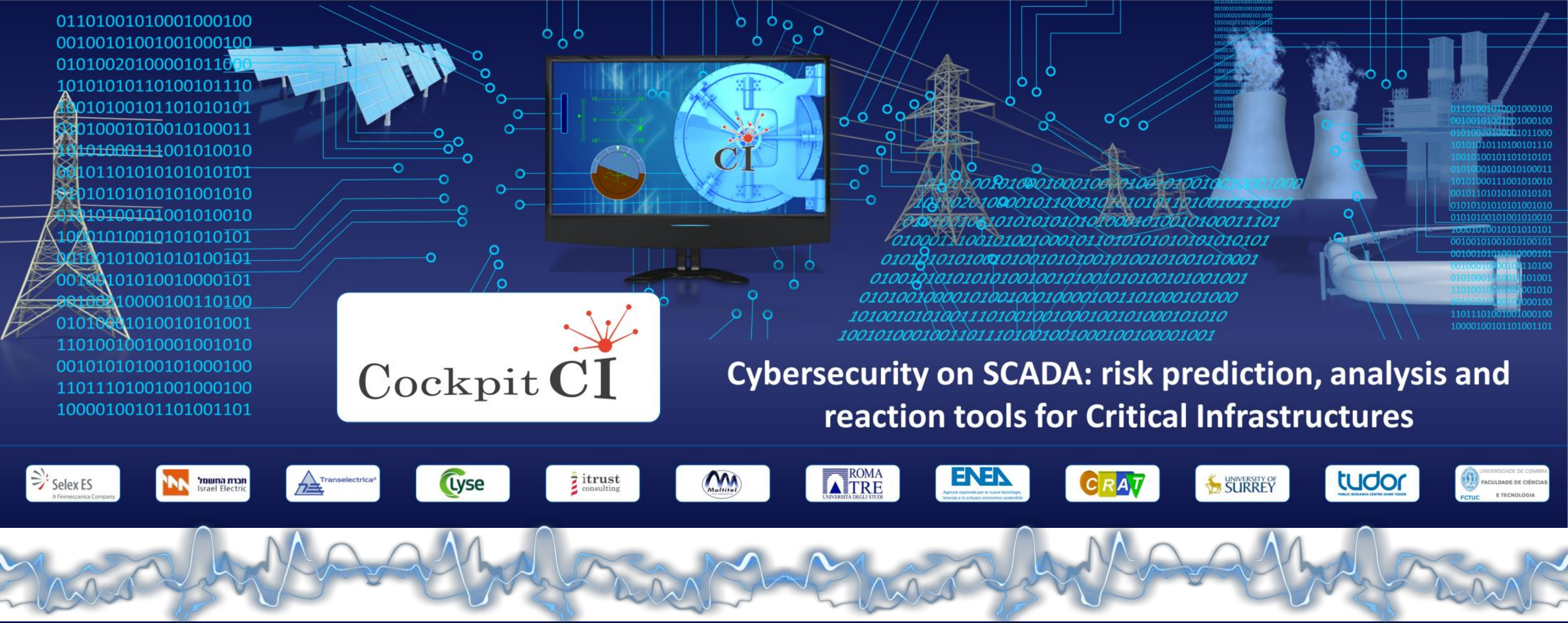
Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Any question ?



Thank you for your attention



Modeling loss & false controllability and observability of electrical grids under SCADA cyber attacks

4th CockpitCI Workshop (Bucharest 16.09.2014)

Michele Minichino, ***ENEA***

Leonid Lev, ***IEC***

Serguei Iassinovski ***Multitel***

Bucharest, 16 September 2014

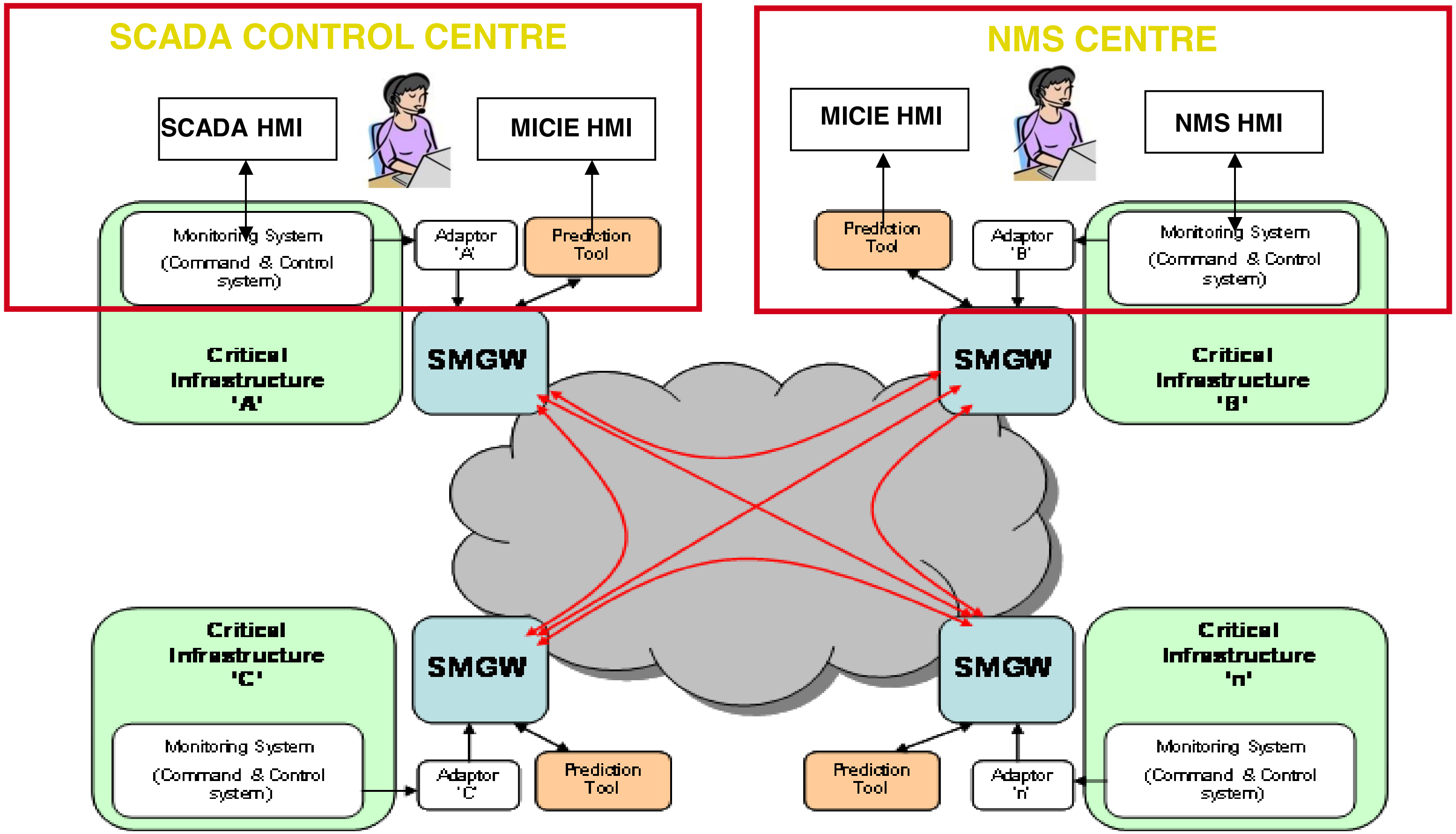
Summary

- ❖ Background
- ❖ Overview of modeling techniques and tools for SCADA systems under cyber attacks
- ❖ Reference Scenario
- ❖ QoS indicators versus adverse events, including cyber attacks
- ❖ Modelling and prediction of QoS by heterogeneous modelling paradigms
- ❖ Modelling versus testbed

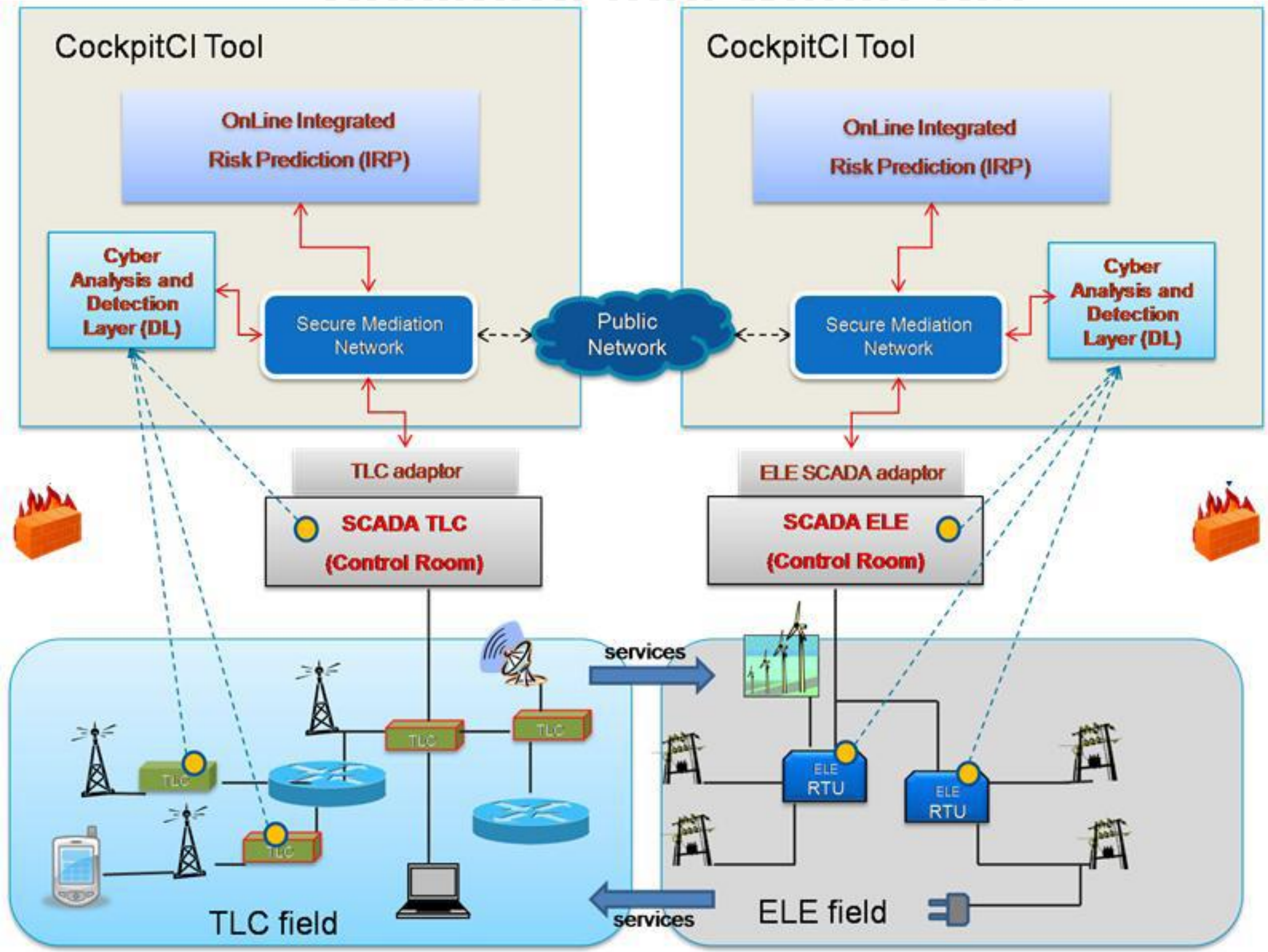
CockpitCI tool , extends MICIE tool

to handle cyber-attacks, supporting decisions of **CI operators** by means of **real time risk levels prediction.**

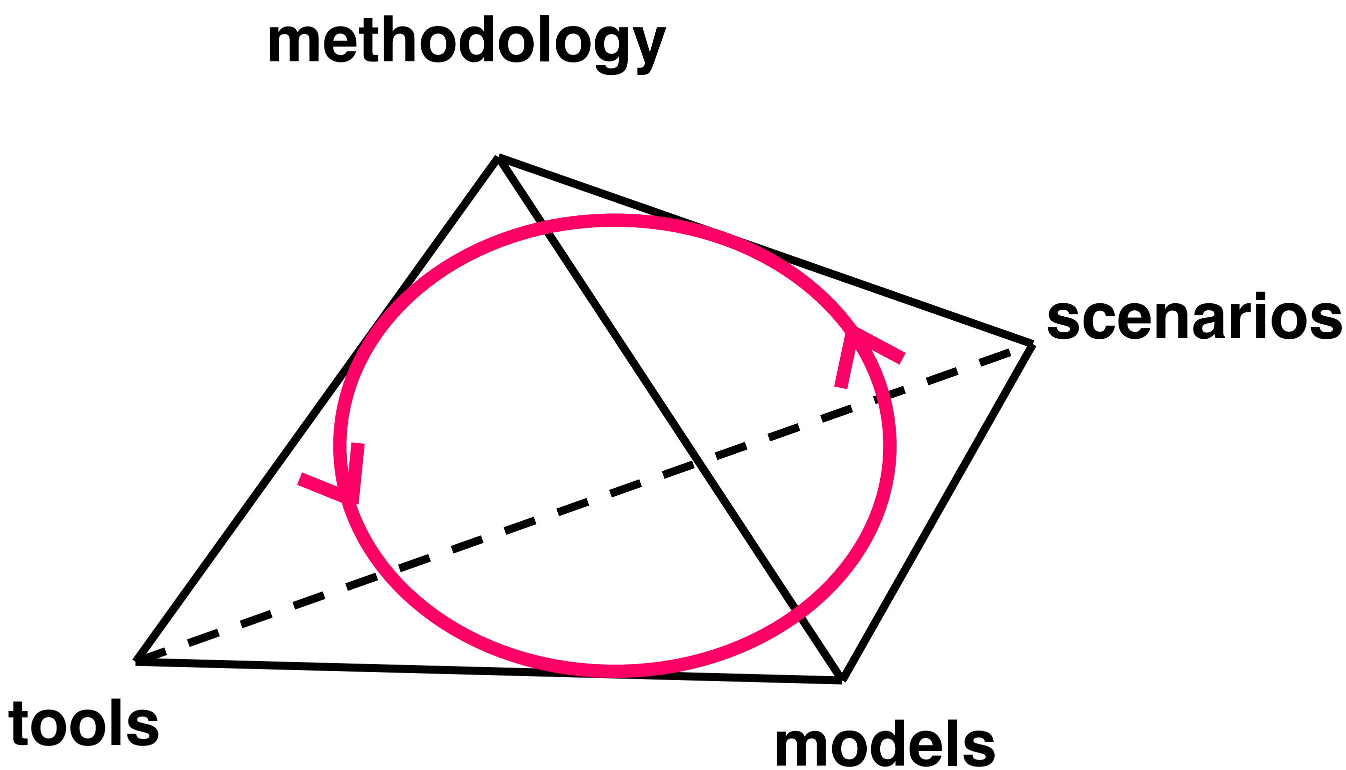
MICIE tool within CIs



CockpiCI tool within CIs



Understanding risk on a physical infrastructure under adverse events (cyber attacks in CockpitCI) and considering interdependencies. Measuring the risk in terms of QoS of SCADA and physical CI (i.e. electricity)



Overview of modeling techniques and tools for SCADA systems under cyber attacks

- techniques based on identification of attacker profiles, attack objectives, attack steps characterization, spreading throughout Industrial Control Systems and consequences on physical Critical infrastructure

  - four kinds of models:

    - Attacks/attacker/vulnerability models (i.e. attack/vulnerability trees, Petri nets, Game theory);

    - ICS & corporate network models (i.e. communication network simulators/emulators);

    - Physical CI models (i.e. electrical models by power flow simulators);

    - Composite models to represent more than one aspect of the attack, including the consequences on the physical Infrastructure.

Overview of modeling techniques

Results: modeling techniques adopted in the project:

- SIR model of epidemics, to study how a malware infection spreads in ICT based networks and systems;
- Attack Tree, which is basically a Fault Tree with the attack goal in place of a fault and basic event probabilities are not failure rates;

Overview of tools

Results (tools adopted by the project are in red)

- ICS security tools
  - Ettercap – MITM attacks
  - NESSUS – vulnerability scanning program
  - Metasploit – penetration testing software
  - NAGIOS – Network Monitoring Tool
  - Wireshark – packet sniffer

- Intrusion detection/prevention tools
  - Snort – network intrusion detection system
  - Commercial solutions by SERVITECNO
    - Netcheck
    - Industrial defender

- ICS security testbeds
  - Sandia National laboratory (DATES)
  - Idaho National laboratory (NSTB)
  - Power Infrastructure cyber security laboratory
  - Experimental investigation of malware attacks (MAISim & Jade)

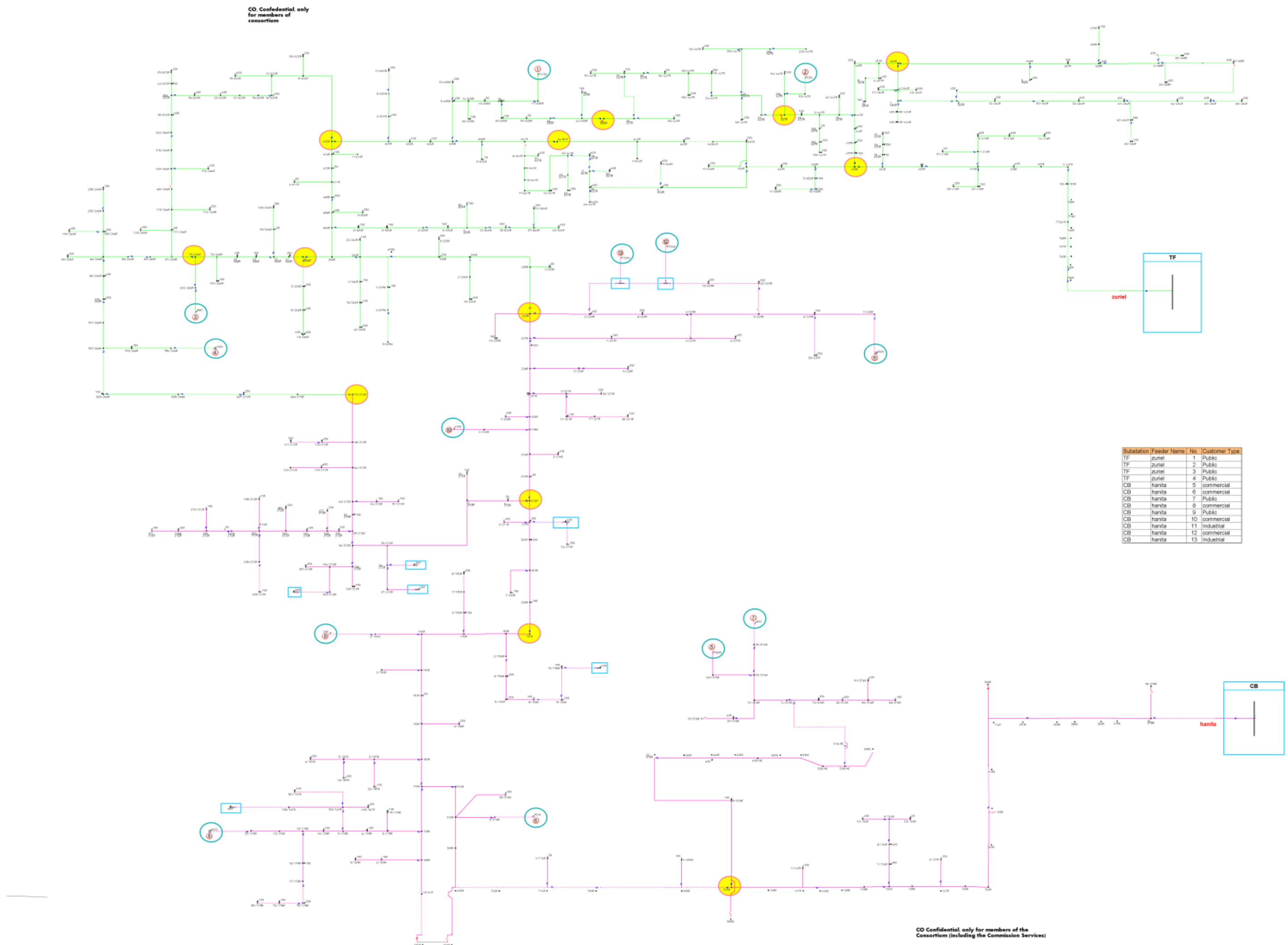
Reference Scenario

- ideally identifies the whole set of knowledge, information and data needed to extract:
  - part of functional design requirements of CockpitCI tool
  - and to demonstrate the tool against such requirements.

- is composed by
  - a SCADA system and its electrical grid,
  - a corporate network
  - main functionalities,
  - topologies,
  - main devices,
  - main communications among devices,
  - communication protocols with special attention on TCP/IP based protocols,
  - interdependencies
  - cyber security issues such as cyber threats, vulnerabilities, pre-existent cyber security policies and technical solutions, and attack cases

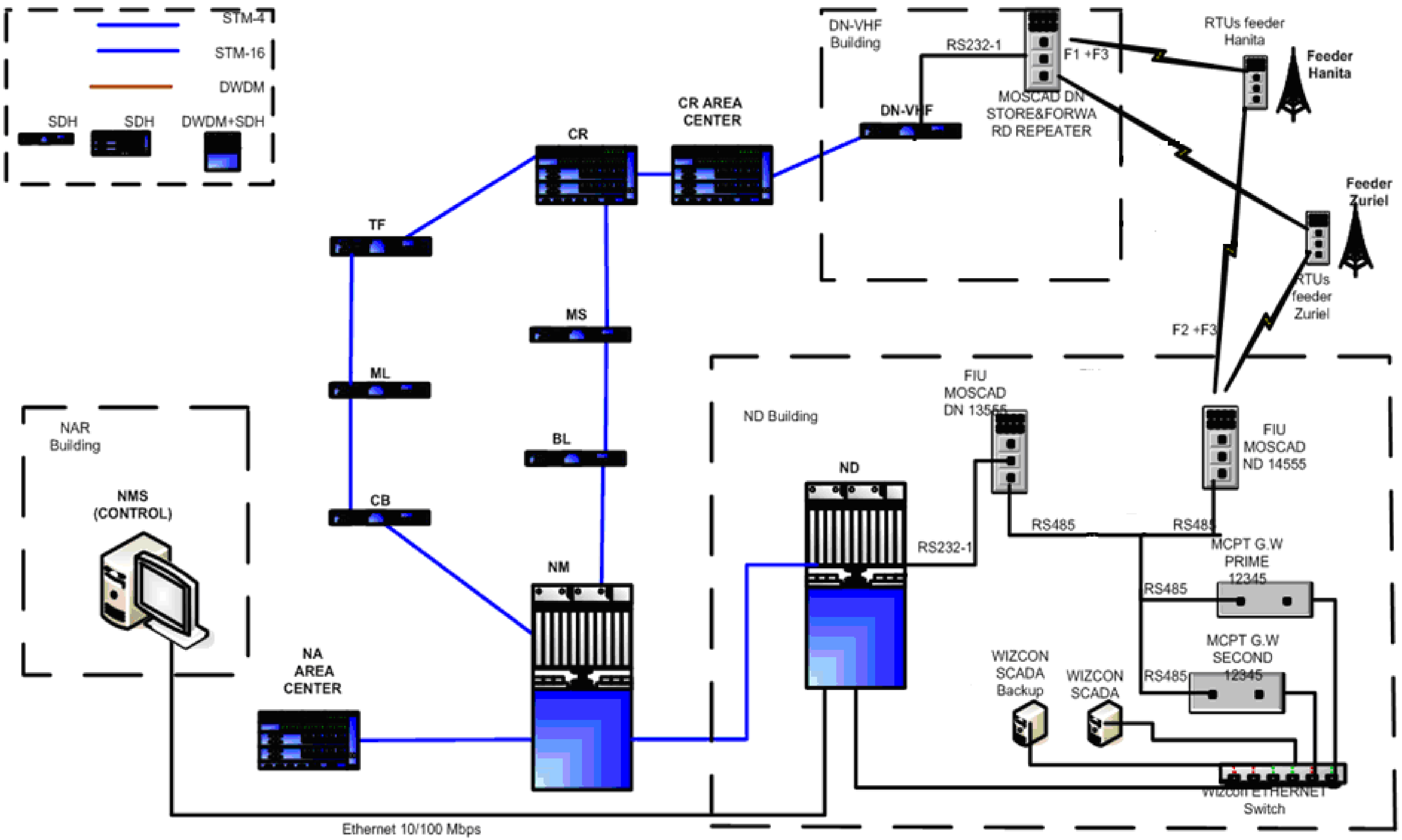
- acts as a whole interdependent System of Systems

MV electrical grid



Substation	Feeder Name	No.	Customer Type
TF	zuriel	1	Public
TF	zuriel	2	Public
TF	zuriel	3	Public
TF	zuriel	4	Public
CB	hanita	5	commercial
CB	hanita	6	commercial
CB	hanita	7	Public
CB	hanita	8	commercial
CB	hanita	9	Public
CB	hanita	10	commercial
CB	hanita	11	Industrial
CB	hanita	12	commercial
CB	hanita	13	Industrial

SCADA & corporate network



SCADA (Supervision Control and Data Acquisition)

- nervous system of physical infrastructures (CI)
- communication links between control center & RTUs dependent on (public/private) Telco networks (ICT)
- mutual propagation of disturbances and adverse events between CI and telecommunication CI (ICT)

loss/degradation of SCADA functionalities impacts on QoS and efficiency of physical infrastructures (i.e. electrical grid)

What does SCADA control?

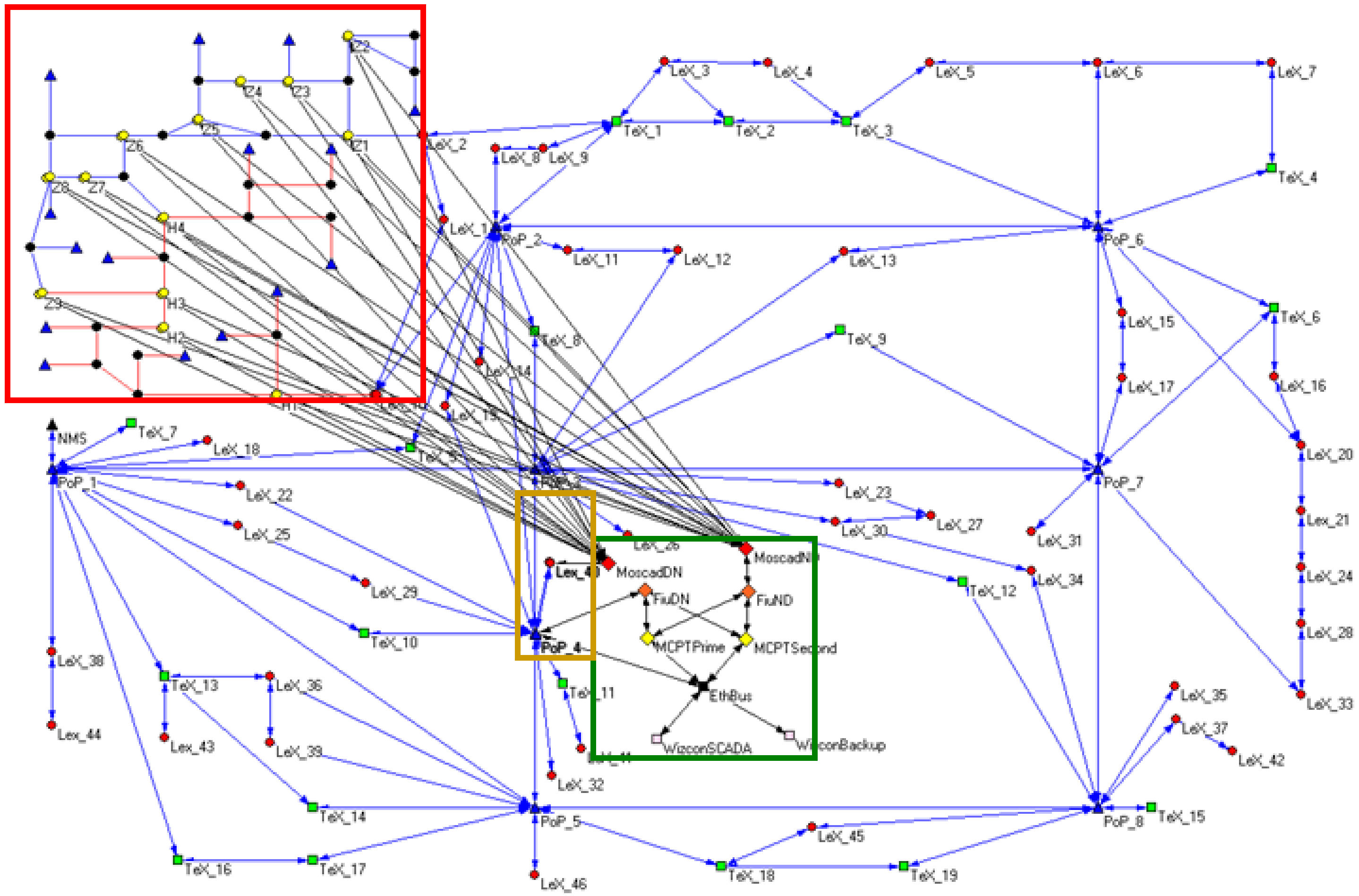
Switch disconnector: Interruttore di Manovra Sezionatore in sottostazione AV/MV (centro ENEL di Aquila)

What does SCADA control?

HV/MV Transformers (i.e. TAPS di regolazione tensione)

(centro ENEL di Aquila)

Power grid, SCADA system, corporate network act as a whole interdependent System of Systems



Functionalities of reference scenario include

- SCADA: Fault Isolation and System Restoration procedure, which is executed by SCADA operator, on a permanent failure of the electrical grid;

- Corporate network: Fault identification and handling procedure

FISR performed by SCADA operator

- In electrical grids, failures may cause the de-energisation even of large part of power customers and need to be located, isolated and repaired quickly and safely.

  - Failure location consists in the progressive re-energisation of electrical sections of the grid, by closure/aperture of circuit breakers, starting from the most upstream section of the grid to the most downstream section of the breaker originally tripped.

  - The process ends when the feeder protection at substation is activated and the faulty section is located and isolated.

  - Finally, on the repair of the faulty section, the grid is restored to its original configuration.

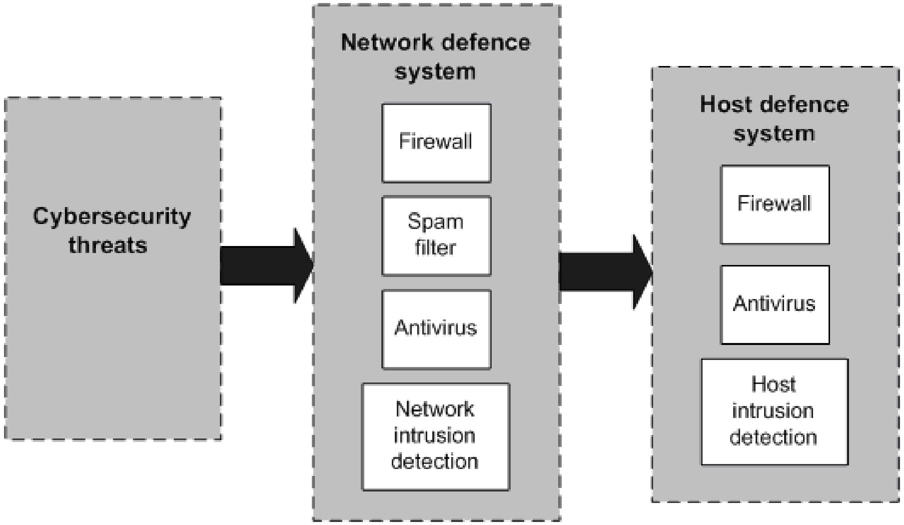
- FISR: Fault Isolation and System Restoration - procedure is based on grid monitoring, sensing of loss of power, circuit breakers operations, performed throughout Remote Terminal Units (RTUs).

FISR degradation affects the quality of electricity supplied to grid customers

Cyber threats, vulnerabilities, pre-existent security policies

- may impact the bills that (electrical) customers pay

- CockpitCI tool requirements ideally should not neglect pre-existent cyber security policies from (electrical) utilities



  - should help in improving context awareness of CockpitCI tool to ideally avoid the replica of existing solutions and to propose detection and reaction strategies on the frontier of the technology

- a questionnaire adapted to Project scope from the questionnaire of National Association of Regulatory Utility Commissioner (NARUC) to project stakeholders, into the limits of not violation of confidentiality issues

Three kinds of cyber attacks and consequences

- Malware spreading
- Denial of Service (DoS)
- and Man in the Middle (MITM)
  - each attack, specified in terms of
  - peculiar characteristics,
  - attack initiation sources,
  - attack targets
  - and expected consequences
- instantiated to topology and main devices of SCADA and corporate network
- Consequences on SCADA and the grid (QoS)
  - when SCADA executes FISR
  - when altering SCADA and grid status

Consequences of cyber attacks - when SCADA executes FISR

- Under special attention is a successful cyber attack which puts out of service the redundant (primary and secondary) connections between SCADA Control Centre and RTUs, while SCADA operator is performing FISR procedure on the electrical grid.

- The consequence on SCADA could be
  - the lack of observability and controllability of the electrical grid
  - and in turn the impossibility to execute FISR

- The consequences on the electrical grid could be degradation of reliability, resilience, safety and quality of electricity to customers, typically regulated by a National Electric Authority, such as:

  - the duration of electrical interruptions for customer for year
  - the number of long/short electrical interruptions for customer per year

- A timely actuation of FISR, reduces the outage duration and then contributes to keep indicators of quality of electricity to customers within prefixed values.

- On the contrary a delayed actuation of FISR service gets worst such indicators.

Consequences of cyber attacks - altered behavior of compromised corporate network or SCADA devices

could lead to lowering of electrical service level for customer or increasing risks of quality of service degradation, as viewed by Israel Electrical Corporation:

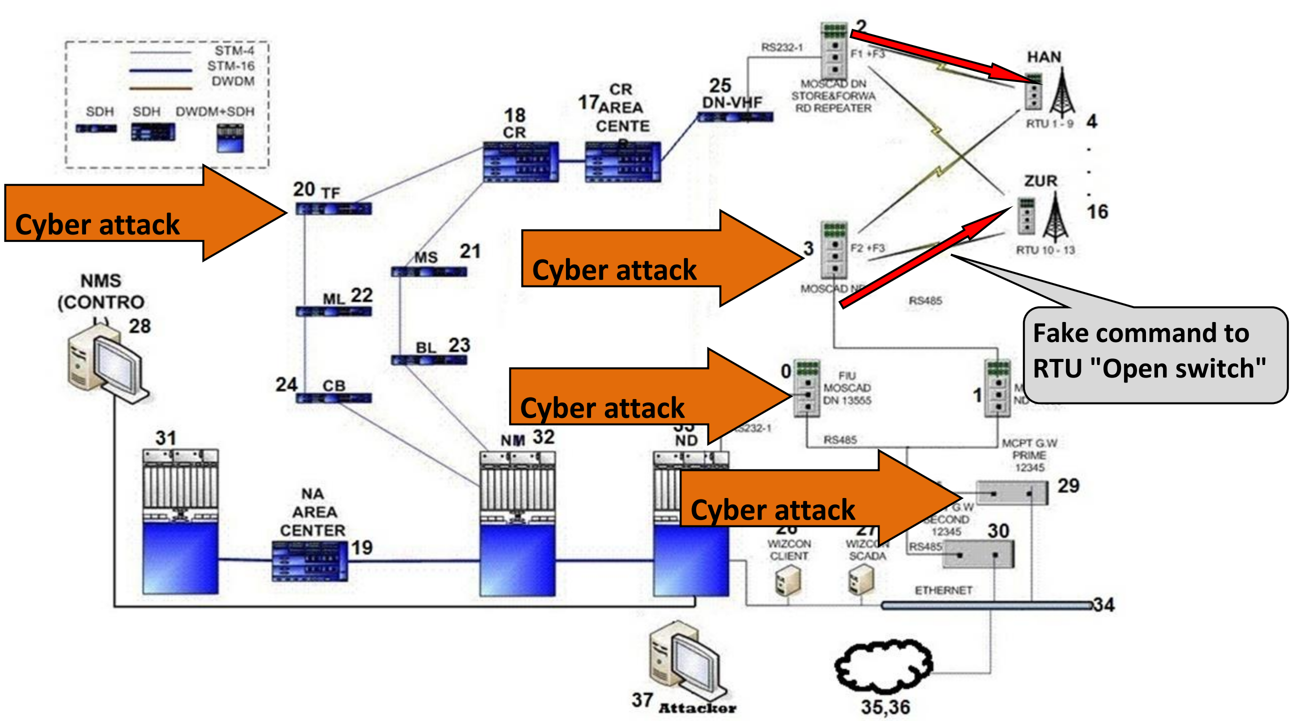
- fake commands to RTU (by malicious SCADA operator, malware on SCADA, MITM attack, etc) or to substations, for example malicious opening of a breaker (not protection, not SCADA command);
- false messages about RTU status (switch position, battery level,...), substation status ("out of limit voltage"), corporate network room status (temperature, battery level) to SCADA, provoking false view of system (MITM) and thus wrong reaction (automatic or by SCADA operator);
- altering commands issued by SCADA at some stage of transmission (MITM attack);
- destruction of true SCADA commands, causing loss of control;
- destruction of true messages from ECI, corporate network room or RTU (DoS, MITM), for example "AC loss" alarms, RTU status messages or corporate network room status messages (temperature, battery level), provoking loss of view at SCADA side;
- breaking to substation (denial of service at SDH level) making MPLS services not operational.

Consequences of cyber attacks: altered behavior of compromised corporate network or SCADA devices

Number	Event	Effect	Diagnostics
1	Breaking to Substation. Connection to MPLS switch by wire or by wireless modem (have to know management password) - MITM	Executing command to RTU, e.g. opening a switch. Causes unsupplied energy to customers	No alarm to NOC, neither to SCADA
2	Breaking to Substation, connection to management channel of the SDH element (IP), make Denial of Service (DoS).	MPLS services are not operational	SCADA operator notices no acknowledgment on command to RTUs
3	Connect to RTU communication infrastructure and disguise to an authentic control command	Example: A switching element (CB, SW, etc) opened, resulting in unsupplied energy to customers	• The control action reflected as an unwanted action since it wasn't executed from SCADA • No protection alarm indication appears and no reclosing of CB
4	Sending a constant out limit voltage value (low or high) to SCADA, unaffected by transformer tap changer control attempts	• Dispatcher tries repeatedly to balance the voltage by changing the tap position of the transformer. • The voltage value can reach a dangerous level and may cause damages to equipment or to customers.	The indication of tap position is changed with no correlation to the voltage value (constant) - no timeout commands received in SCADA log
5	Taking control of a network RTU (SCADA blocked) and block "AC loss" alarms from all downstream RTUs, which communicate with the same base station.	Opened remote switch caused unsupplied customers, fed from all downstream lines, with no indications on SCADA.	• Trouble calls from customers in contradiction with normal load & status in SCADA • Manual action is needed - takes time

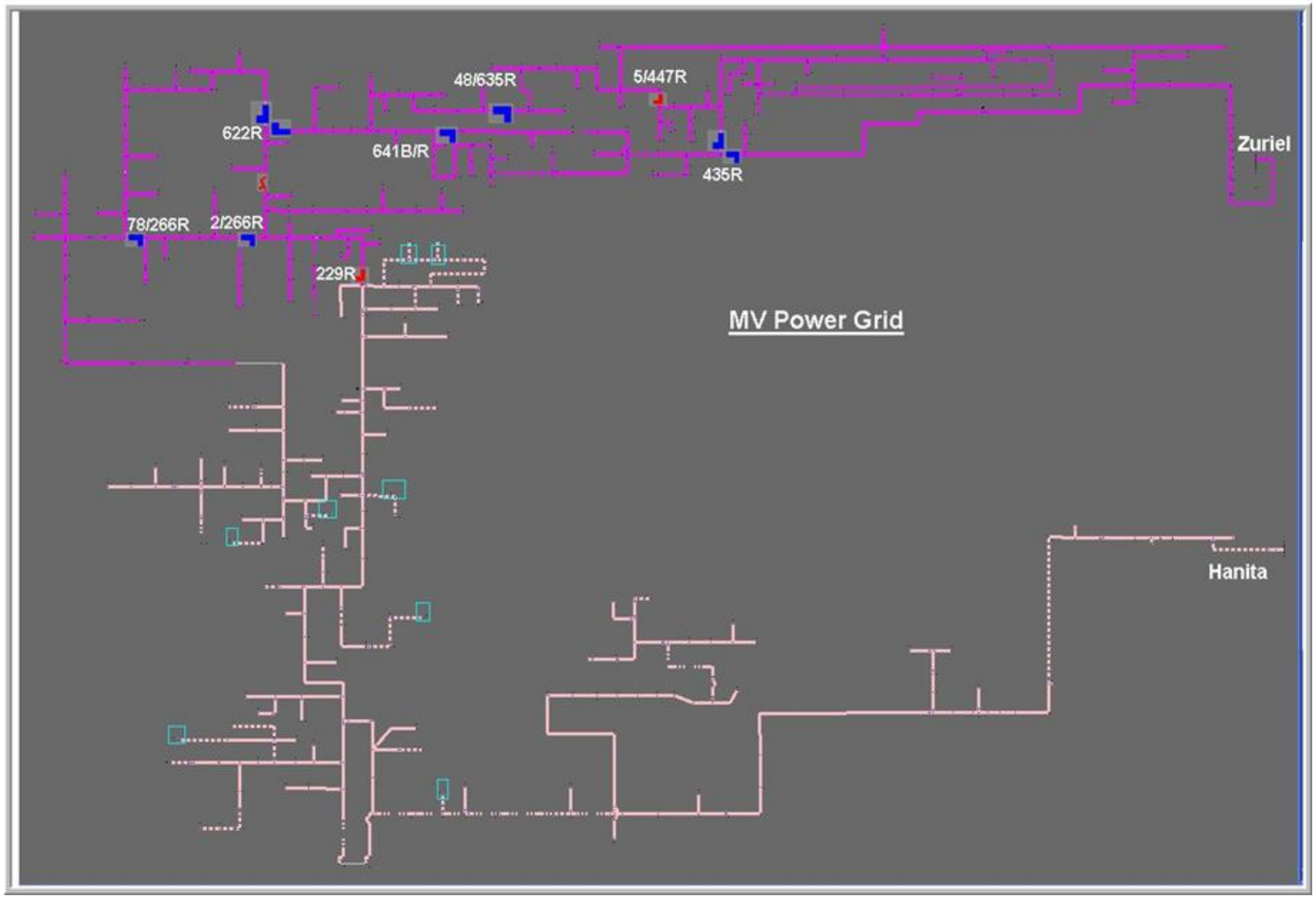
Cyber attack n.3 - MITM attack: Connect to RTU communication infrastructure and disguise to an authentic control command

- Possible attack targets: MCPT Gateway, FIU, Radio VHF Unit, ...



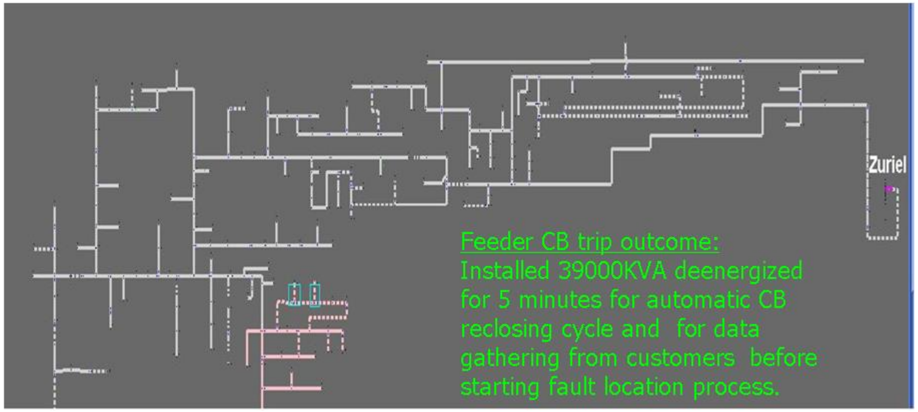
Nominal conditions of electrical grid fed by Zuriel and Hanita substations, before MITM attack n.3

MV Feeders – Zuriel & Hanita

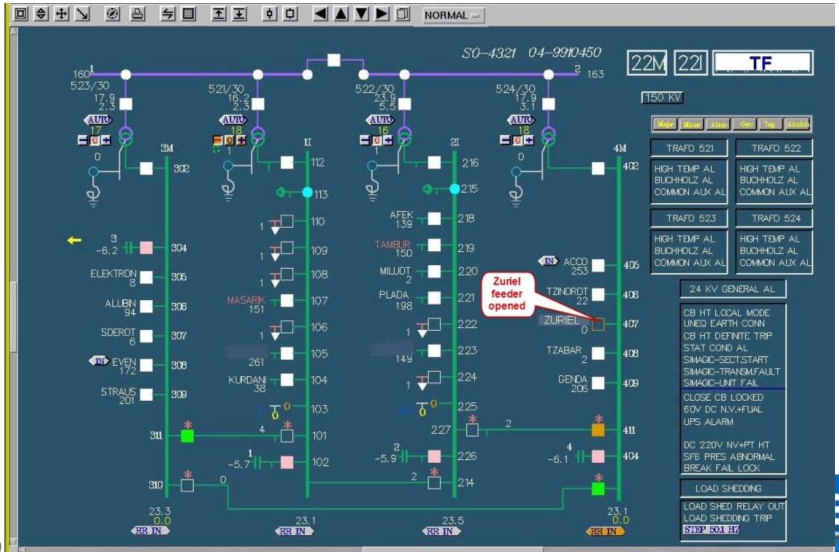


Consequences of cyber attack n.3 - Connect to RTU communication infrastructure and disguise to an authentic control command

- Electrical grid: unwanted remote switch opening or unwanted feeder breaker opening, causing loss of supply for all or part of customers of given feeder - Feeder is coloured in white to symbolize a de-energized status.



- SCADA Control Centre: No alarm indication of fault protection appears, no automatic reclosing of Circuit Breakers (CB).



QoS indicators versus adverse events, including cyber attacks

The consequences of cyber attack on SCADA could be

- the lack or alteration of observability and controllability of the electrical grid
- and in turn the impossibility to execute adequate commands from SCADA

SCADA QoS indicators

- *DPR*, a global vision of how many packets are missing on the network;
- *TTBP*, Transmission Time Between two Packets;
- *RTT*, Packet Round Trip Time, composed by TCP transmission time plus ACK transmission time;
- *Packets routing*;
- *LoV*, Loss of View, if the SCADA Control Center can't receive packets from the RTUs;
- *LoC*, Loss of Control, if the RTUs can't receive packets from the SCADA Control Center;
- Time Response of SCADA in executing FISR procedure

QoS indicators of consequences of cyber attacks on the electrical grid

- The consequences of cyber attacks on the electrical grid could be the degradation of reliability, resilience, safety and quality of electricity to customers, typically regulated by a National Electric Authority

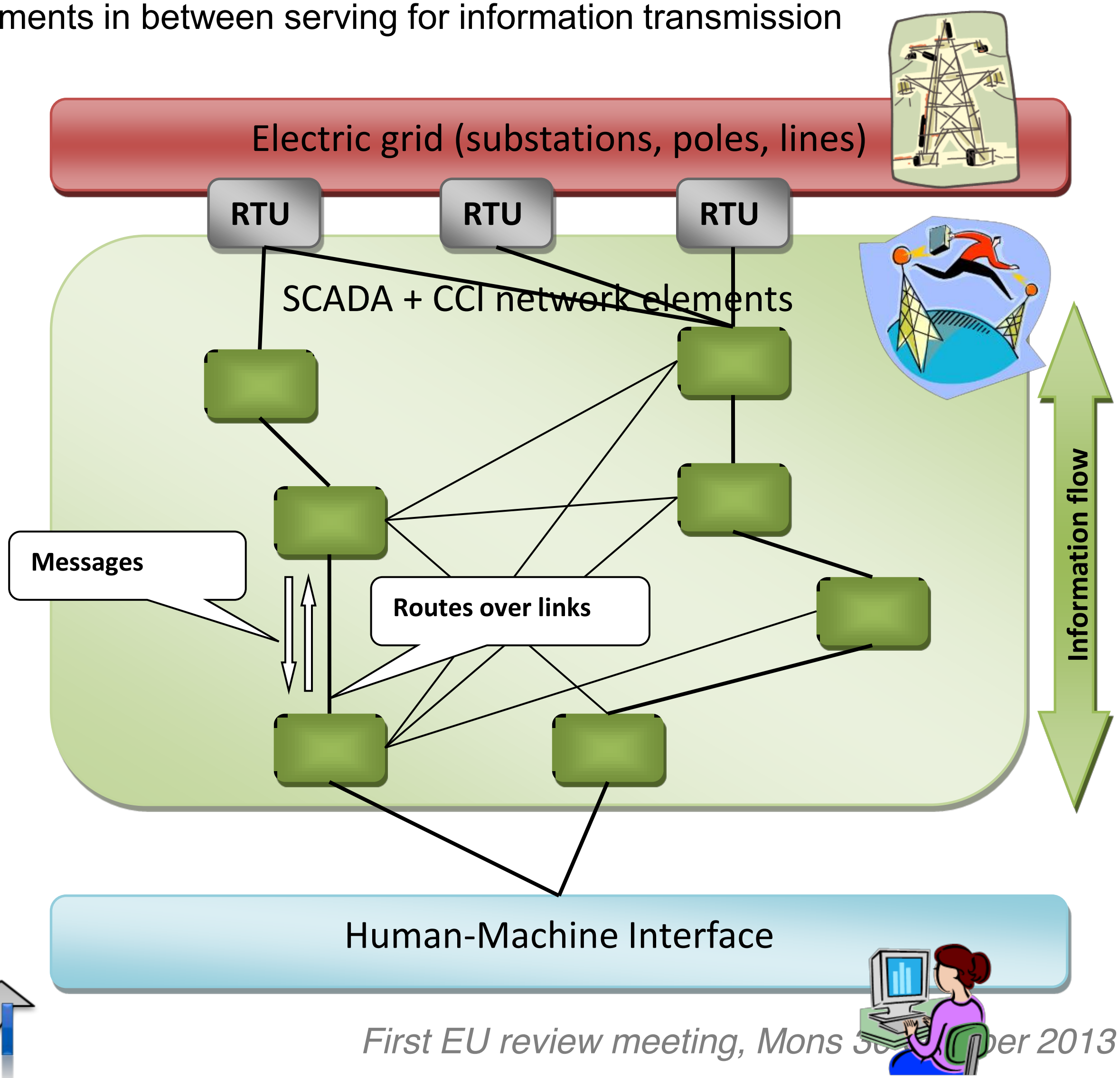
- Electrical grid QoS indicators:
  - duration of electrical interruptions for customer for year
  - the number of long/short electrical interruptions for customer per year
  - SAIDI - System Average Interruption Duration
  - SAIFI - System Average Frequency Interruption
  - CAIDI - Customer Average Interruption Duration
  - overvoltage values and duration dangerous levels - damages to equipment or to customers.

Prediction of QoS of SCADA and electrical grid by heterogeneous modelling paradigms

- Modeling is a crucial step in knowledge structuring for complex system comprehension
- Based on adequate formalisms, simulation models can be developed to:
  - study system behavior under various scenarios without affecting real running system and thus to improve the system
    - to better understand system vulnerabilities and to detect critical elements within Reference Scenario
  - feed algorithms of on-line applications with predictive possibilities on near-term system functioning, thus improving awareness
    - to feed algorithms of the Integrated Risk Predictor
  - create virtual environment for testing and validation of third party applications dedicated to system control and management
    - to test and validate CockpitCI tool

Modelling framework (Serguei)

From cyber attack modelling point of view the system can be considered as constituted of three layers - pure electrical infrastructure (without RTUs), HMI of SCADA and corporate network (CCI) and SCADA elements in between serving for information transmission



Composing epidemic and performance models : consequences on SCADA and electrical grid QoS

Models of

- Worm propagation
- Denial of Service (DoS)
- Man-In-The-Middle (MITM)

cyber attacks targeted at a source node may spread throughout SCADA and corporate network nodes up to affect (i.e. disconnect) the primary and the redundant communication between SCADA Control Centre and its RTUs while performing FISR procedure

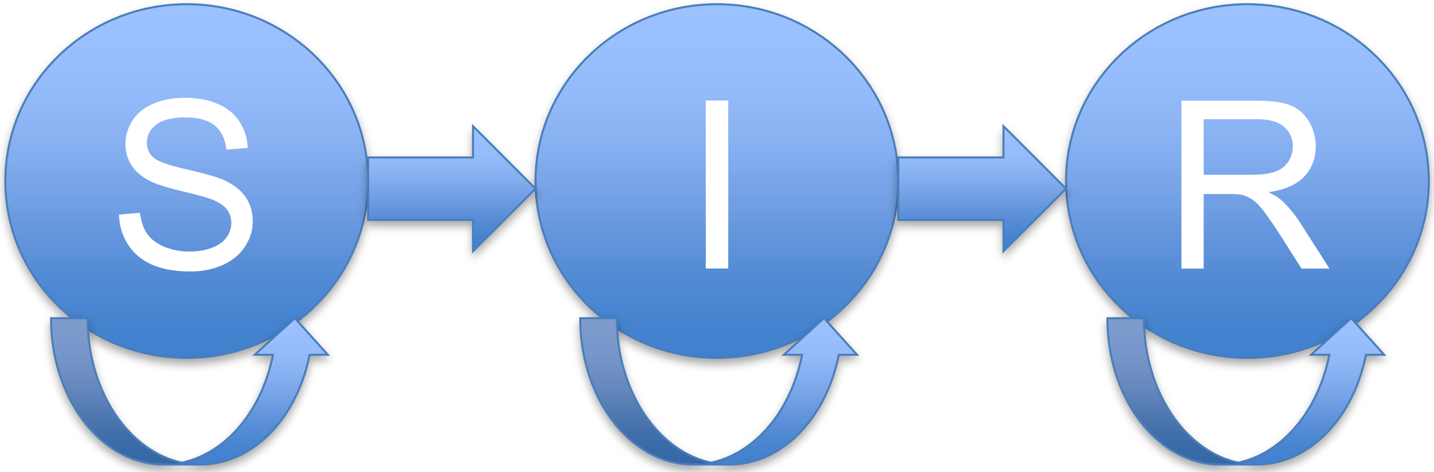
- Epidemic models for malware propagation, by Net Logo open source simulator
- Performance models for MITM and DoS attacks and consequences (QoS) on SCADA and the grid by NS2 open source simulator for telco networks

Results: QoS indicators

- before the attack, normal conditions
- during the attack, anomalous conditions
- after the attack, tail of anomalous conditions

Worm and SIR (Susceptible, Infected, Resistant) model

- A malware (MALicious softWARE) infects a computer and may infect other computers in a network
- Once a computer is infected, it is under the control of the attacker. In our model, an infected node goes in DoS
- Malware spreads itself from computer to computer similarly to epidemics for biological populations



- Node is susceptible
- Malware can reach it

- Node is infected
- Malware controls it

- Node is resistant
- It is immune to malware

SIR epidemic models

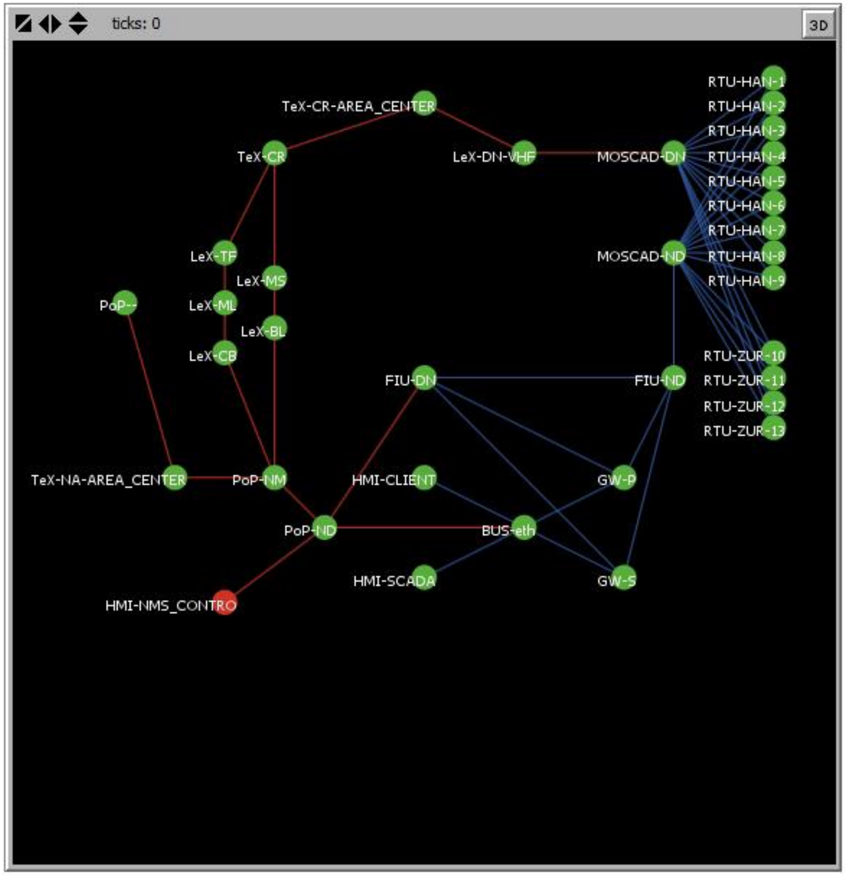
- Classic SIR epidemic models considers all individuals equals, with the same tendency to become infected
- Our model considers each node, which represent an ICT device, with its own different tendency to become infected
- To remove an infection, it's necessary an antivirus scan with a certain probability of success in finding and removing the malware

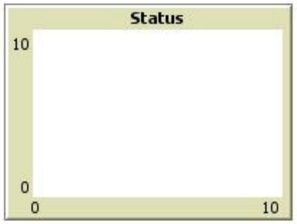
SIR model parameters

- 3 states for each node (S,I,R):
  - transition from S → I: γ
  - transition from I → R: φ
- efficiency of the antivirus: *k*
- number of neighbors of a node: *d*
- infected neighbors at each time step: $\beta = \alpha \cdot d$
  - infectability of the malware: α
- For each node a specific value of parameter according to node typology and the related security solutions (excluded α).

SIR implementation of corporate network and SCADA by NetLogo

NetLogo is a programmable modeling environment for simulating natural and social phenomena.





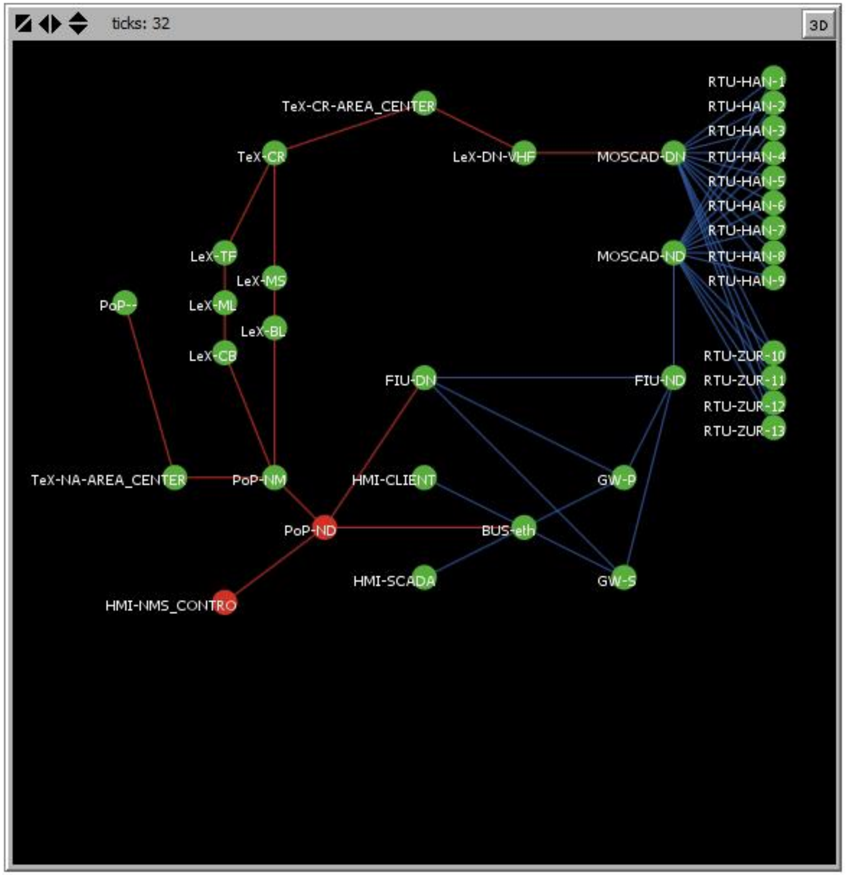
Green: susceptible
Red: infected
Grey: resistant

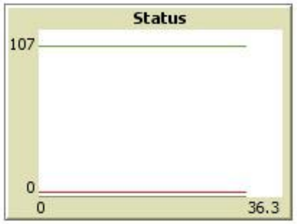
DEMO VERSION GeoVid www.geovid.com

CockpitCI

ENEA AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

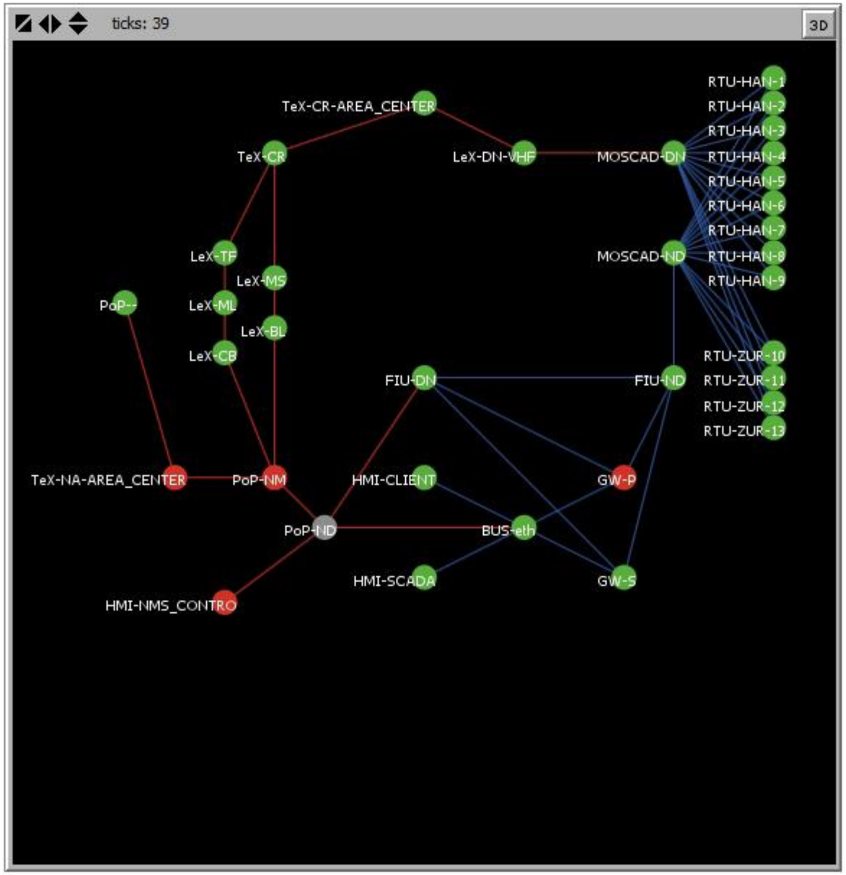
SIR implementation of corporate network and SCADA by NetLogo

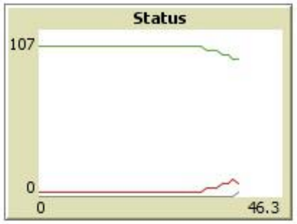




Green: susceptible
Red: infected
Grey: resistant

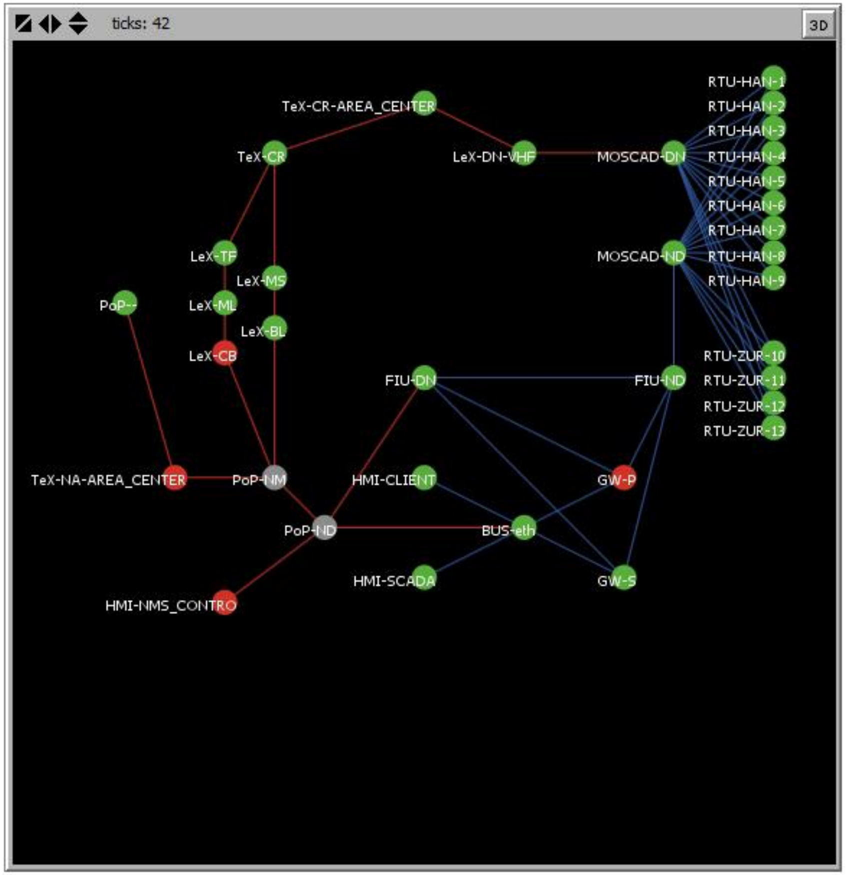
SIR implementation of corporate network and SCADA by NetLogo

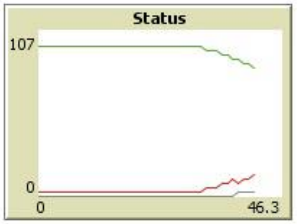




Green: susceptible
Red: infected
Grey: resistant

SIR implementation of corporate network and SCADA by NetLogo

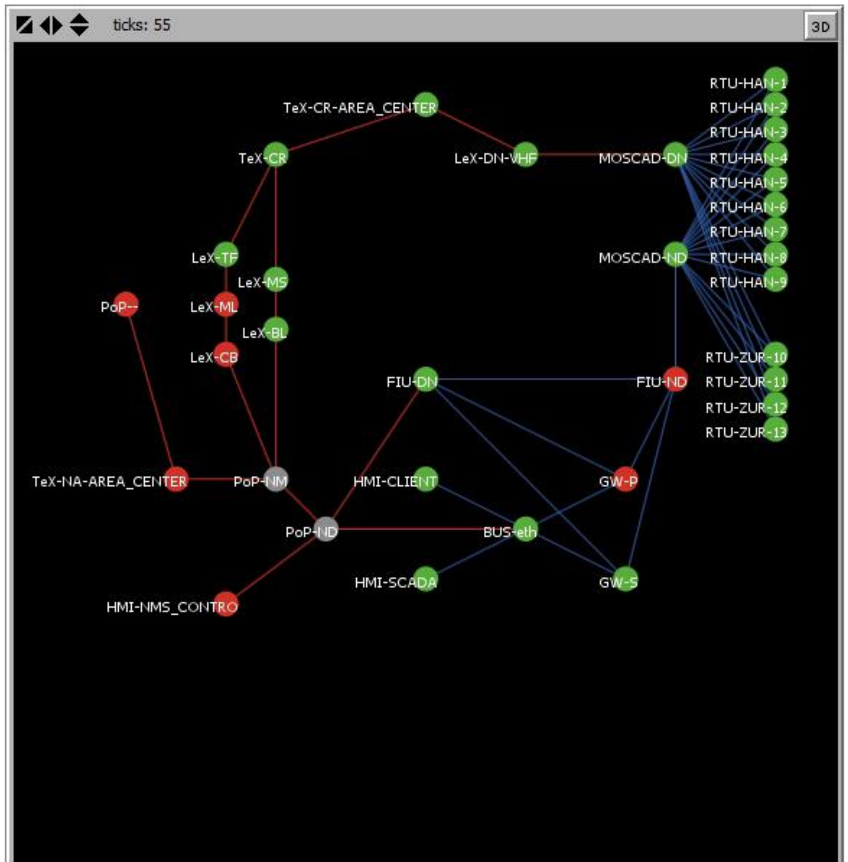


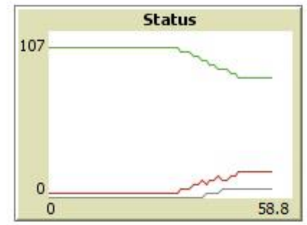


Green: susceptible
Red: infected
Grey: resistant

DEMO VERSION GeoVid www.geovid.com

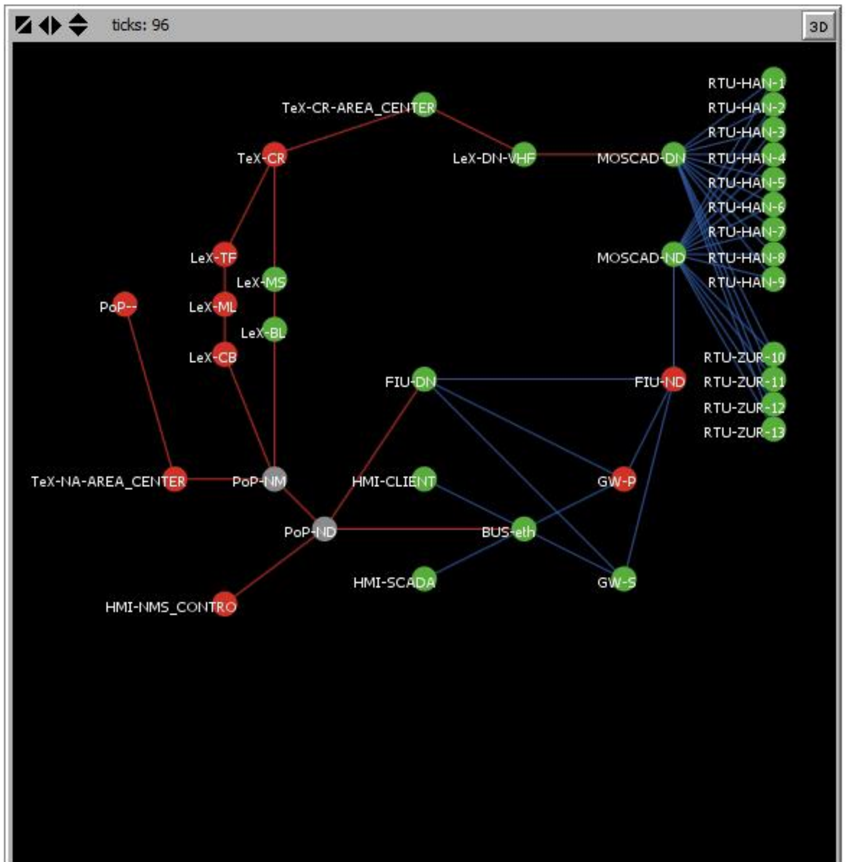
SIR implementation of corporate network and SCADA by NetLogo

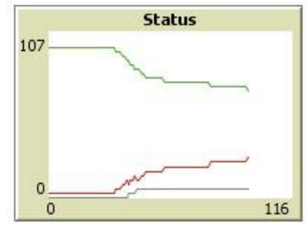




Green: susceptible
Red: infected
Grey: resistant

SIR implementation of corporate network and SCADA by NetLogo





Green: susceptible
Red: infected
Grey: resistant

Modelling assumptions

Assumptions on corporate network

Link Type	**Backbone (DWDM)**	**TeX (STM-16)**	**LeX (STM-4)**
Capacity	10 Gbps	2.5 Gbps	600 Mbps
Source/Destination Node	PoP-PoP	PoP-TeX, TeX-TeX	PoP-LeX , TeX-LeX, LeX-LeX
Traffic Type	TCP+UDP	TCP	TCP
Traffic Bit-Rate	12 GB (TCP) + 8 GB (UDP)	12 GB	12 GB
Type of Agents	CBR for UDP		FTP for TCP
Number of Agents	100 for UDP		100 for TCP

Assumptions on SCADA communication links

Link Type	**Ethernet**	**RS-485**	**RS-232**	**VHF-radio**
Capacity	100 Mbps	19.2 Kbps	19.2 Kbps	4.8 Kbps
Source/Destination Node	SCADA - MCP_T – PoP	MCP_T-FIU FIU- RF modem	RF modem - Telco Nodes	RF modem - RTU
Traffic type	DLC (TCP)+ TCP	DLC (TCP)	DLC (TCP)	DLC (TCP)
Traffic bit-rate	256 bytes /30 sec	256 bytes /30 sec	256 bytes/30 sec	256 bytes /30 sec

DoS & MITM by open source telco simulator: NS2

- Attack initiation source(s)
- Attack target(s)

DoS:

Packet size	
Interval	
N. Of packets sent during the attack	
Flood attack protocol	

MITM

- Intercept of a communication
- Block of the communication to the RTUs

Consequences of cyber attacks on SCADA: indicators by NS2

a) *LoV,* Loss of View - if the SCC can't receive packets from the RTUs.
   In case of MITM, SCC receives false information/data from the attacker and the consequent false observability of the electrical grid from SCC may induce a tricky behavior of SCADA operator;

b) *LoC* , Loss of Control - if the RTUs can't receive packets from the SCC.
   In case of MITM, the RTU receives false commands from the attacker instead of SCC;

c) *DPR, Dropped Packet Rate -* a global vision of how many packets are missing;

d) *TTBP,* Transmission Time Between two Packets;

e) *RTT* , Packet Round Trip Time - composed by TCP transmission time plus ACK transmission time;

c) *Packets routing*.
   It changes in case of MITM

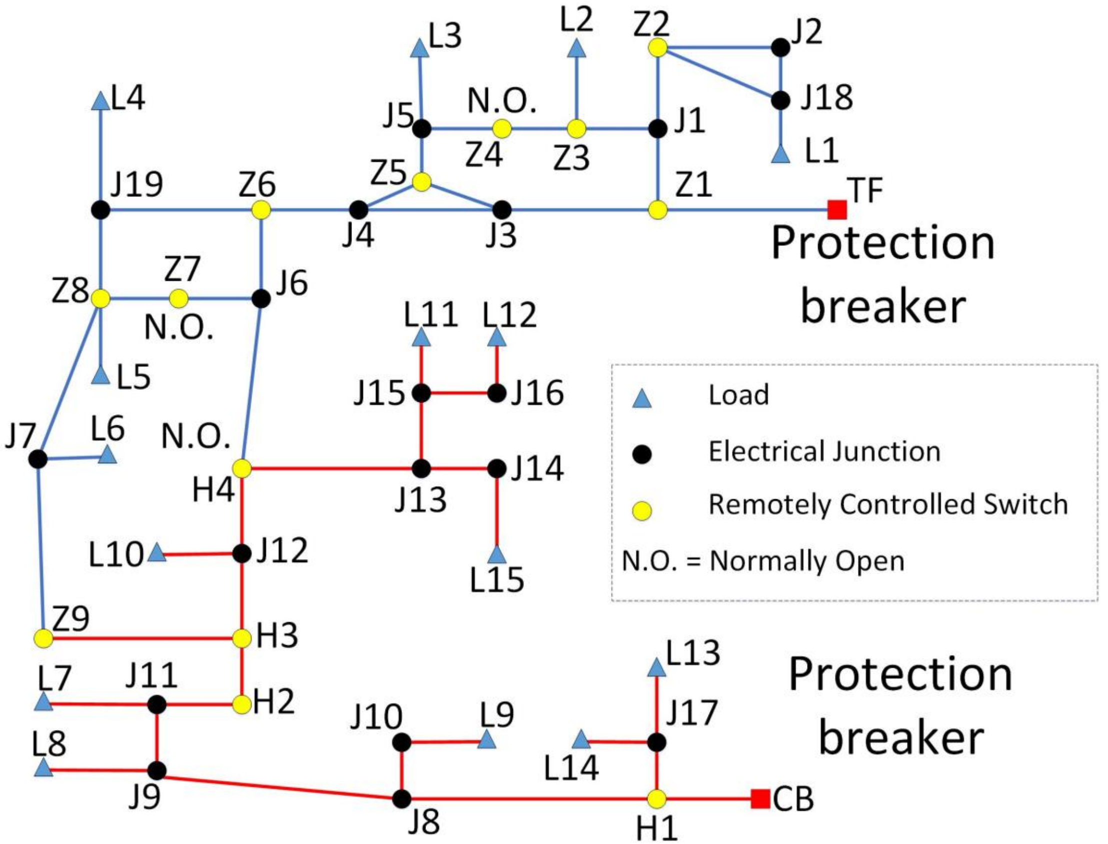
Cyber attacks and consequences on SCADA - QoS results by NS2: DoS and MITM

Attack Source	PoP --	TeX-CR	LeX-BL	Internet
Attack Target	Moscad DN	Moscad DN	Moscad DN	Moscad DN
Start Time [sec]	??	??	??	??
Stop Time [sec]	??	??	101	101
Loss of View (LoV)	??	??	??	??
Loss of Control (LoC)	??	??	??	??
RTT Max/Min [sec]	??	??	??	??
Dropped Packet Rate (DPR)	??	??	??	??
Simulated Time [sec]				
Comput. Time[min]				

SCADA QoS: FISR response time

- FISR response time is intended as the time between the occurrence of loss of electricity supplied to customers (due to a grid failure) and the restoration of electricity to customers

- The time response of FISR service is critical because it is strictly correlated to the quality of electricity to customers.



Consequences of cyber attacks on SCADA & electrical grid

FISR response time on malware spreading, MITM and DoS attacks by NS2

Percentage of grid customers which remain isolated

Grid failure section		Initial	Intermediate	Terminal
Response Time [sec]	Case 1	18,4	34,8	29,1
	Case 2	??	??	??
	Case 3	??	??	??
Affected Customers [%]	Before FISR	??	??	??
	After FISR	??	??	??

FISR response time and % of affected grid customers

for three different sections of the permanent failure on the power grid:

i) failure in an initial section of the grid (bounded by the feeding substation and its closest RTU): the loads of failed sub-grid are energized by the other substation, up to the manual repair, that restores the initial configuration of the grid;

ii) failure in an intermediate section of the grid (bounded by two RTUs): the loads into this section are isolated, the loads bounded by failed the section and the tie switch are powered by the other substation, up to the manual repair, that restores the initial configuration of the grid;

iii) failure in a terminal section of the grid (bounded by RTU and loads): the loads of failed section are isolated, up to the manual repair, that restores the initial configuration of the grid.

for different operative conditions of SCADA system and corporate network:

case 1) normal condition of the SCADA system and corporate network before attack consequences i.e. initial infection spreading;

case 2) the attcak, i.e. the infection spreading gets out of service the primary connection between SCADA Control Centre and RTUs;

case 3) on failure of the primary connection between SCC and RTUs, any cyber attack (Malware or DoS OR mitm) gets out of service the back up connection between SCC and RTUs;

- The operator looses the grid observability and controllability as final consequence of the attack.

Modelling versus an hybrid testbed

- Modeling is in charge of predicting consequences of cyber attacks on SCADA and the electrical grid

- while the test bed is in charge to reproduce cyber attacks and their propagation more realistically then modeling

- the hybrid test bed is constituted by the coexistence of actual and simulated systems and devices of SCADA, corporate network and the electrical grid

  - Ideally, to validate CockpitCI tool

Validation process

- to be performed through different phases, with an incremental approach, starting from the scenario identified in CIGRE demo up to a set of selected use cases (i.e. from D2.2 Reference Scenario)

- in a first phase CockpitCI tool is considered as a black box
  - interfaces of the tool with the physical infrastructure have to be carefully identified, in terms of CockpitCI tool inputs and outputs

- the physical infrastructure and cyber attack cases have been respectively fully described and proposed within D2.2 Reference Scenario deliverable

- the HTB (Hybrid Test Bed) is under continuous improvement in IEC
  - to host the deployment of CockpitCI tool interfaced with the physical infrastructure
  - to perform the validation with an incremental approach
  - the incremental approach regards the tool deployment, the HTB functionality and validation purpose.

Rif. “Food for thoughts: ENEA preliminary contribute for validation of CockpitCI tool” internal CockpitCI document - July 2014

The tool is intended composed by

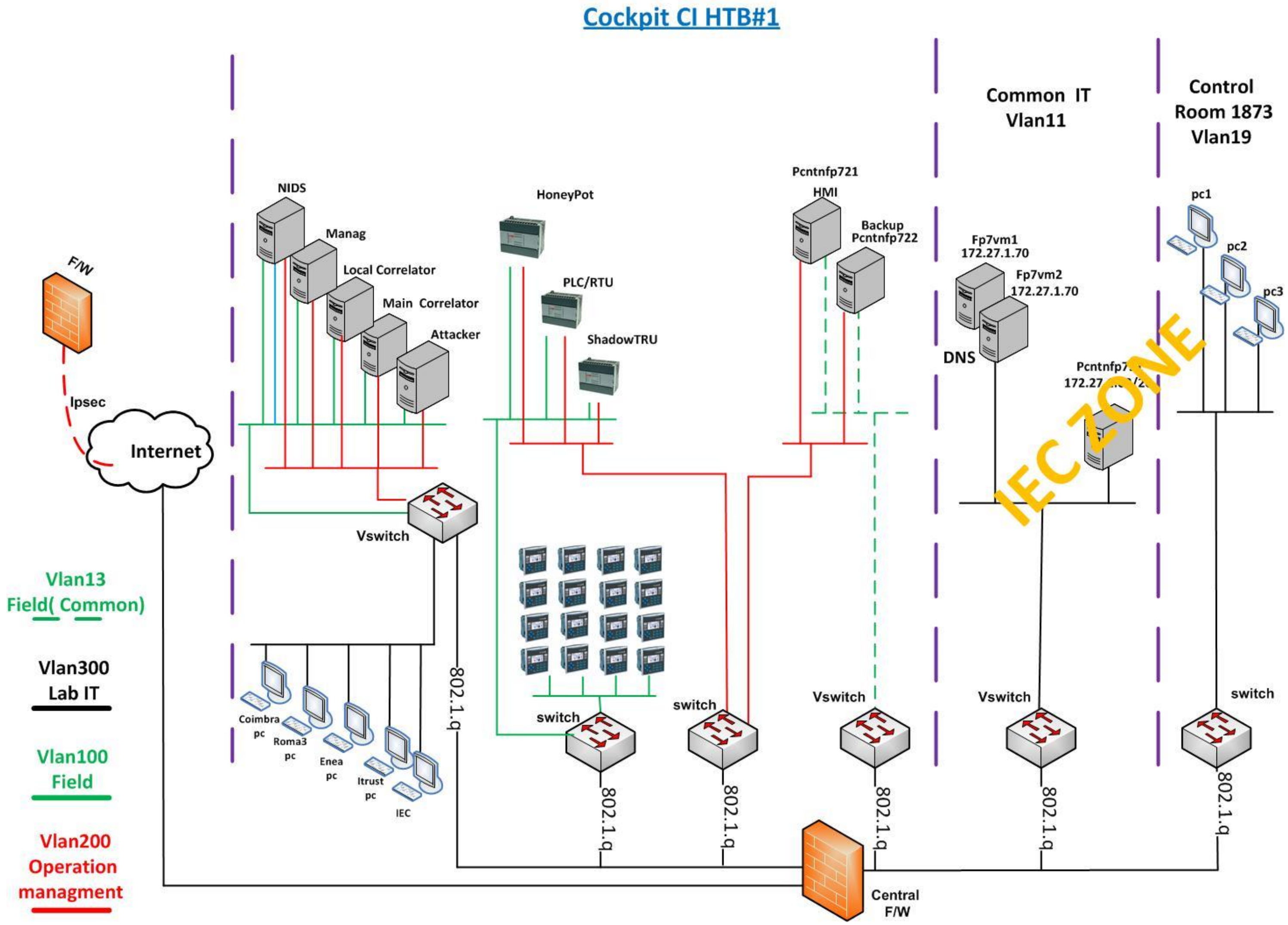
- interfaces with the physical infrastructure
- SMGW/SMN,
- Detection Layer
- Risk predictor

Validation of CockpitCI tool

the following items are needed to be identified:

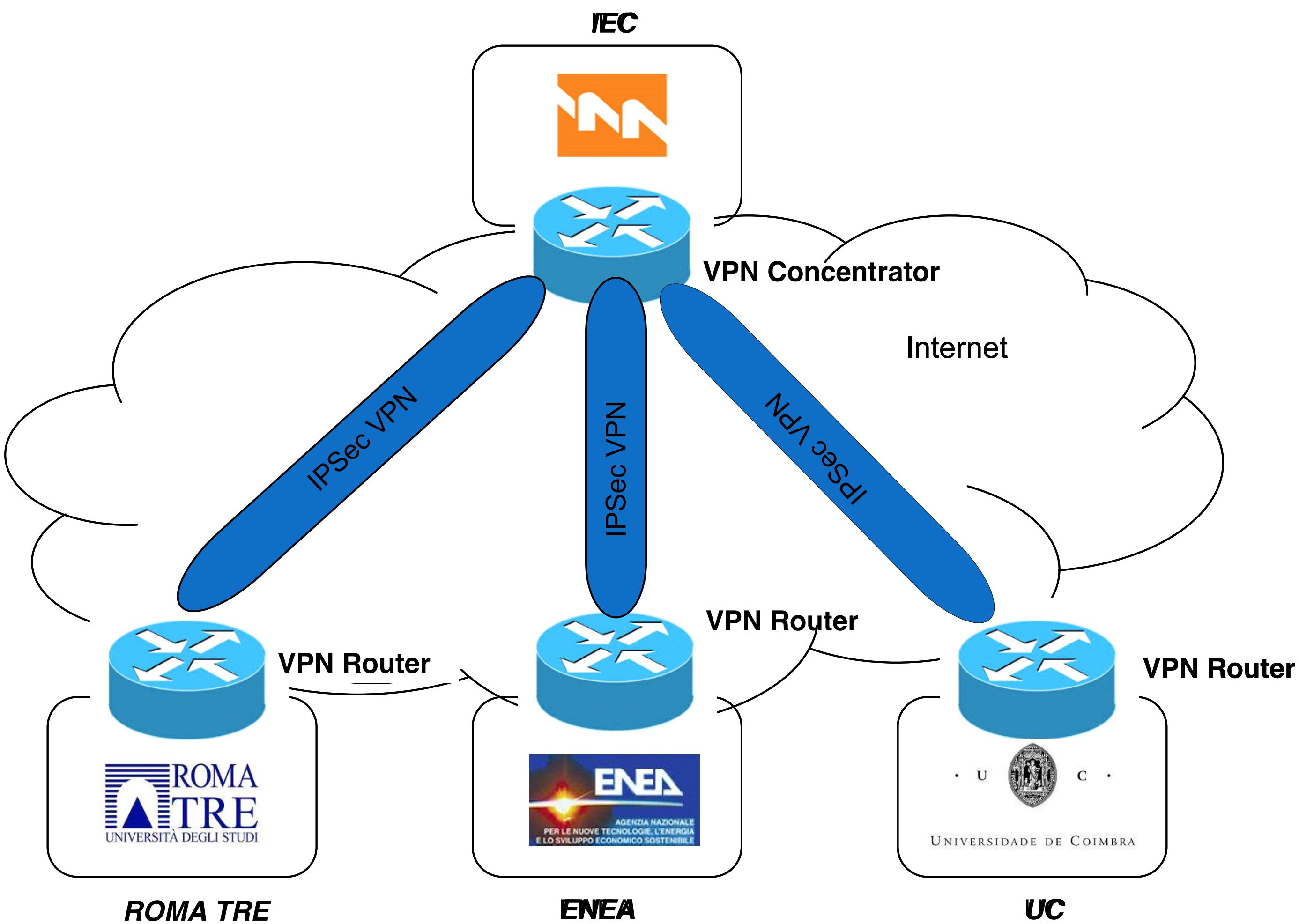
- the normal state of the physical infrastructure
  - without any cyber attacks and without CockpitCI tool;
  - without any cyber attacks and with CockpitCI tool: in this case, it is expected that CockpitCI tool do not modify the normal state (in value and in time)
- the deviation from the normal state of the physical infrastructure (in time and value) as effect of selected cyber attacks:
  - without CockpitCI tool;
  - with CockpitCI tool. Capability of CockpitCI tool in terms of Attack Detection, Risk prediction and Risk mitigation are to be shown.

IEC Hybrid Test Bed (HTB)

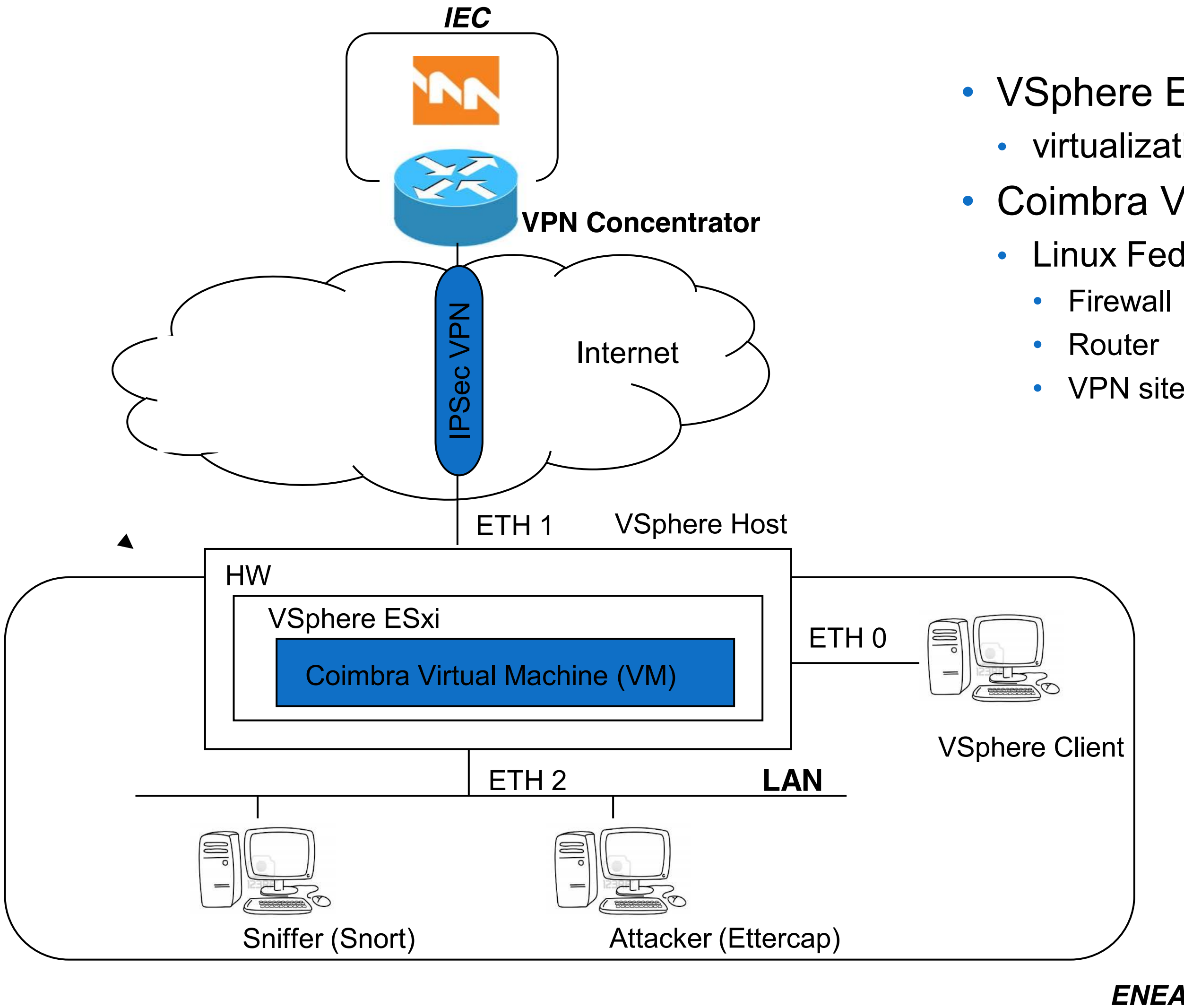


Remote test beds versus IEC HTB

by IPSEC VPN with IEC testbed using Coimbra VM first and Checkpoint then

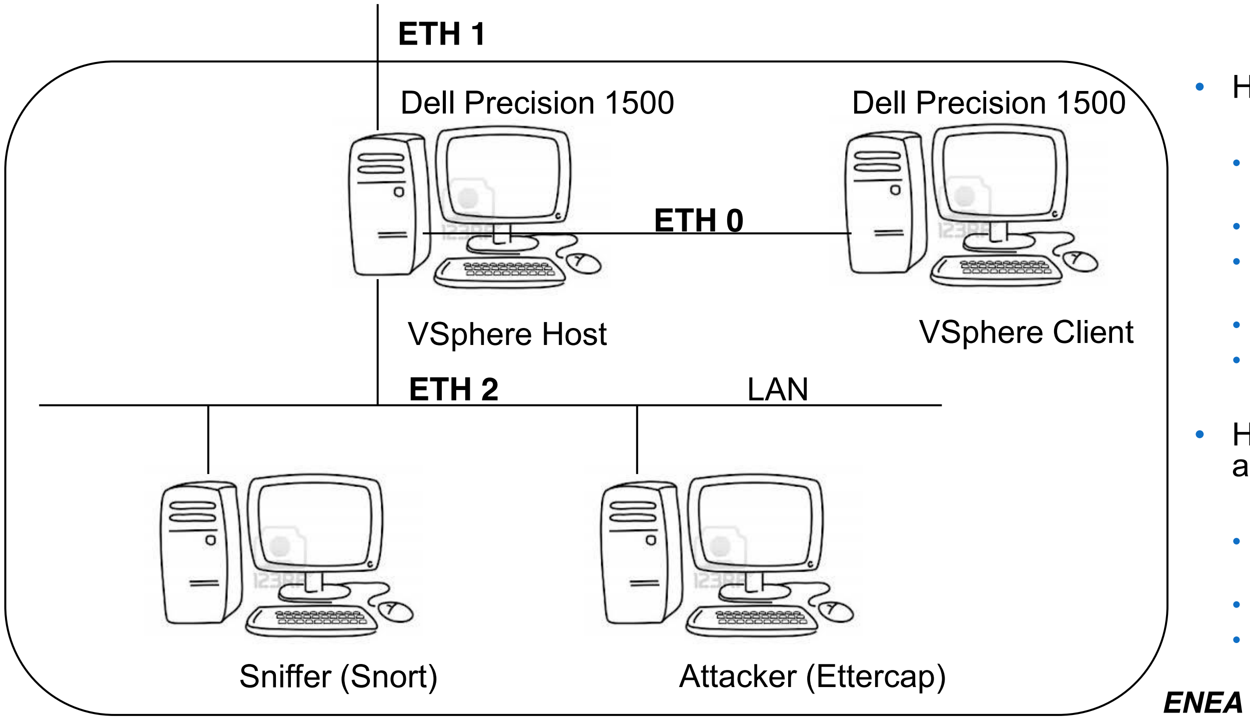


Open Source Solution by Coimbra VM



- VSphere ESxi:
  - virtualization platform
- Coimbra Virtual Machine (VM):
  - Linux Fedora 16
    - Firewall
    - Router
    - VPN site-to-site

Hardware Features of Testbed at ENEA



- Hardware VSphere Host:
  - Processor: Intel Core i7 CPU 860 @ 2.80 GHz
  - RAM: 8 GB
  - NIC 0: Broadcom NetLink Gigabit Ethernet
  - NIC 1: Intel PRO GT 1000
  - NIC 2: Intel PRO GT 1000
- Hardware VSphere Client, Sniffer and Attacker:
  - Processor: Intel Core i3 CPU 530 @ 2.93 GHz
  - RAM: 4 GB
  - NIC 0: Broadcom NetLink Gigabit Ethernet

QUALITY OF SERVICE INDICATORS SIMULATION UNDER CYBER ATTACKS USING INTELLIGENT RAO SIMULATOR

4th CockjpitCI Workshop (Bucharest 16.09.2014)

S.Iassinovski
Multitel

Information Society

Table of content

System structure (ECI, CCI, SCADA, RTUs)

ECI Reference scenario - FISR

Simulation tool: Intelligent RAO simulator

CCI/SCADA Modeling framework

Simulation model implementation

1. ECI simulation
2. FISR process simulation
3. SCADA simulation
4. CCI under cyber attack simulation

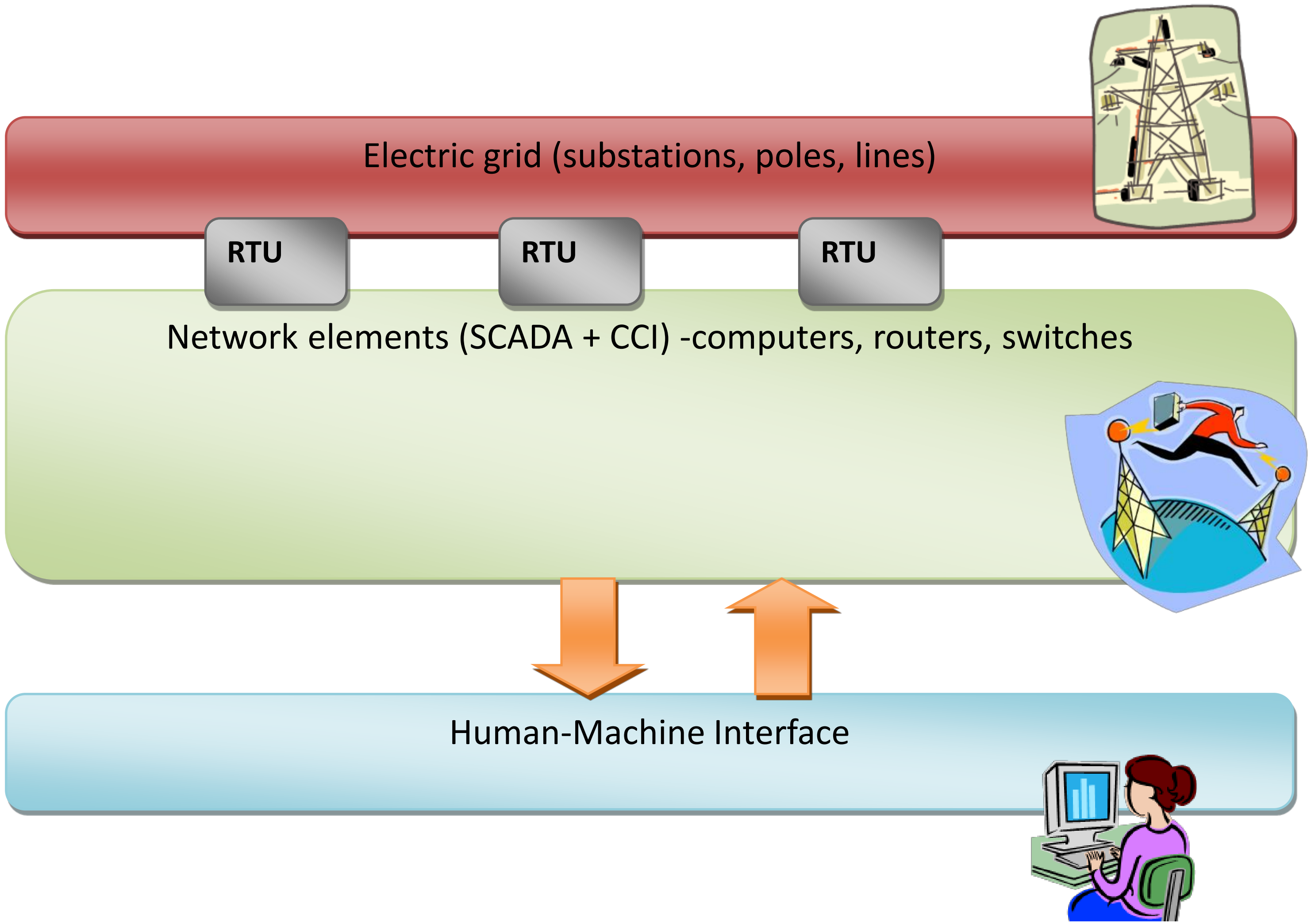
Quality of service indicators

Manual simulation

FISR simulation results on different segments

Cockpit CI

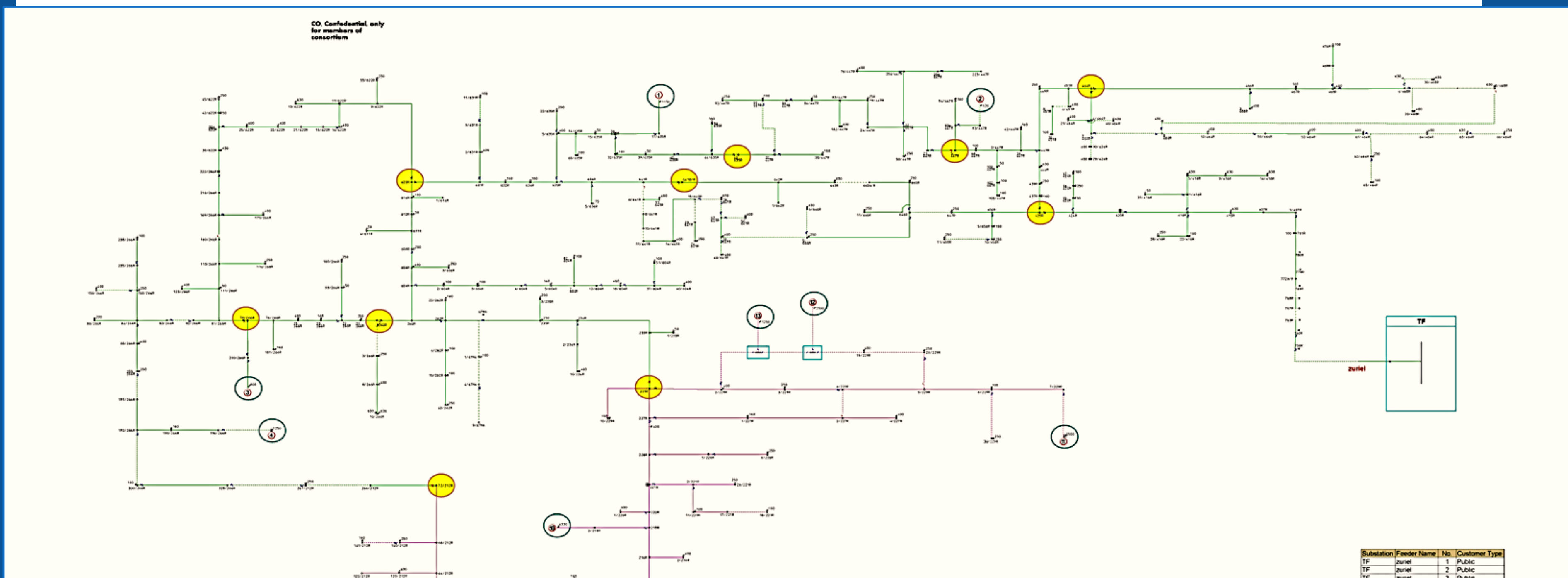
Three-layers view on the system



Cockpit CI

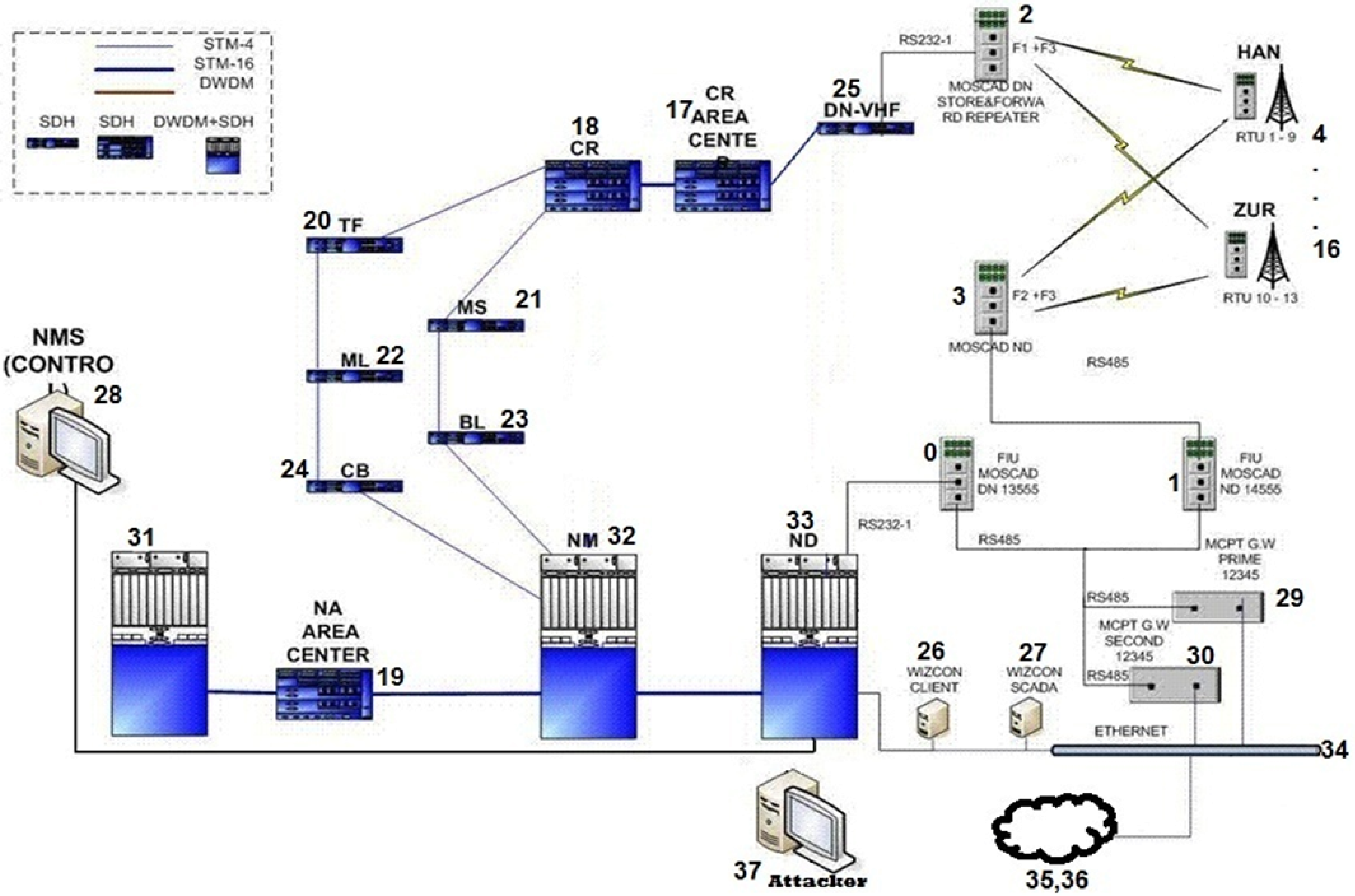
ECI: Reference scenario fragment

Zuriel feeder of TF substation



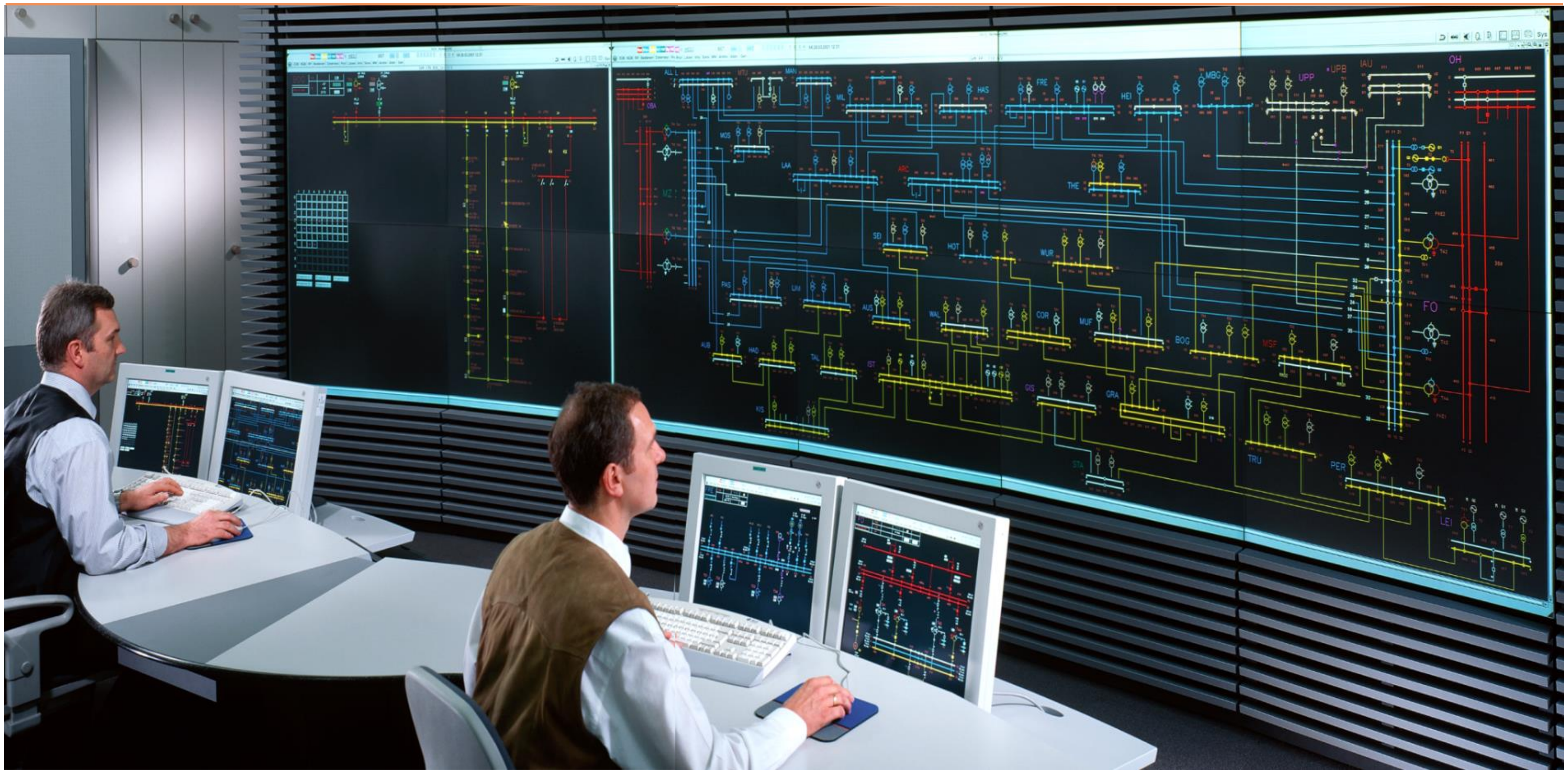
Cockpit CI

Information and telecommunication CI



Cockpit CI

IEC SCADA control center



Cockpit CI

CI/ECI intersection point - RTU

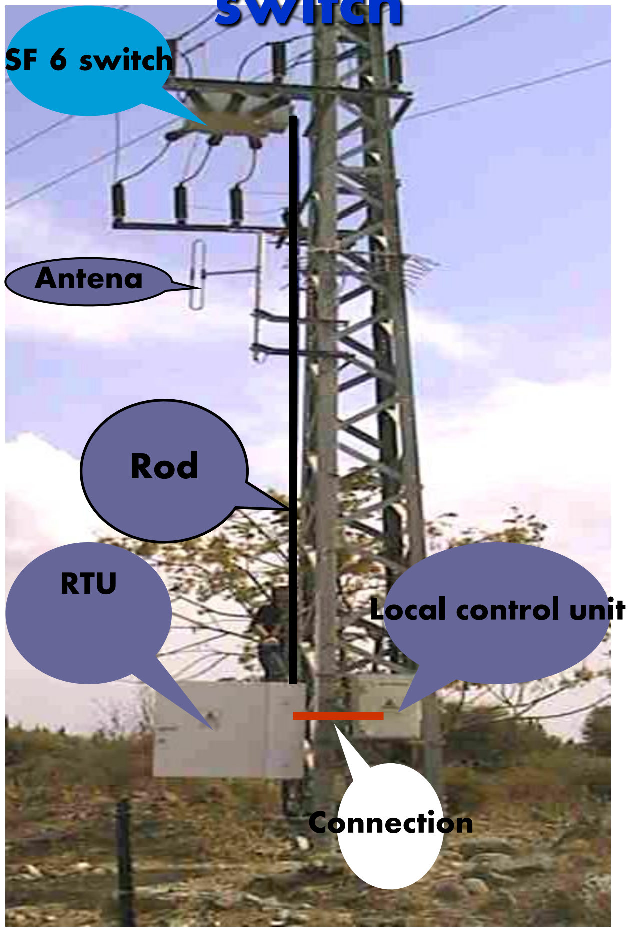
Automatic fault localization and isolation on the ECI is not possible without telecommunication and SCADA running

This affects the ECI QoS indicators and thus the level of risk under cyber attack

State of the art: a lot of works, models, ECI, CI, cyber security, but almost nothing on ECI QoS under cyber attack

Need a modeling tool capable to model and simulate heterogeneous ECI, CI, SCADA and cyber attacks

Pole mounted switch



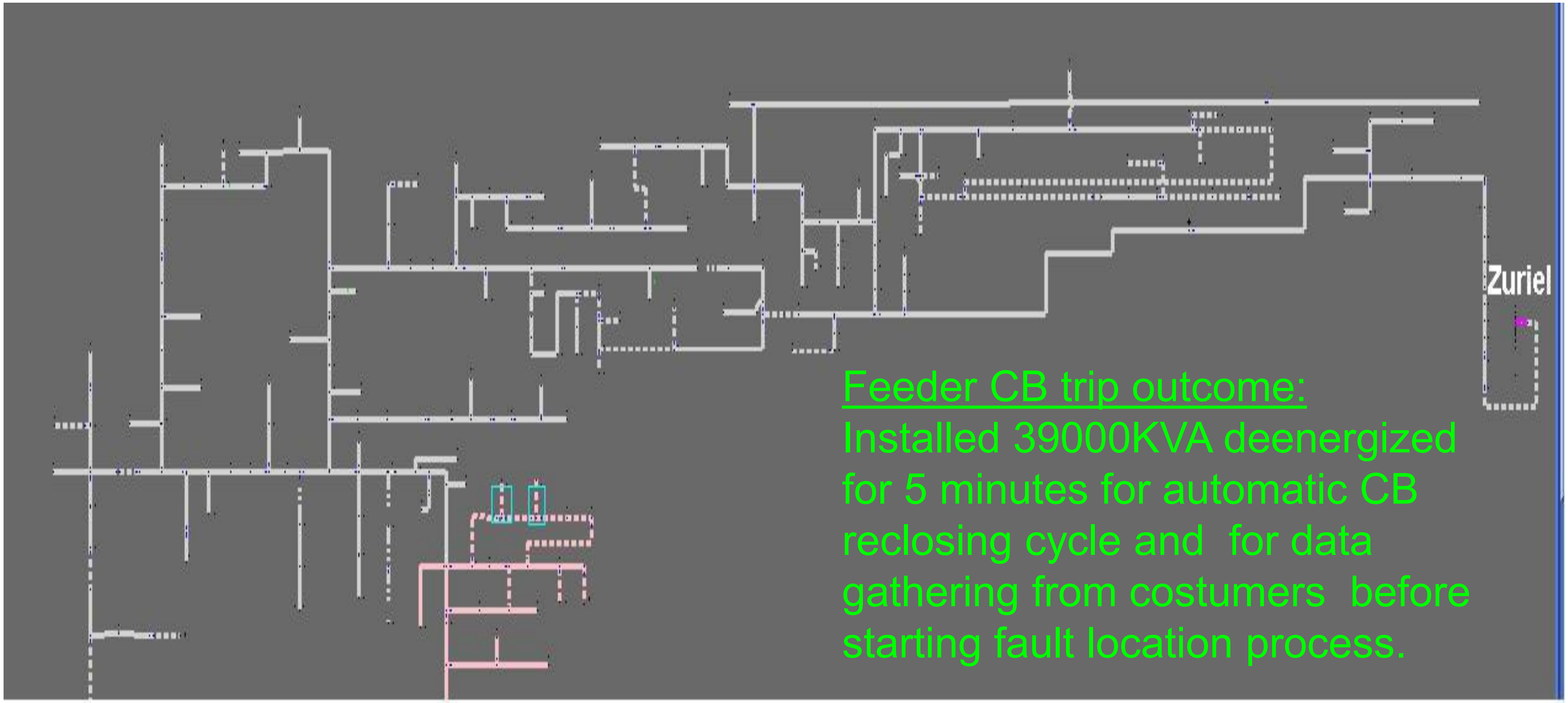
Cockpit CI

What do we need to model and simulate?

- **Electrical infrastructure** (our reference scenario – fragment of MV distribution grid supplied by Zuriel feeder of TF HV/MV substation)
- **Communication infrastructure and SCADA**
- **RTUs and switches**
- **SCADA procedures** (our reference scenario – fault isolation and system restoration (FISR) process)
- **Cyber attacks**
- **QoS indicators**

Cockpit CI

FISR example: Zuriel CB trips by protection

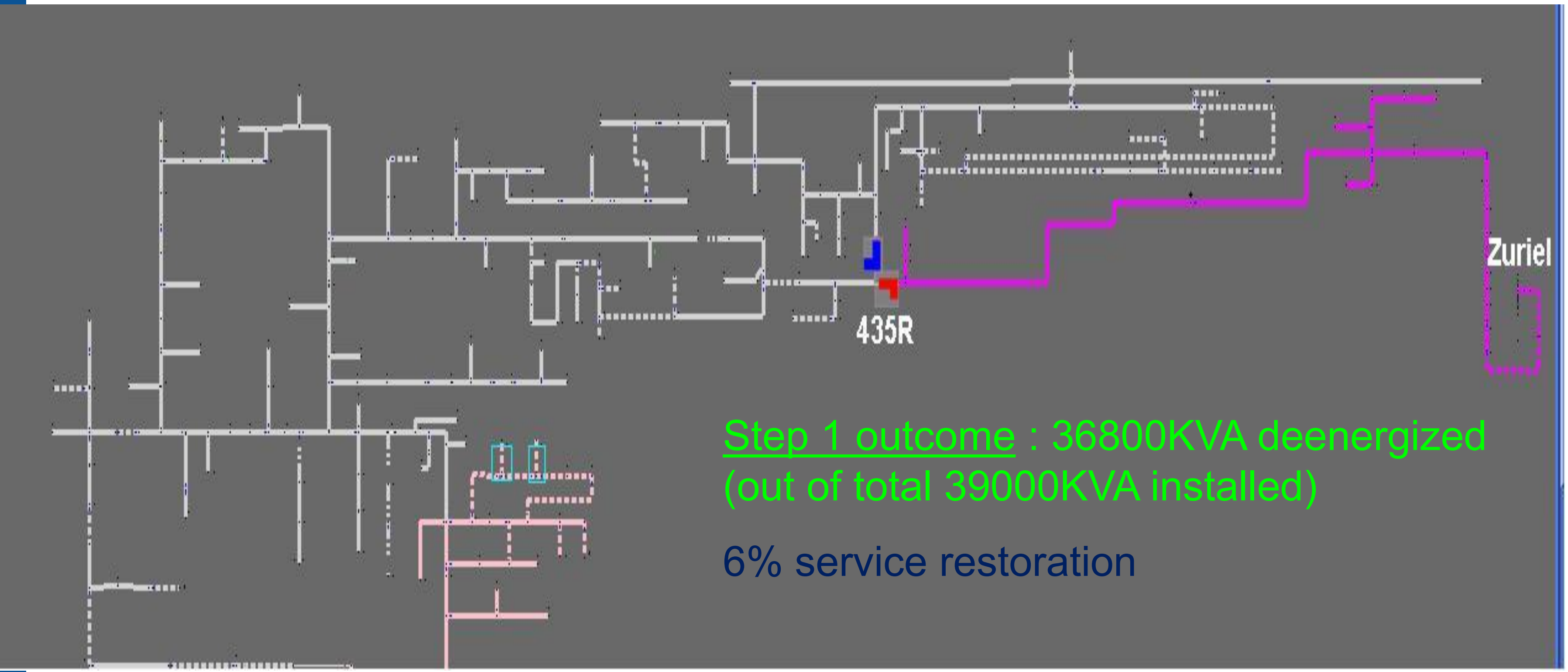


Alarms from SCADA for Feeder CB tripping event:

- Audible notification : Gong
- Substation button and CB symbol are blinking on SCADA display
- Feeder is colored by white to symbolize a deenergized status

Cockpit CI

Fault Location Process-step 1

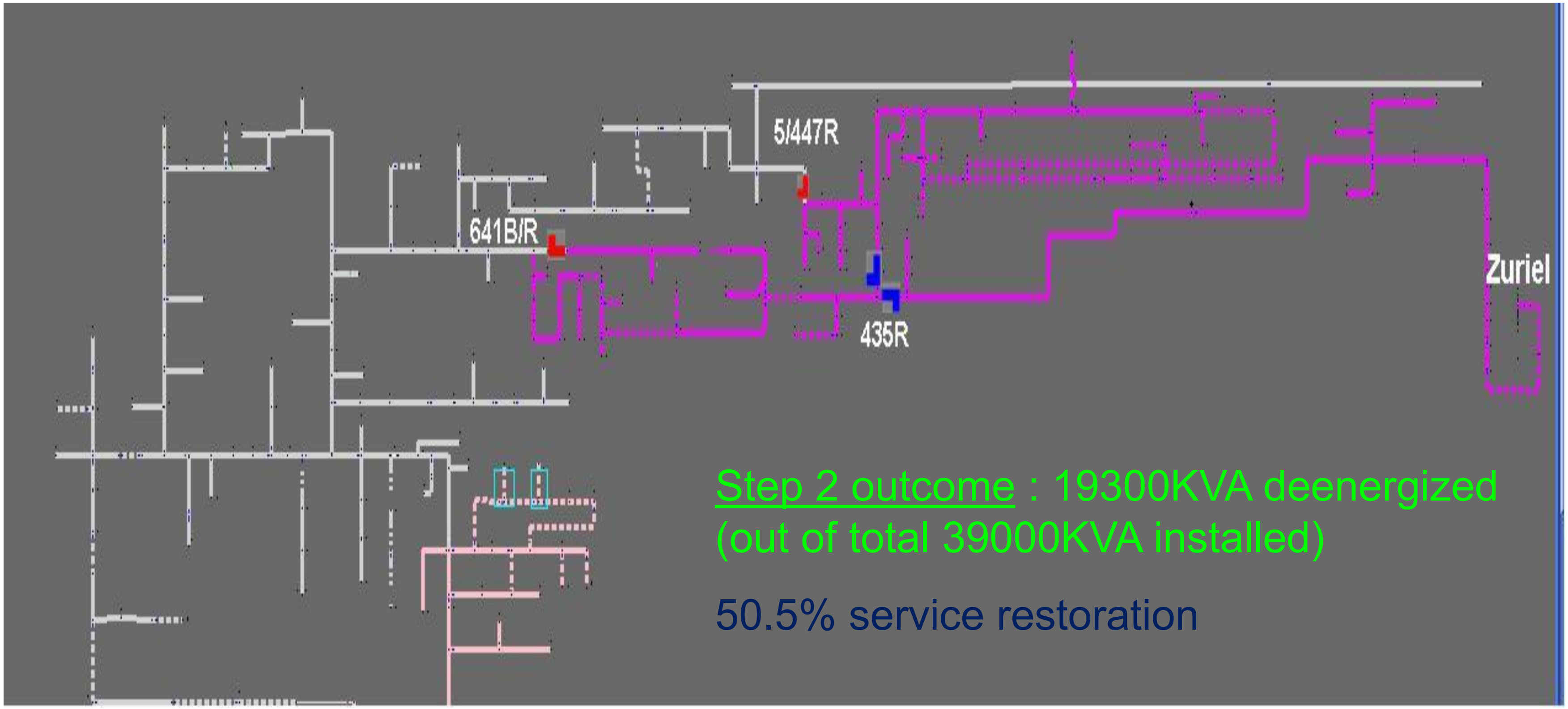


Fault Location process – step 1 (6 min after CB trip):

- First downstream switch (435R) opened
- Feeder CB closed
- If feeder CB does not trip and no alarms, continue to step 2

Cockpit CI

Fault Location Process-step 2

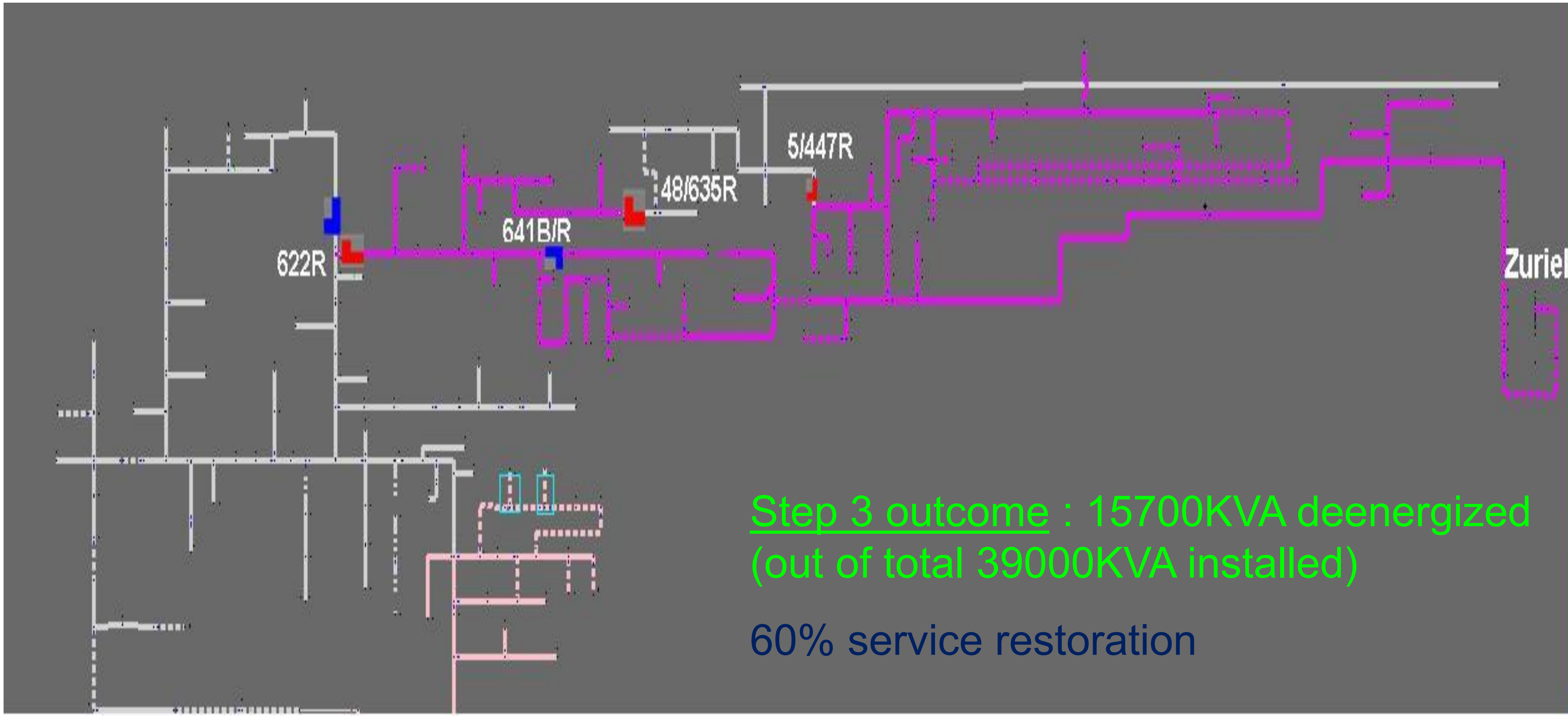


Fault Location process – step 2 (7 min after CB trip):

- Second downstream switch (641B/R) opened
- First downstream switch (435R) closed
- If feeder CB does not trip and no alarms, continue to step 3

Cockpit CI

Fault Location Process-step 3

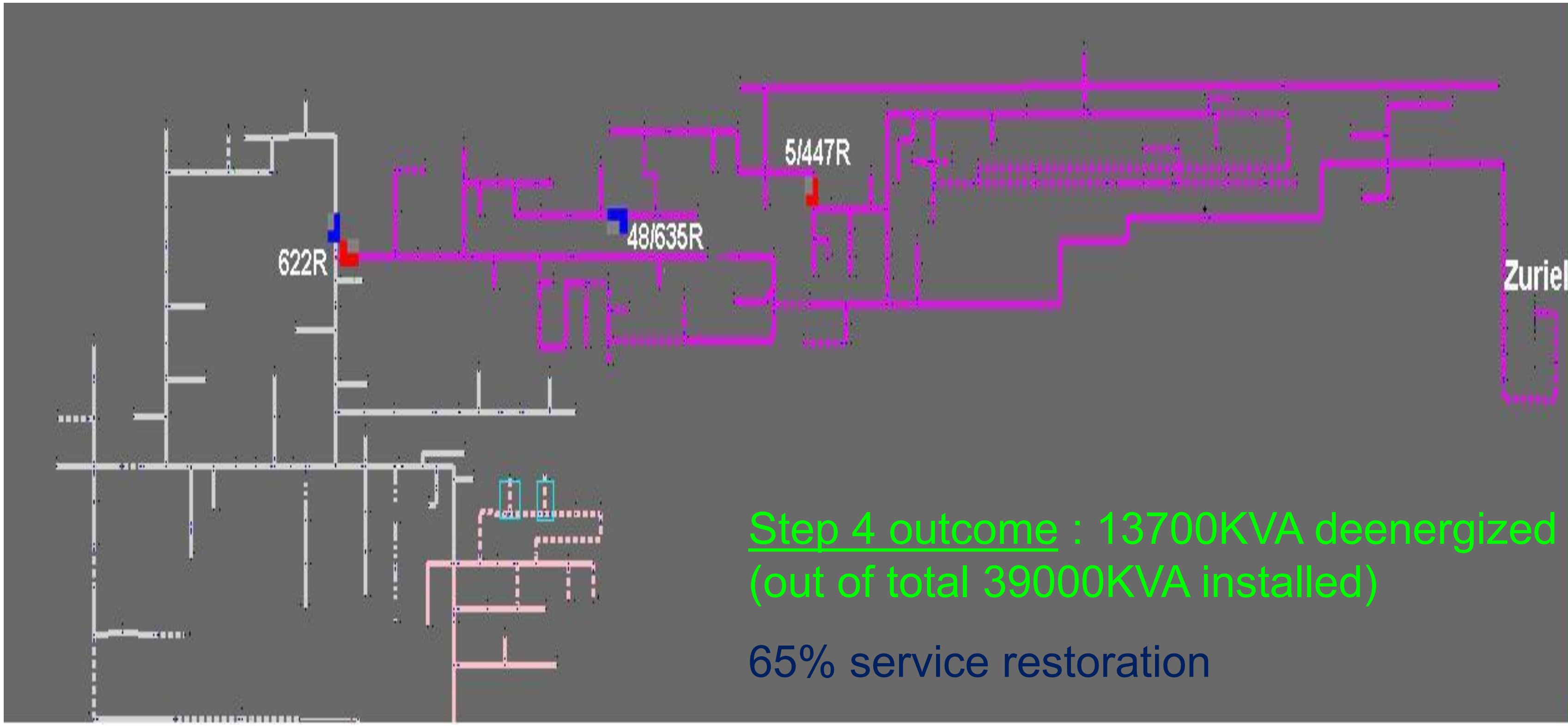


Fault Location process – step 3 (8 min after CB trip):

- 3th downstream switch (622R) opened
- 4th downstream switch (48/635R) opened
- 2th downstream switch (641B/R) closed
- If feeder CB does not trip and no alarms, continue to step 4

Cockpit CI

Fault Location Process-step 4

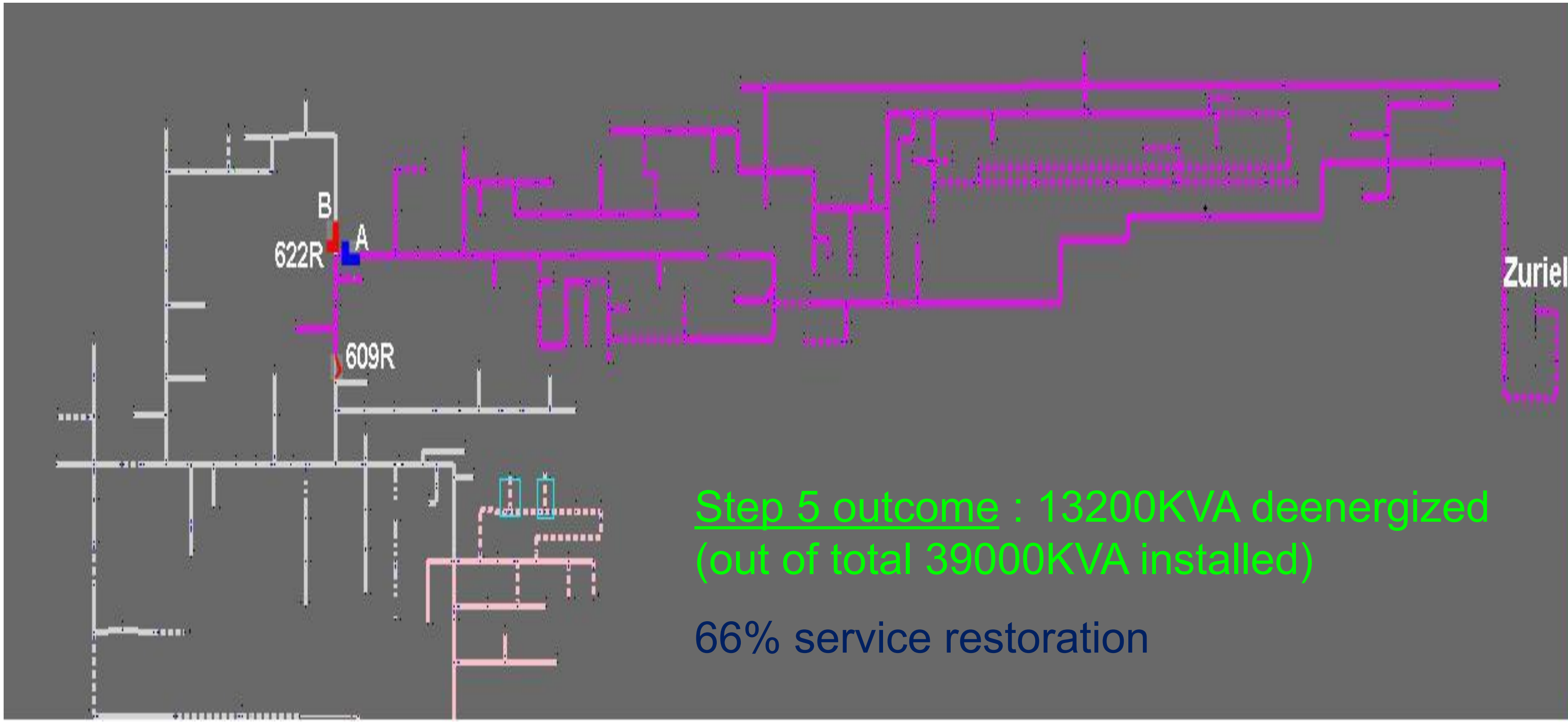


Fault Location process – step 4 (9 min after CB trip):

- 4th downstream switch (48/635R) closed
- If feeder CB does not trip and no alarms, continue to step 4

Cockpit CI

Fault Location Process-step 5

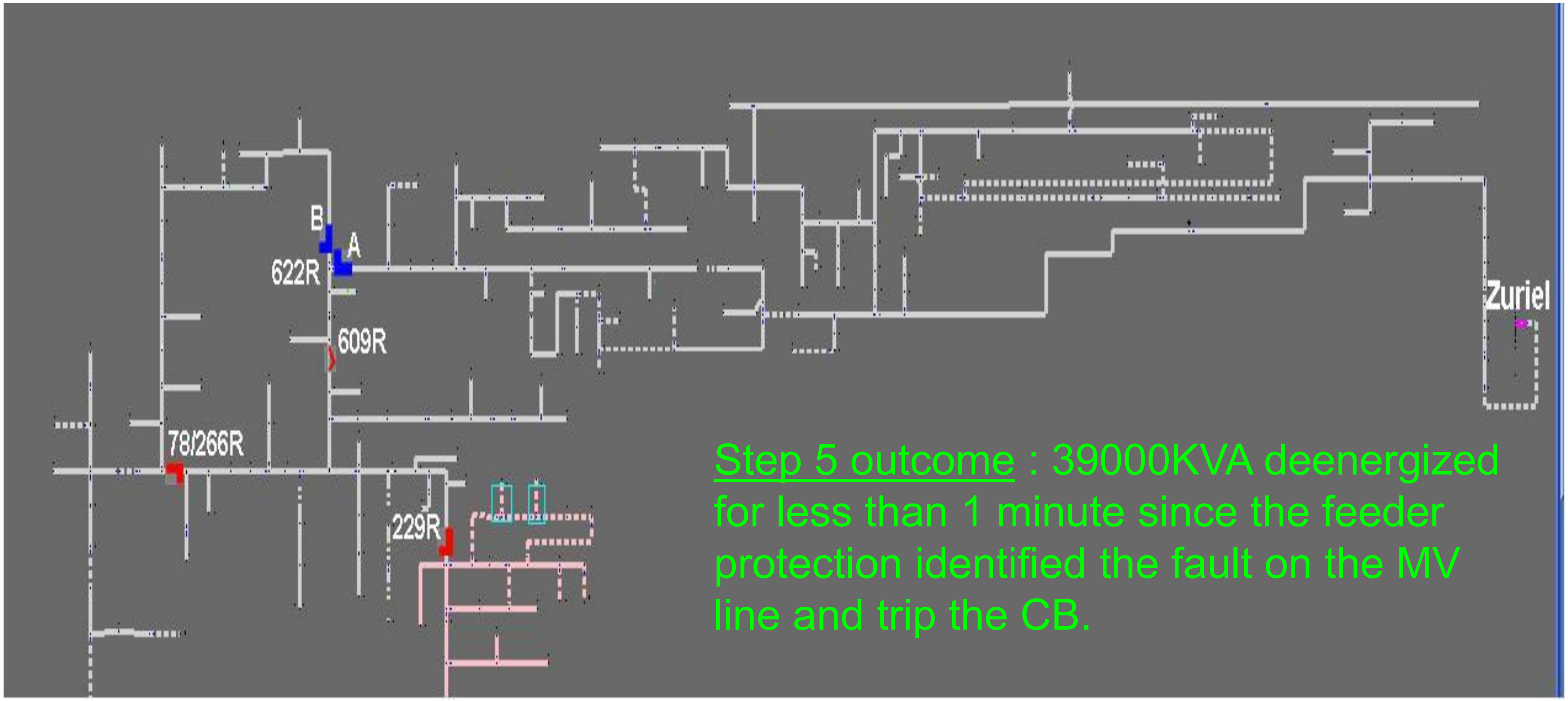


Fault Location process – step 5 (10 min after CB trip):

- 6th downstream switch (622R:B) opened
- 3th downstream switch (622R:A) closed
- If feeder CB does not trip and no alarms, continue to step 6

Cockpit CI

Fault Location Process-step 6

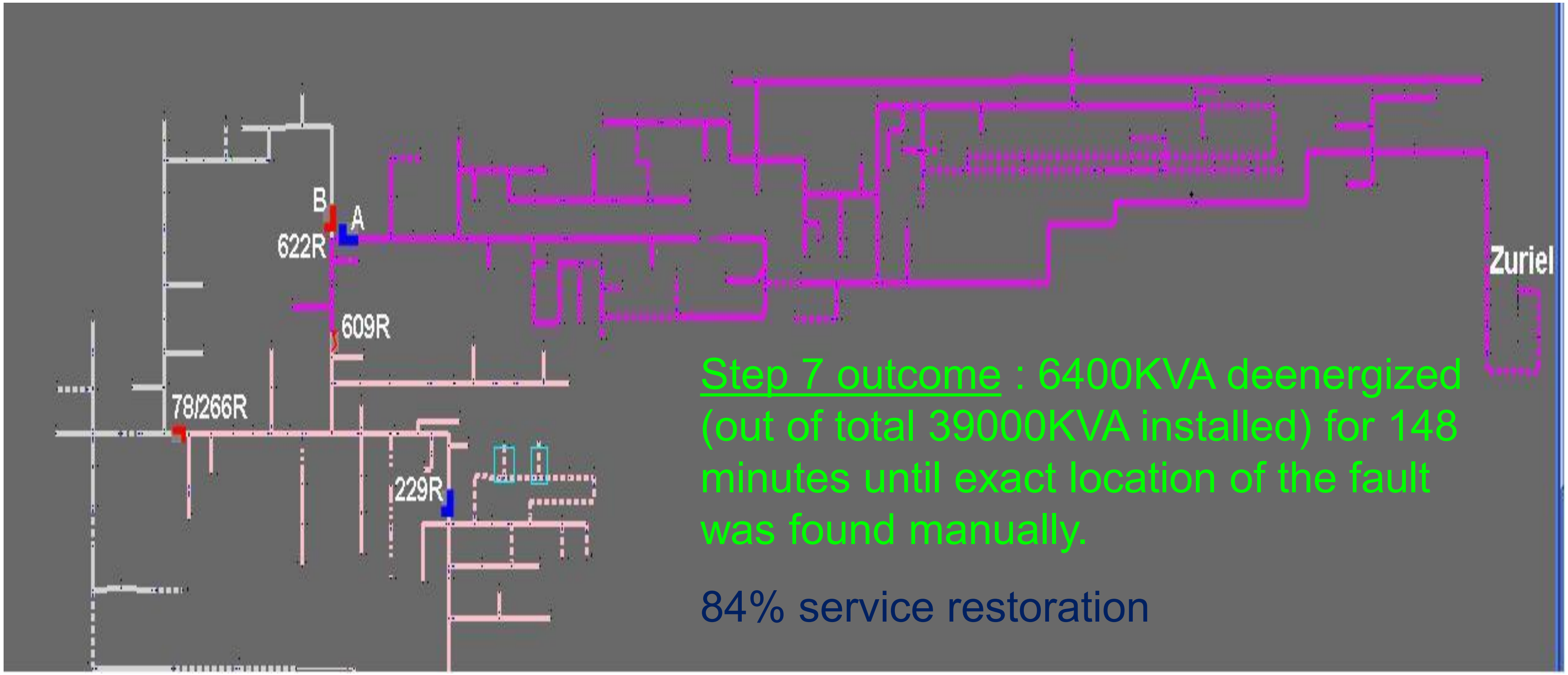


Fault Location process – step 6 (11 min after CB trip):

- 7th downstream switch (78/266R) opened
- 6th downstream switch (622R:B) closed
- Zuriel CB tripped due to a fault on MV line. continue to step 7

Cockpit CI

Fault Location Process-step 7

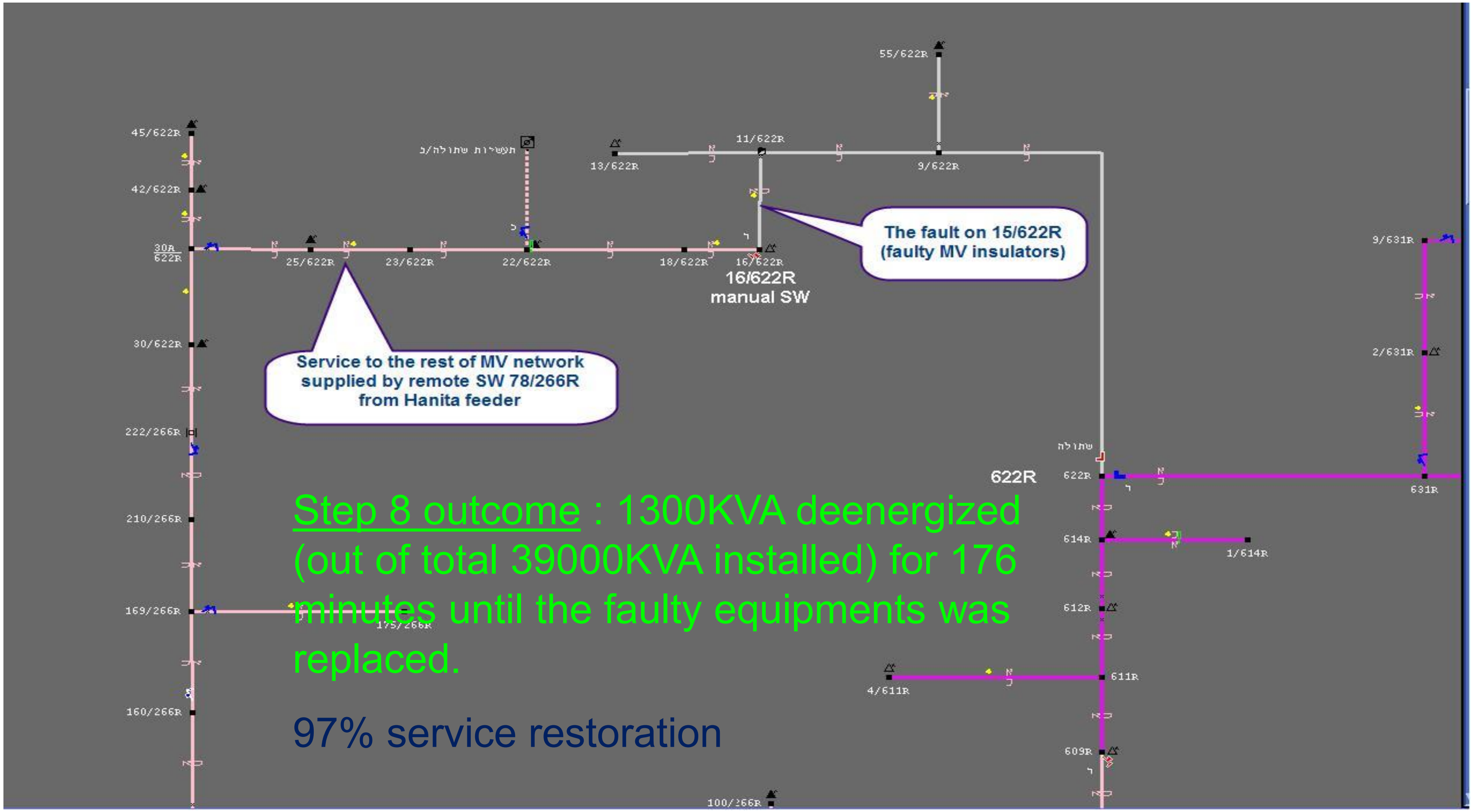


Fault Location process – step 7 (12 min after initial CB trip):

- 6th downstream switch (622R:B) opened and zuriel CB closed
- An alternative supply switch (229R) closed , for service restoration from Hanita feeder

Cockpit CI

Fault isolating Process-step 8



Fault isolating process – step 8 (148 min after initial CB trip):

- The fault located and isolated manually and than service to the rest of MV network supplied by remote switch 78/266R from Hanita feeder.

Cockpit CI

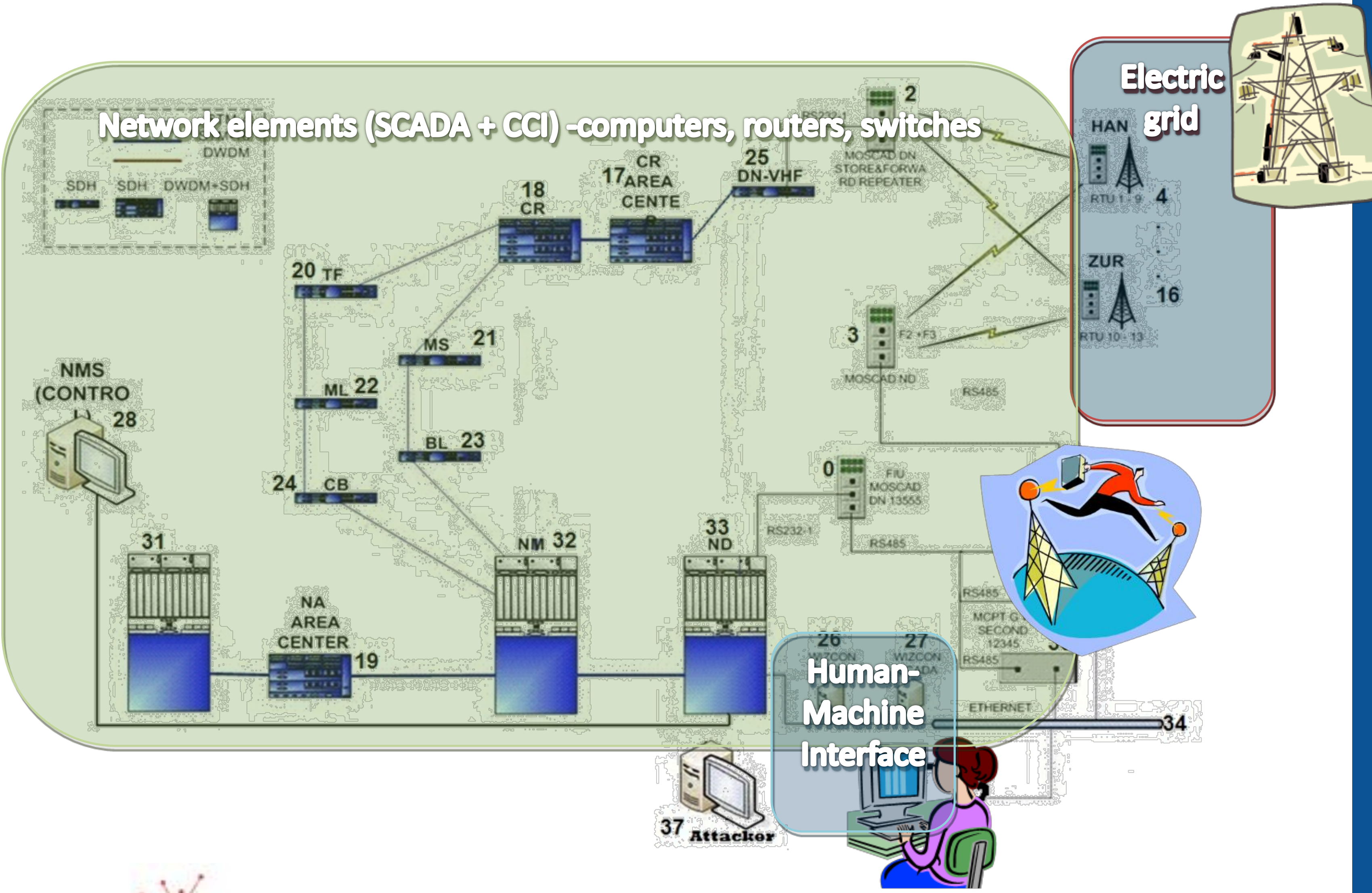
QoS: Calculation of outage duration per customer

STEP	Unsupplied KVA	Duration [min]
0	39000	5
1	36800	1
2	19300	1
3	15700	1
4	13700	1
5	13200	1
6	Not counted - less than 1 minutes	
7	6400	148
8	1300	176

$t_n = \sum(KVA * Duration) / Installed\ KVA = 1469700/39000 = 37.7$ minutes

Cockpit CI

CockpitCI reference scenario: FISR + cyber attack



Cockpit CI

Simulation of ECI QoS under cyber attack: RAO tool

To implement the QoS indicators under cyber attack simulation model, we use the discrete-event simulation and Intelligent RAO simulator

In this approach, one need to represent:

1. objects of a real complex system and
2. the way they are interacting (process or behaviour)

Once the simulation model is developed, we can run numerous simulations to study system behaviour on various scenarios (including cyber attack scenarios) and to calculate necessary QoS indicators

I does not matter in this approach whether we study a homogeneous system or a heterogeneous system of systems

Cockpit CI

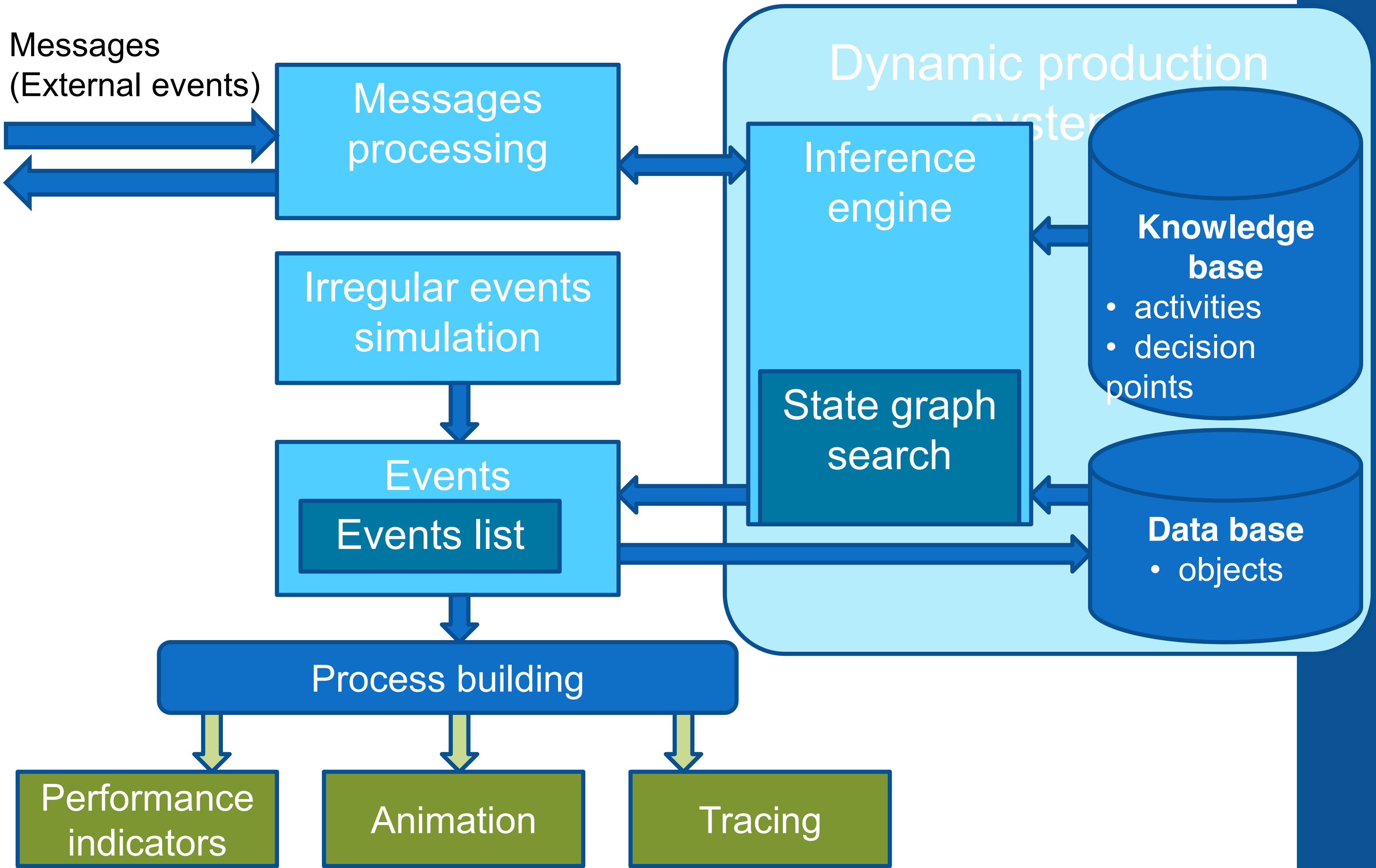
Intelligent RAO simulator

A hybrid tool based on artificial intelligence for on line and off line optimisation and decision making

1. A discrete-event simulator
2. An expert system engine
3. An optimization tool (state graph search)
4. A data driven programming tool

Cockpit CI

RAO: structure



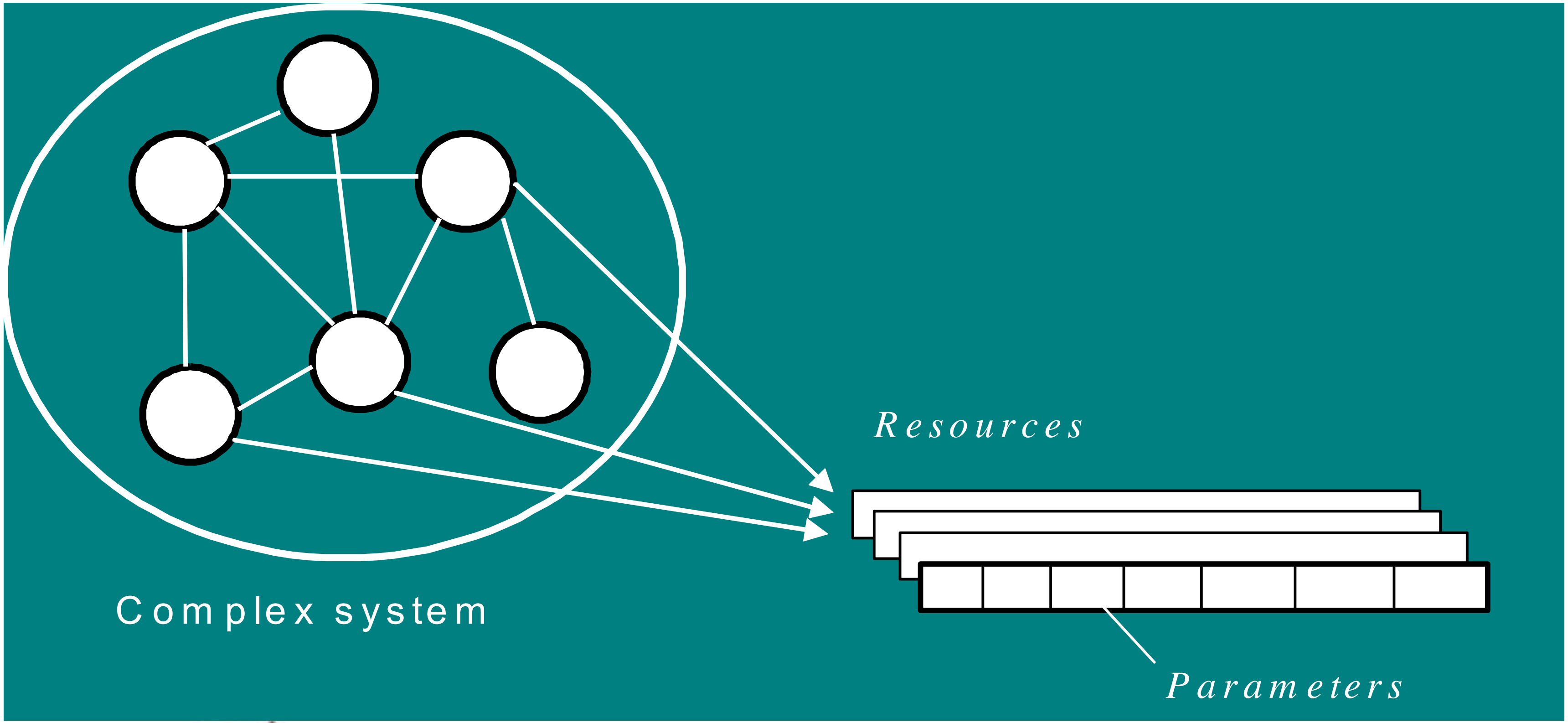
Cockpit CI

RAO: resources (objects)

Complex discrete system (CDS) = set of interacting resources

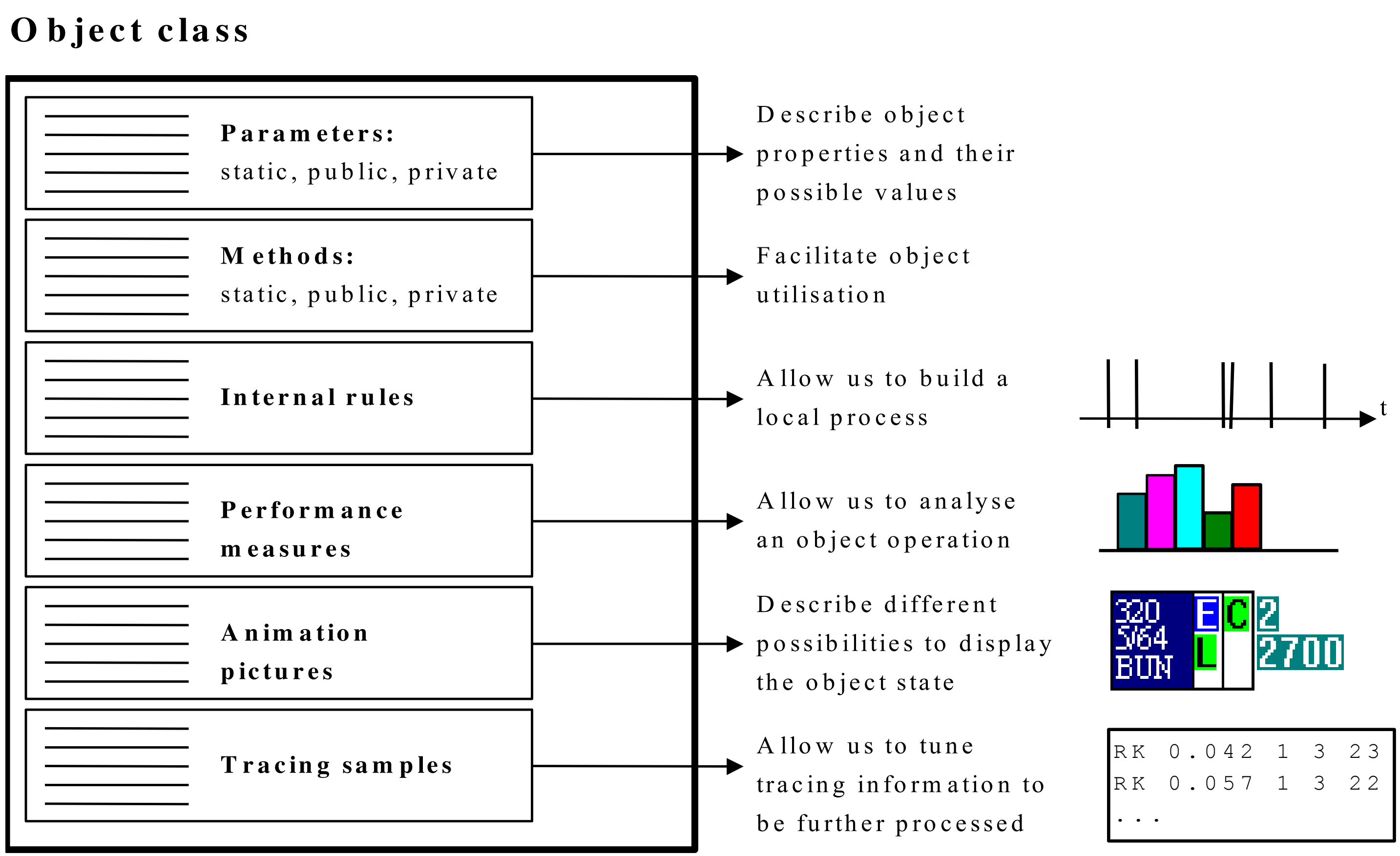
1. Permanents
2. Temporaries

Characterized by a set of *parameters*



Cockpit CI

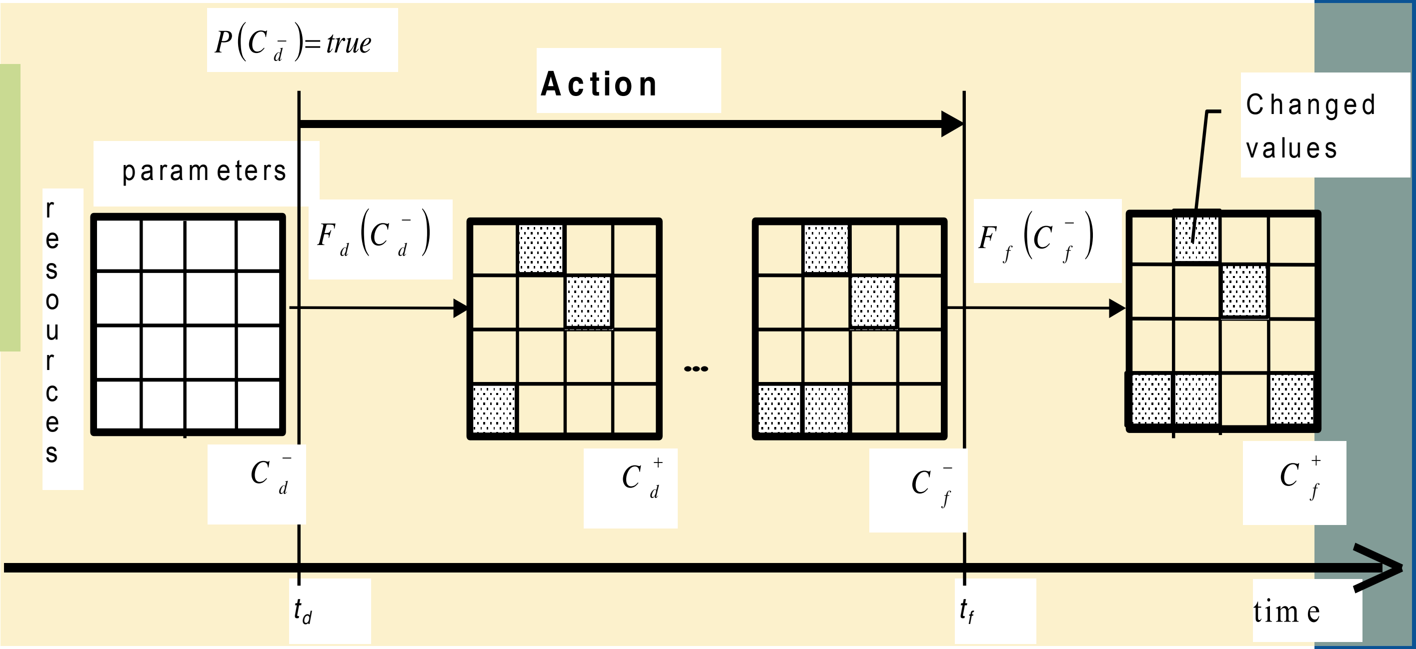
RAO: Object class



Cockpit CI

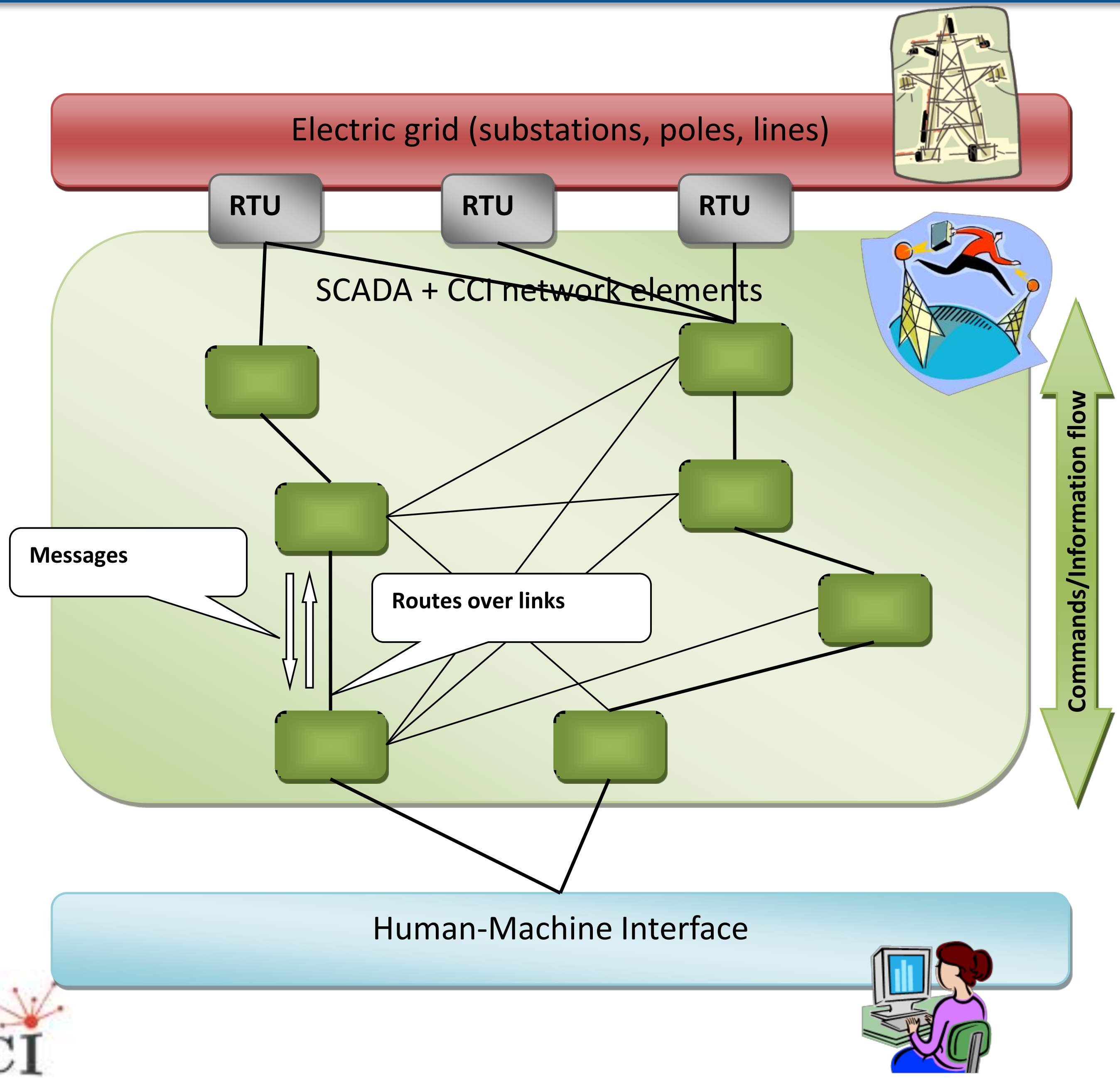
- Limited by two events which change the system state
  - Beginning
  - End
- Characterized by :
  - a precondition
  - the rules of system state change at the beginning and at the end
  - a duration

If ***condition*** then
- ***event of beginning***
- ***wait ΔT***
- ***event of end***



Cockpit CI

CCI/SCADA modeling under cyber attack: Messages and routes



Cockpit CI

CCI/SCADA modeling under cyber attack: elements states related to cyber attacks

Element's behaviour with respect to cyber security can be described by a three state rating of the targeted elements i.e.:

Up: **the functionalities of a service provided by an element are ensured normally.**

Degraded: the service provided by an element still remains available but some functionality is not correctly ensured (timeliness degradation, message de-routing, etc…)

Down: **the service provided by an element is unavailable (for example the element is not reachable or operational).**

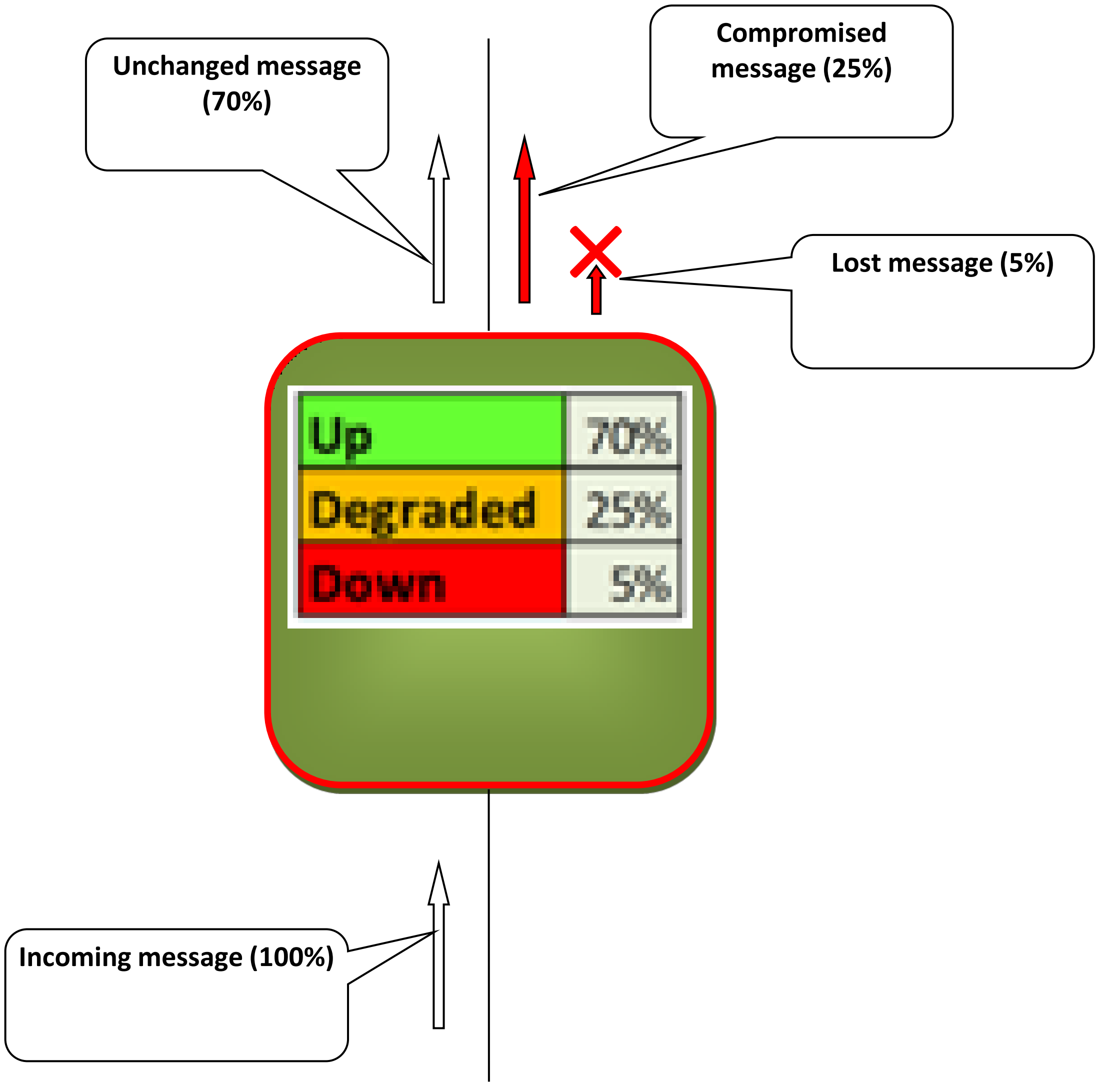
Service delivered by: node 1

State: *Likelihood of Service Availability*

Up	70%
Degraded	25%
Down	5%

Cockpit CI

CCI/SCADA modeling under cyber attack: Compromised element behavior



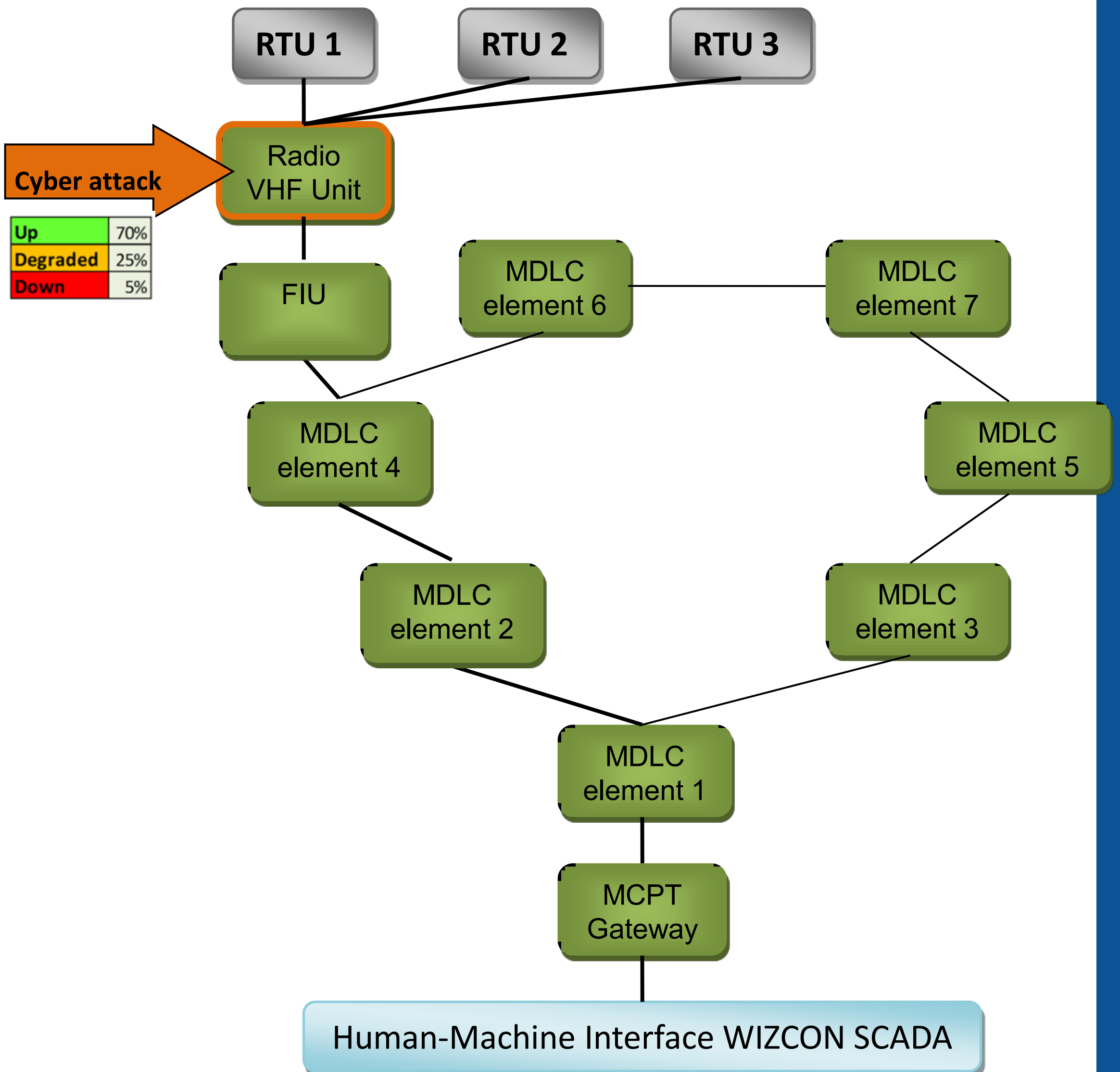
CCI/SCADA modeling under cyber attack: altered elements behavior

The attack logic:

If "Degraded" state ranking of Radio VHF Unit (Base station) is greater than 0.5 then the element behavior is compromised.

Altered behavior:

If "Degraded" >= 0.5 then the element delays messages by two minutes

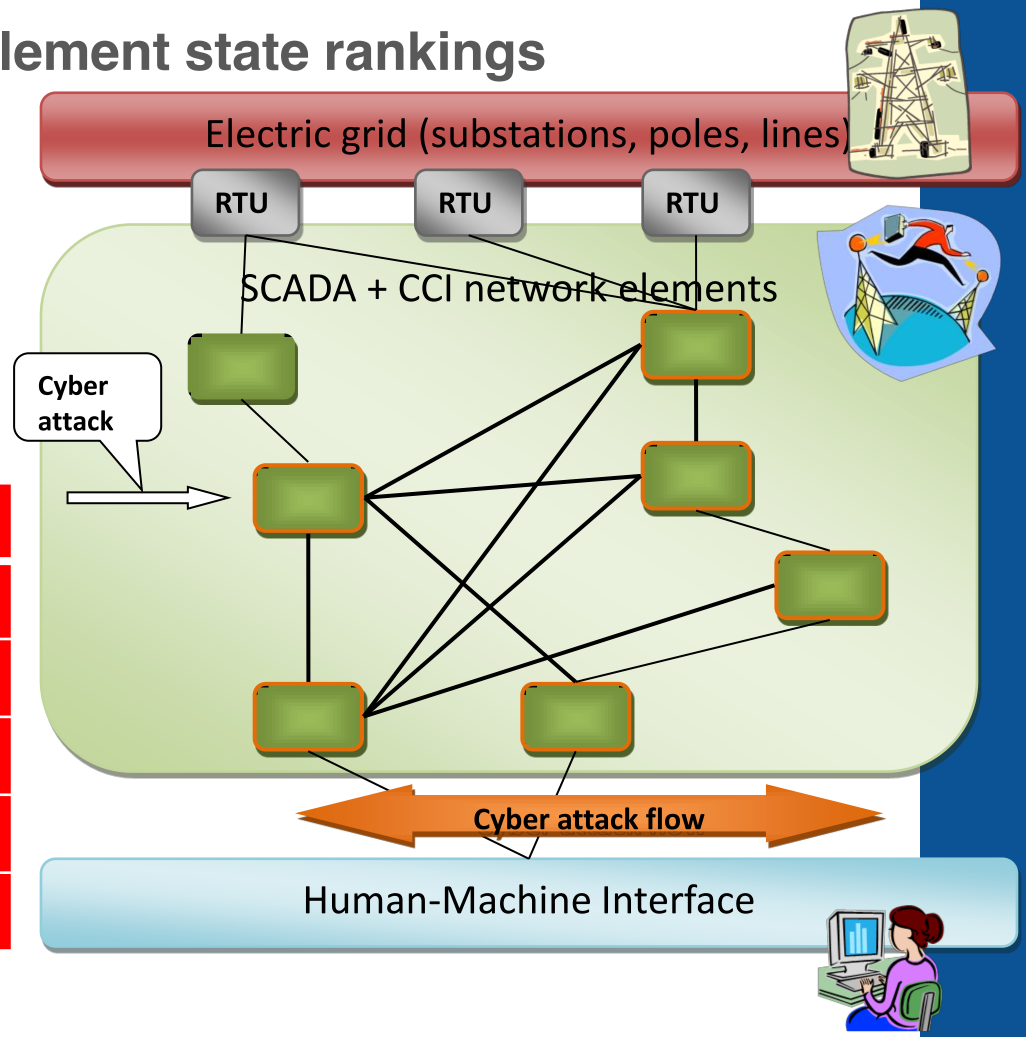


Cockpit CI

CCI/SCADA modeling under cyber attack: Cyber attack scenario

Cyber attack: a time series of element state rankings

Time	Element	Up	Degraded	Down
1	29 (GW prime)	0.5	0.3	0.2
2	1 (FIU)	0.7	0.3	0.0
3	0 (FIU)	0.2	0.8	0.0
4	4 (RTU 1)	0.0	0.0	1.0
5	29 (GW prime)	1.0	0.0	0.0



Cockpit CI

The QoS under cyber attack simulation model

Consists of:

Data base: a set of objects describing system composition and state

1. 223 permanent objects + temporary objects created while simulating)
2. belonging to 20 object types (substation, breaker, line, FIU, gateway, SCADA, message, route, etc.)

Knowledge base: a set of activities describing system behaviour

1. 211 activities of 103 types (toggle breaker state, send a message, repair a line, transmit a message, etc.)

Animation description to illustrate system state

1. 5 main screens

Quality of service indicators and specific technical indicators definition

1. Tn, SAIDI, SAIFI, CAIDI
2. About 1000 specific technical indicators for different elements of the system

Cockpit CI

ECI elements and structure modeling

Object types of the model:

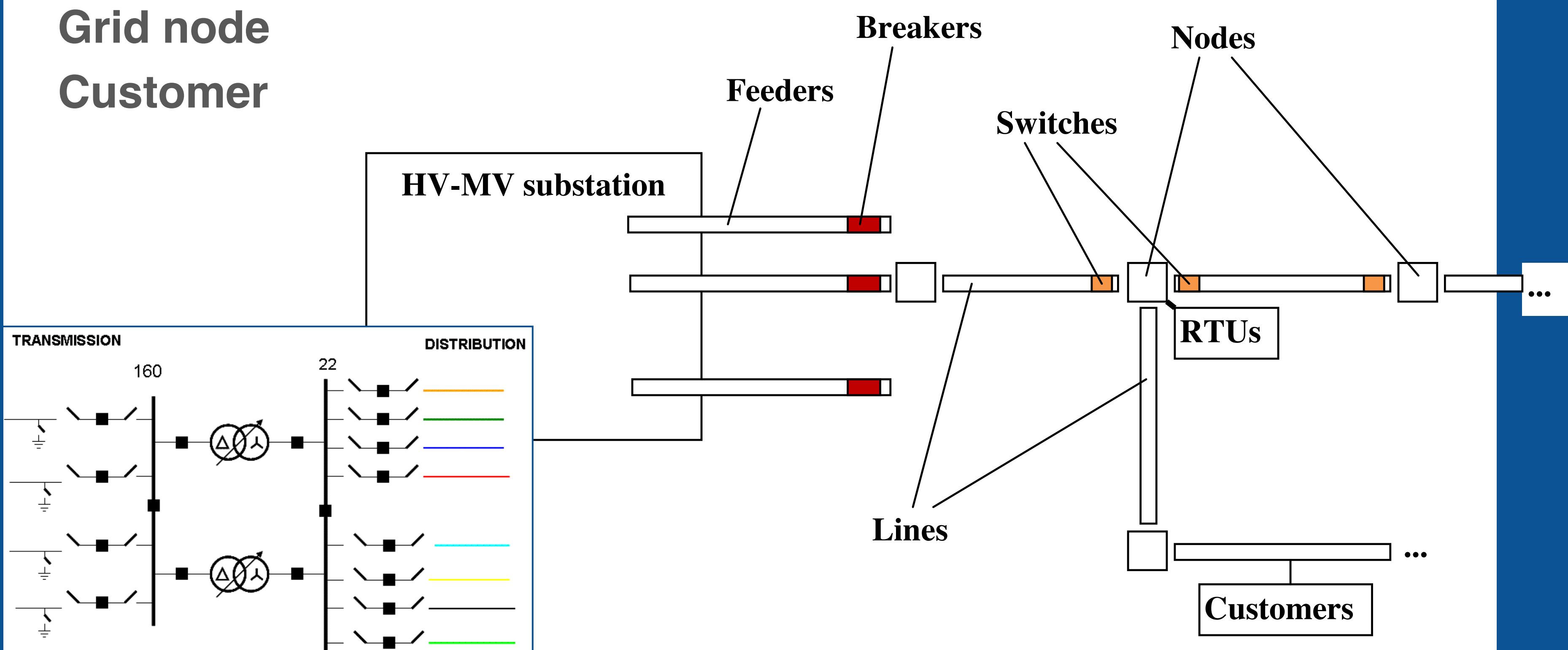
HV_MV substation with Telco room

Feeder

Line

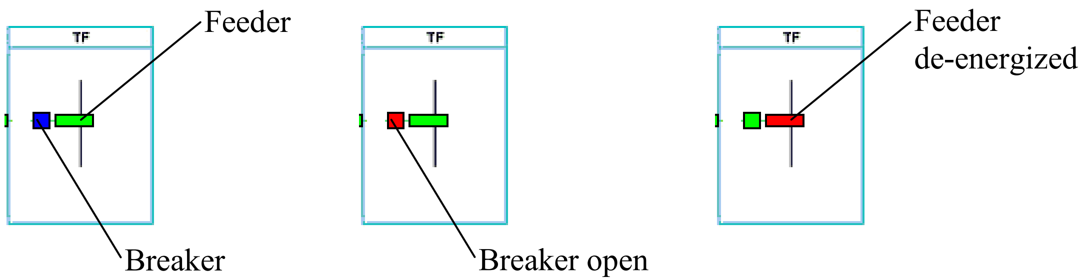
Grid node

Customer

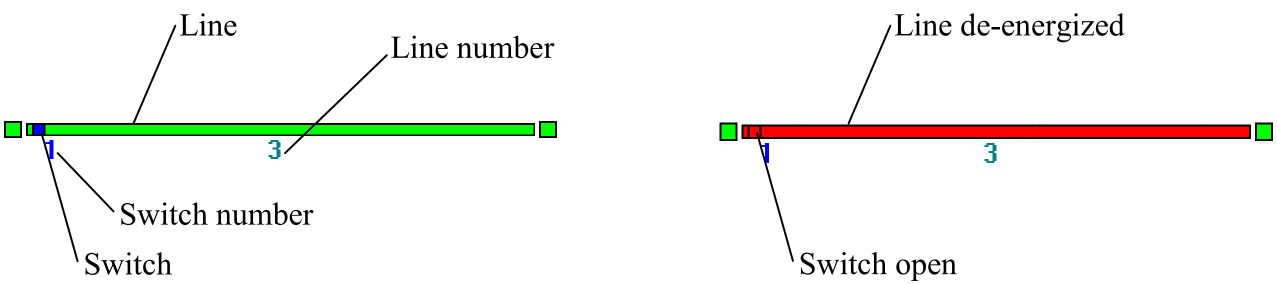


Animation of the objects state and user interaction with the model 1

Feeder + breaker



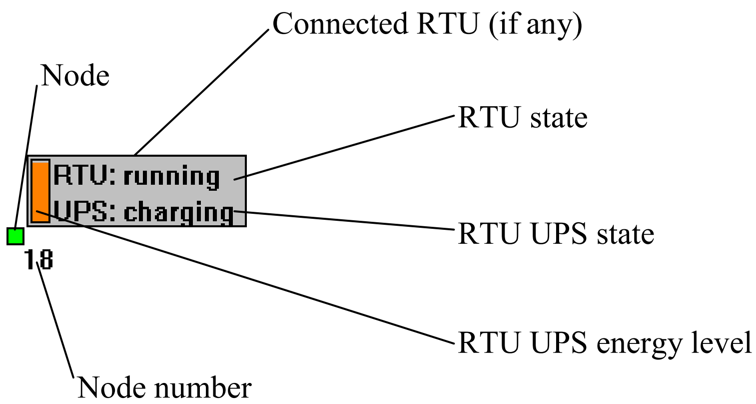
- Transmission line with switch

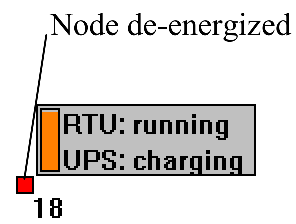


Cockpit CI

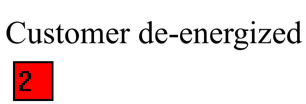
Animation of the objects state and user interaction with the model (2)

Grid node with an RTU



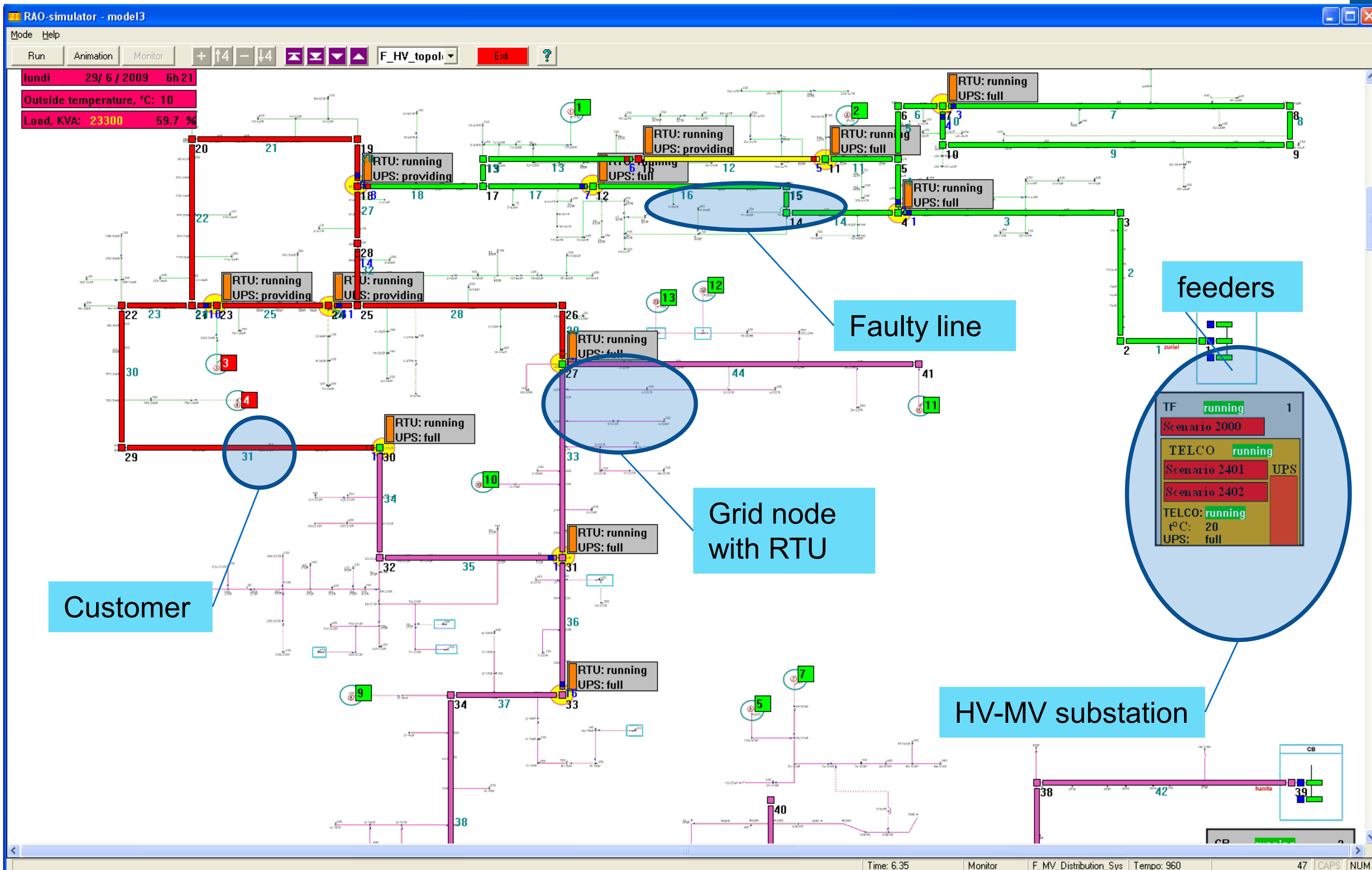


- Customer



Cockpit CI

ECI distribution greed (reference FISR scenario)



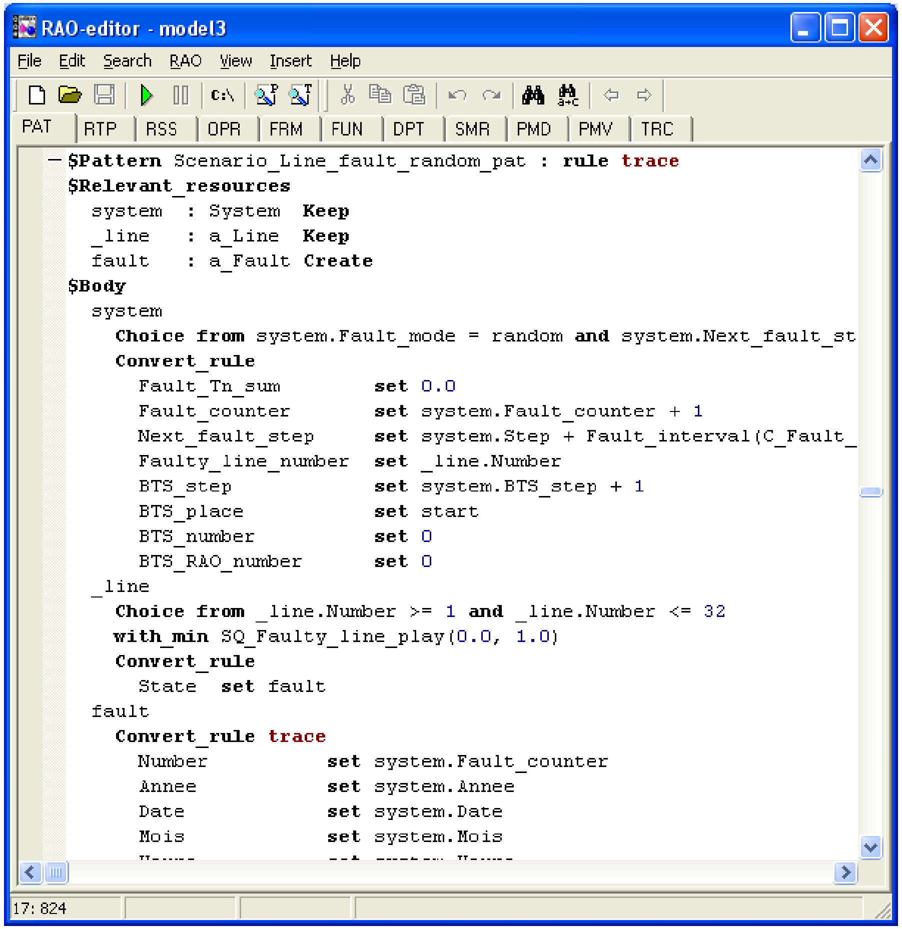
Faults (short circuits) simulation

Three ways to initiate a fault:

Manually by mouse click on a line

Randomly with faulty line number and time interval randomly generated with given distributions

Programmed scenario with time of arrival and faulty line number defined by user at the beginning of simulation



Cockpit CI

Fault localization process

Step1

1. open switch 435R
2. close breaker on Zuriel feeder

Step 2

1. open switch 641B/R
2. close switch 435R

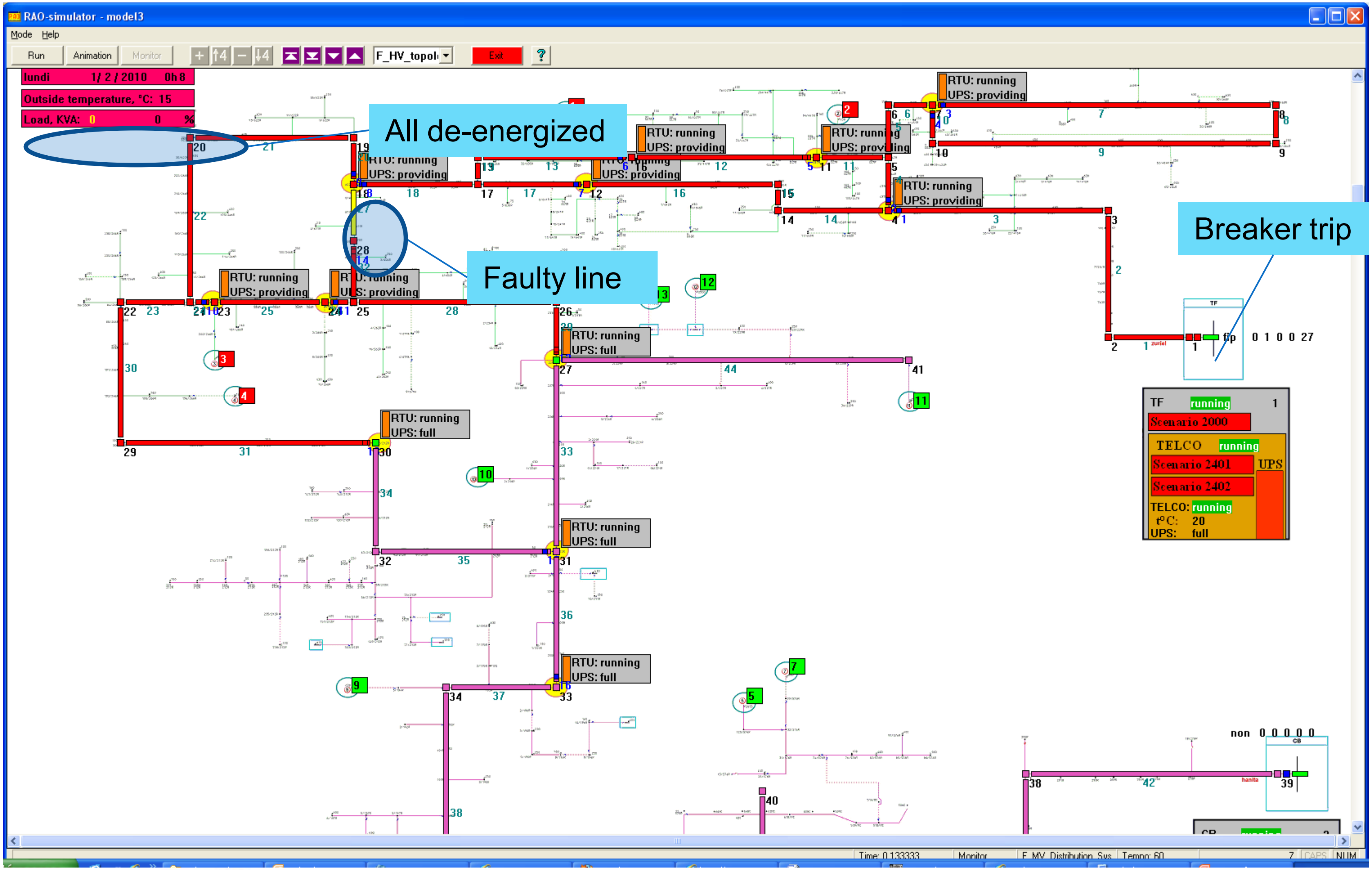
Step 3

1. open switch 622R:A
2. open switch 48/635R
3. close switch 641B/R

- Step 4
  - close switch 48/635R
- Step 5
  - open switch 622R:B
  - close switch 622R:A
- Step 6
  - open switch 78/266R
  - close switch 622R:B

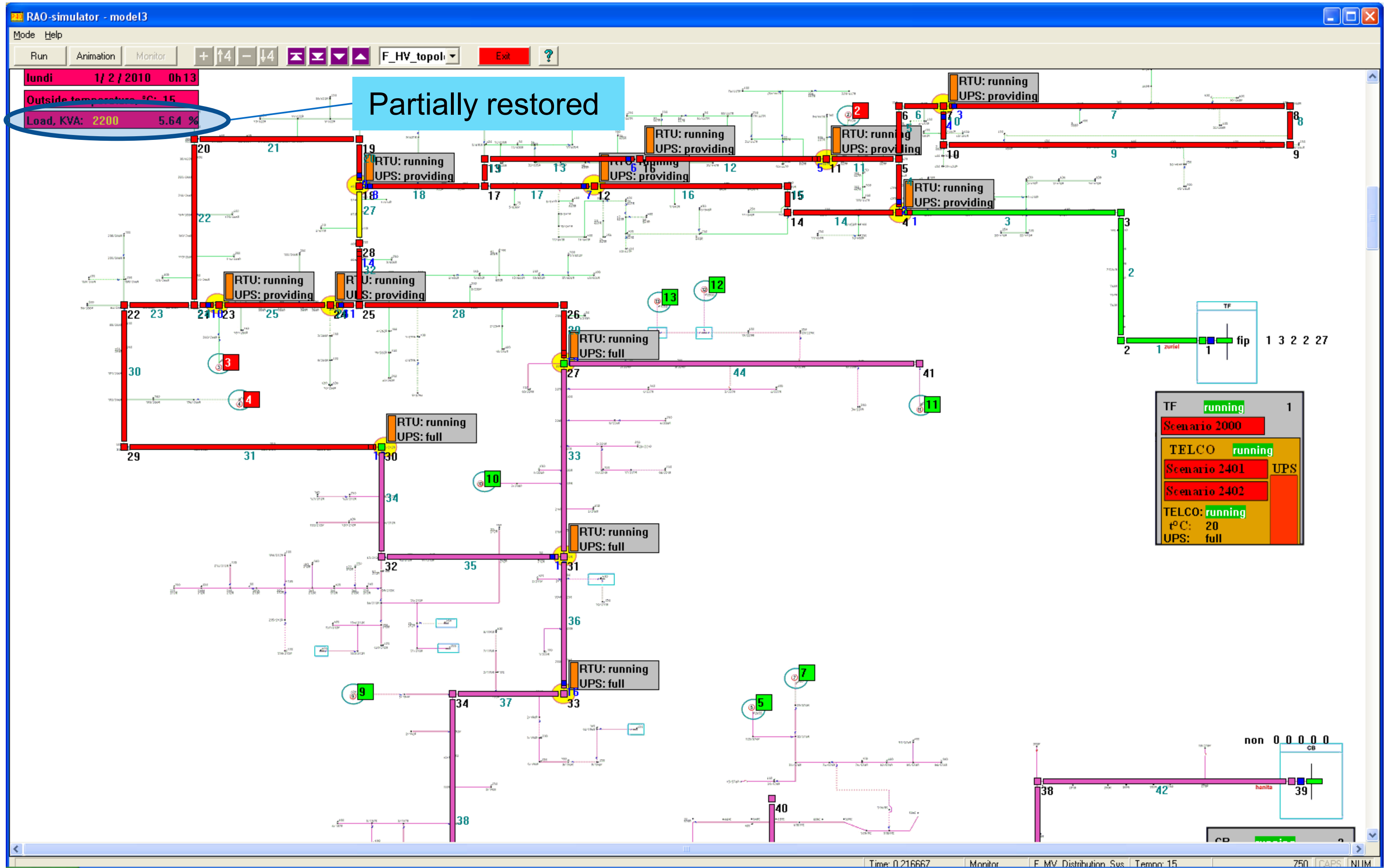
Cockpit CI

Manual fault simulation on line 27 (5th segment)



Cockpit CI

Fault localization, step 1



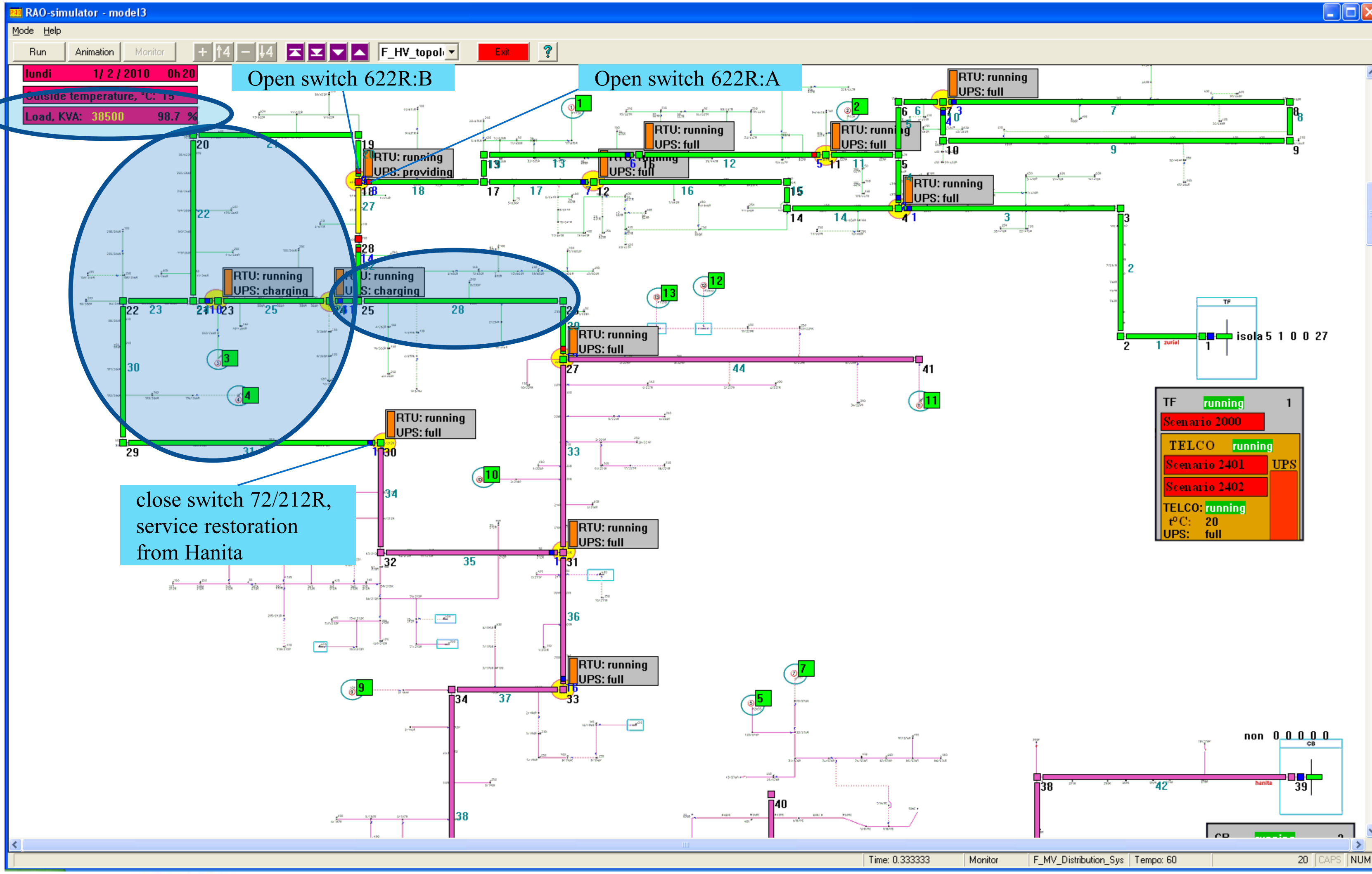
Cockpit CI

Fault isolation process

Faulty segment number	Isolation procedure
1	1. close switch 72/212R
2	1. open switch 435R 2. close breaker on Zuriel feeder 3. close switch 72/212R
3	1. open switch 641B/R 2. close switch 5/447R 3. close breaker on Zuriel feeder 4. close switch 72/212R
4	1. open switch 48/635R 2. close switch 622R:A 3. close breaker on Zuriel feeder
5	1. open switch 622R:B 2. open switch 622R:A 3. close breaker on Zuriel feeder 4. close switch 72/212R
6	1. open switch 622R:B 2. open switch 78/266R 3. close breaker on Zuriel feeder 4. close switch 609R (the switch is only manually controlled)
7	Nothing to do, the segment is already isolated after localization

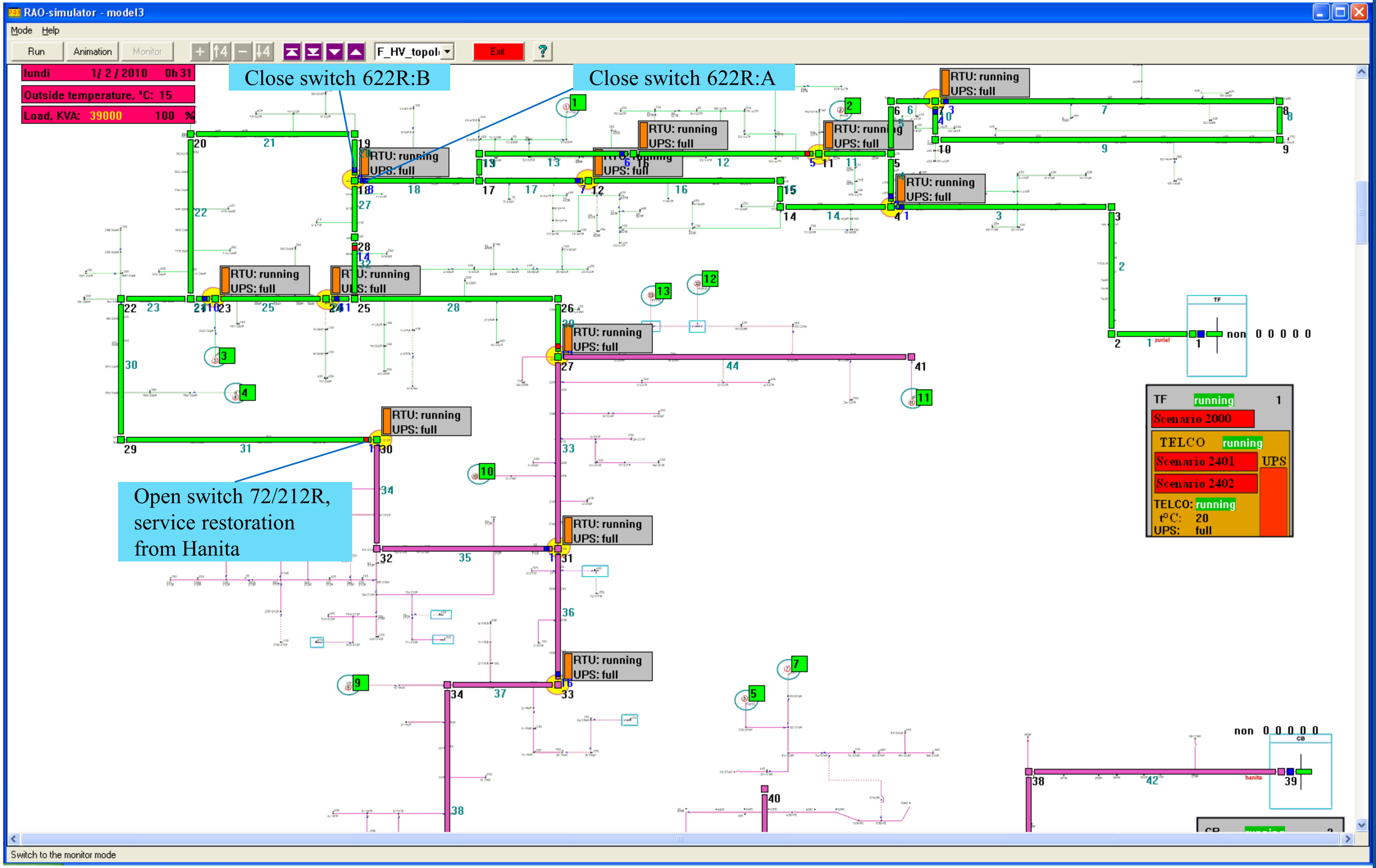
Cockpit CI

Fault isolation for 5th segment



Cockpit CI

Initial configuration restoration



Cockpit CI

SCADA simulation

The fault localization and isolation processes are modeled step by step by giving explicitly all the actions to be done

Each action is represented by an object of type a_FIP_step with the following parameters:

1. Substation number
2. Feeder number
3. Process (localization, isolation)
4. Step number
5. Sub step number
6. Time delay if any
7. ECI element to act on (breaker or switch)
8. Element number
9. Action (open or close)

Cockpit CI

SCADA simulation:
Fault localization process

Step 3

1. open switch 622R:A
2. open switch 48/635R
3. close switch 641B/R

1	1	localisation	3	1	0.0	switch	8	open	{622R:A}
1	1	localisation	3	2	0.0	switch	6	open	{48/635R}
1	1	localisation	3	3	0.0	switch	7	close	{641B/R}

Cockpit CI

SCADA simulation: Fault isolation process

Faulty segment number	Isolation procedure
5	1. open switch 622R:B 2. open switch 622R:A 3. close breaker on Zuriel feeder 4. close switch 72/212R

```
1  1    isolation  5  1   0.0  switch   9  open  {622R:B}
1  1    isolation  5  2   0.0  switch   8  open  {622R:A}
1  1    isolation  5  3   0.0  breaker  *   close {Zuriel}
1  1    isolation  5  4   0.0  switch  13  close {72/212R}
```

Cockpit CI

SCADA simulation:
Initial configuration restoration

Procedure is automatically generated on the basis of normal switch states

Normal switch states are defined by table (for Zuriel feeder):

Switch	Switch number	Normal state	Switch	Switch number	Normal state
435R	1	closed	622/R:A	8	closed
435R	2	closed	622/R:B	9	closed
464R	3	closed	78/266R	10	closed
464R	4	closed	2/266R	11	closed
5/447R	5	open	229R	12	open
48/635R	6	closed	72/212R	13	open
641B/R	7	closed	609R	14	open

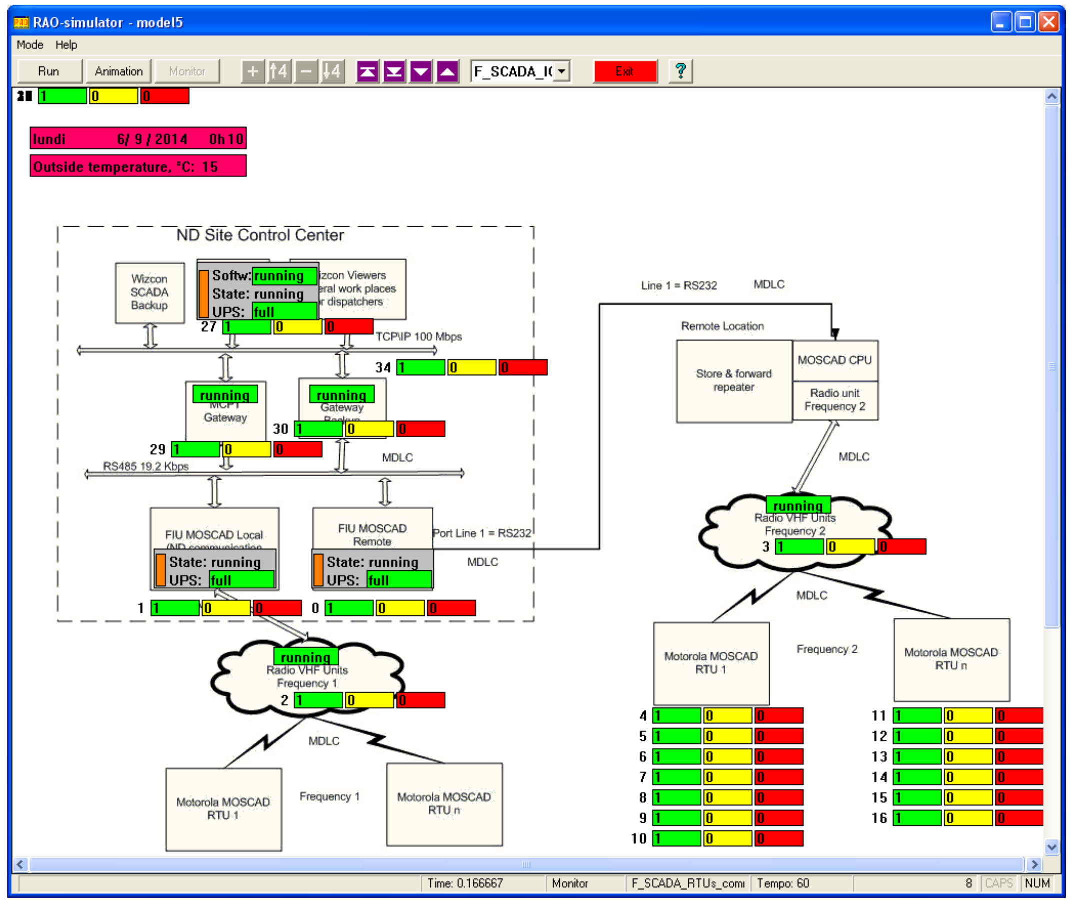
Cockpit CI

CCI under cyber attack simulation

Communication infrastructure delivers SCADA commands to RTUs

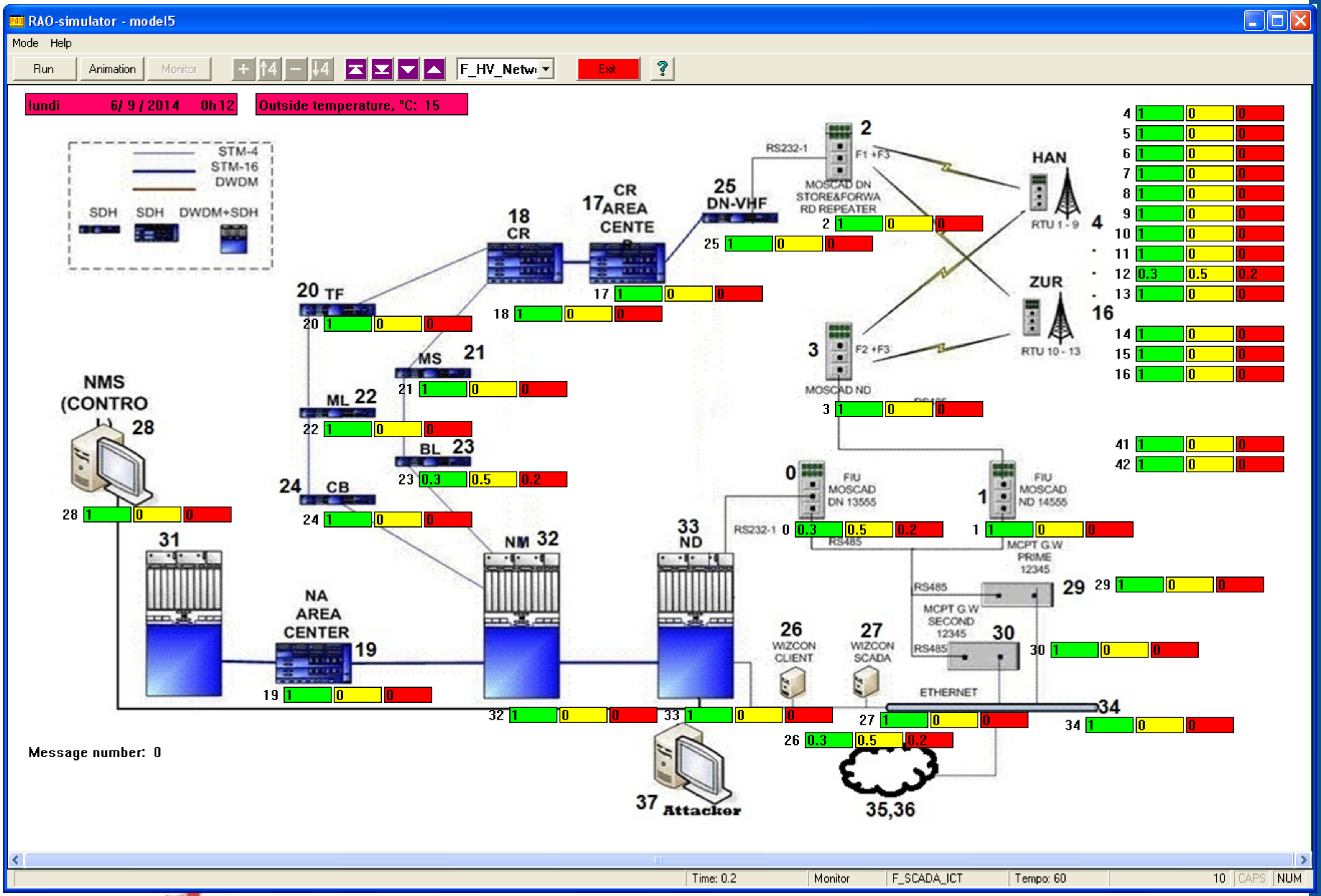
Command objects have the following main parameters:

1. Number
2. Creation time
3. Execution order
4. Substation number
5. Feeder number
6. Element (breaker, switch)
7. Element number
8. Action
9. State (issued, delivered)
10. Execution time



Cockpit CI

CCI/SCADA elements with state rankings animation screen



Cockpit CI

Quality of service indicators

T_n - equivalent de-energized time for fault n

$$T_n = \sum(KVA*Duration)/Installed\ KVA$$

SAIDI- System Average Interruption Duration

$$SAIDI = \sum(unsupplied\ KVA*tn)/Installed\ KVA$$

SAIFI- System Average frequency Interruption

$$SAIFI = \sum(unsupplied\ KVA)/\ Installed\ KVA$$

CAIDI- Customer Average Interruption Duration

$$CAIDI = SAIDI/SAIFI$$

CAIDI index is the most important index for power utilities. Annually reducing this value indicates an improvement of the overall distribution system performance and reliability.

Cockpit CI

Quality of service indicators for fault on segment 5

Totally the process lasts for 14 minutes:

Five minutes for automatic reclosing cycle and for data gathering from costumers before starting fault location process

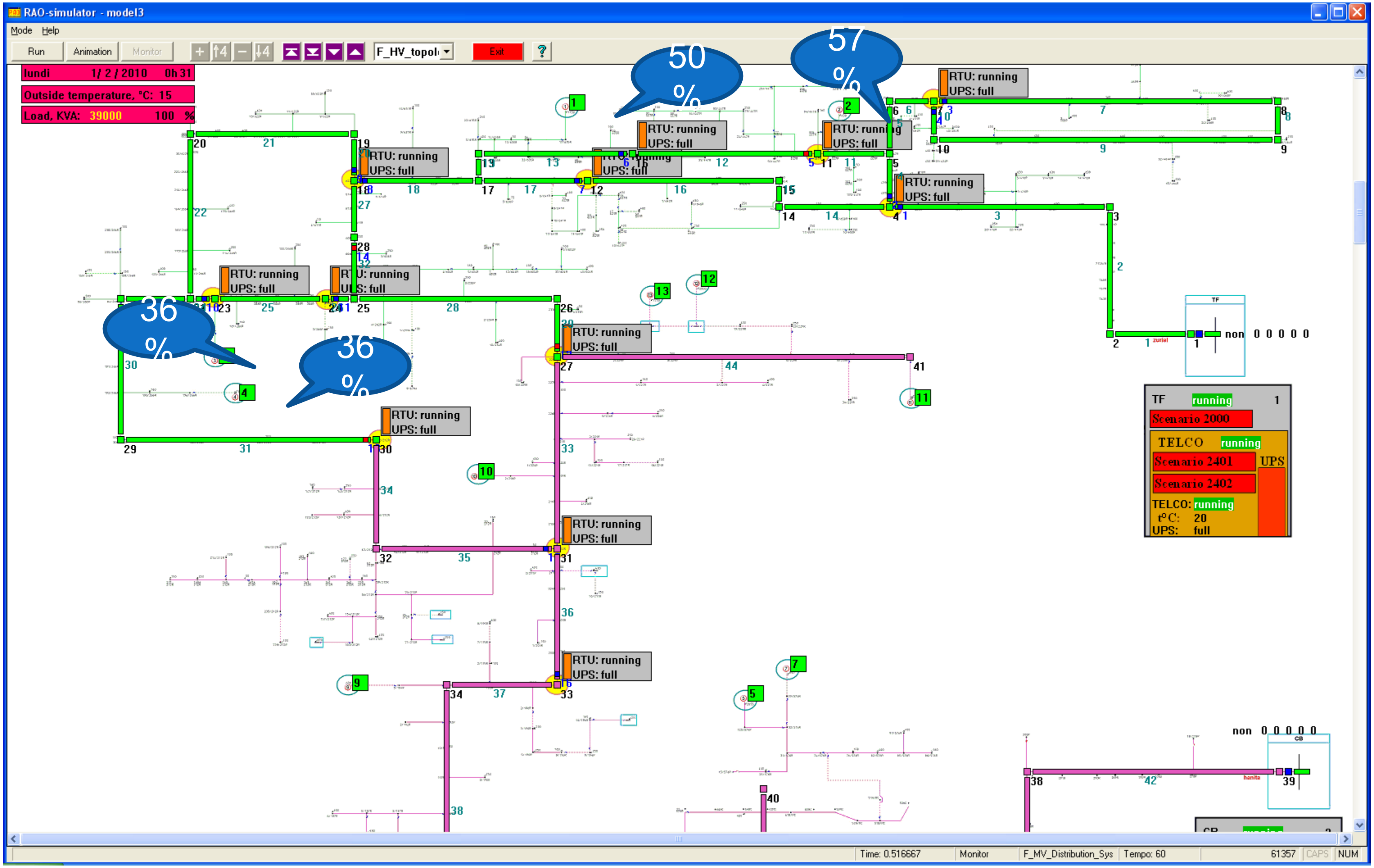
Four minutes for four additional steps of localization process

Five minutes for reparation

Indicator	Value
Tn	7.26 min
SAIDI - System Average Interruption Duration	7.26 min
SAIFI - System Average Frequency Interruption	1
CAIDI - Customer Average Interruption Duration	7.26 min

Cockpit CI

Quality of service indicators: detailed



Cockpit CI

Reference scenario on different segments
no cyber attack

Indicator	Segment number						
	1	2	3	4	5	6	7
Duration, min	10	11	12	13	14	52	16
Tn, min	5.28	8.19	6.9	7.1	7.26	20.87	8.58
Customer 1	54.5%	45.5%	0%	46.2%	50%	86.5%	56.3%
Customer 2	54.5%	0%	50%	53.8%	57.1%	88.5%	62.5%
Customer 3	54.5%	45.5%	41.7%	38.5%	35.7%	9.6%	0%
Customer 4	54.5%	45.5%	41.7%	38.5%	35.7%	0%	37.5%
Commands sent	6	10	16	12	17	19	13
Delivery time, min	0	0	0	0	0	1.95	0

Cockpit CI

Reference scenario on different segments
cyber attack on Radio VHF Unit 1

Cyber attack scenario:

Time	Element	Up	Degraded	Down
0	2 (Radio VHF Unit 1)	0.0	1.0	0.0

Indicator	Segment number						
	1	2	3	4	5	6	7
Duration, min	16	18	20	16	20	59	20
Tn, min	9.28	14.03	12.52	10.13	10.64	25.9	11.77
Customer 1	43.75%	38.9%	0%	31.3%	45%	78%	45%
Customer 2	43.75%	0%	45%	43.8%	55%	81.4%	55%
Customer 3	43.75%	38.9%	35%	31.3%	35%	11.9%	0%
Customer 4	43.75%	38.9%	35%	31.3%	35%	3.4%	35%
Commands sent	6	10	16	12	17	19	13
Delivery time, min	1.333	1.6	1.25	0.67	0.71	2.89	0.92

Cockpit CI

Reference scenario on different segments
cyber attack on Radio VHF Unit 2

Cyber attack scenario:

Time	Element	Up	Degraded	Down
0	3 (Radio VHF Unit 2)	0.0	1.0	0.0

Indicator	Segment number						
	1	2	3	4	5	6	7
Duration, min	10	11	16	20	22	61	20
Tn, min	5.28	8.19	8.18	10.59	11.03	25.28	10.48
Customer 1	54.5%	45.5%	0%	45%	50%	82%	55%
Customer 2	54.5%	0%	62.5%	60%	63.6%	86.9%	70%
Customer 3	54.5%	45.5%	43.8%	35%	31.8%	11.5%	0%
Customer 4	54.5%	45.5%	43.8%	35%	31.8%	0%	25%
Commands sent	6	10	16	12	17	19	13
Delivery time, min	0	0	0.5	1	1.06	3	0.92

Cockpit CI

Reference scenario on different segments
cyber attack on Radio VHF Units 1 and 2

Cyber attack scenario:

Time	Element	Up	Degraded	Down
0	2 (Radio VHF Unit 1)	0.0	1.0	0.0
0	3 (Radio VHF Unit 2)	0.0	1.0	0.0

Indicator	Segment number						
	1	2	3	4	5	6	7
Duration, min	16	18	20	22	24	63	24
Tn, min	9.28	14.03	12.52	13.04	13.47	27.73	13.28
Customer 1	43.75%	38.9%	0%	40.9%	45.8%	79.4%	54.2%
Customer 2	43.75%	0%	45%	50%	54.2%	82.5%	62.5%
Customer 3	43.75%	38.9%	35%	31.8%	29.2%	11.1%	0%
Customer 4	43.75%	38.9%	35%	31.8%	29.2%	0%	29.2%
Commands sent	6	10	16	12	17	19	13
Delivery time, min	1.333	1.6	1.75	1.67	1.76	3.74	1.85

Cockpit CI

Reference scenario on different segments
"sophisticated" cyber attack on Radio VHF Units 1 and 2

Cyber attack scenario:

Time	Element	Up	Degraded	Down
6	2 (Radio VHF Unit 1)	0.0	1.0	0.0
8	3 (Radio VHF Unit 2)	0.0	1.0	0.0
10	2 (Radio VHF Unit 1)	1.0	0.0	0.0
12	2 (Radio VHF Unit 1)	0.0	1.0	0.0

Indicator	Segment number						
	1	2	3	4	5	6	7
Duration, min	10	17	17	21	23	62	23
Tn, min	5.28	12.97	9.47	11.98	12.42	26.68	12.22
Customer 1	54.5%	41.2%	0%	42.9%	47.8%	80.6%	56.5%
Customer 2	54.5%	0%	52.9%	52.4%	56.5%	83.9%	65.2%
Customer 3	54.5%	41.2%	41.2%	33.3%	30.4%	11.3%	0%
Customer 4	54.5%	58.8%	41.2%	33.3%	30.4%	0%	30.4%
Commands sent	6	10	16	12	17	19	13
Delivery time, min	0	1.4	1.25	1.5	1.65	3.63	1.69

Reference scenario on different segments
"sophisticated" cyber attack on Radio VHF Units 1 and 2

Cyber attack scenario:

Time	Element	Up	Degraded	Down
6	2 (Radio VHF Unit 1)	0.0	1.0	0.0
8	3 (Radio VHF Unit 2)	0.0	1.0	0.0
10	2 (Radio VHF Unit 1)	1.0	0.0	0.0
12	2 (Radio VHF Unit 1)	0.0	0.0	1.0

Indicator	Segment number						
	1	2	3	4	5	6	7
Duration, min	10	56	59	21	65	81	67
Tn, min	5.28	21.05	12.5	11.98	26.12	32.05	26.63
Customer 1	54.5%	82.1%	22%	42.9%	81.5%	81.5%	85.1%
Customer 2	54.5%	37.5%	86.4%	52.4%	84.6%	84%	88.1%
Customer 3	54.5%	82.1%	83%	33.3%	15.4%	19.8%	0%
Customer 4	54.5%	82.1%	83%	33.3%	15.4%	11.1%	14.9%
Commands sent	6	10	16	12	17	19	13
Delivery time, min	0	9.7	7.06	1.5	4.12	5.1	5.08

Monte-Carlo simulations, static security state

Cyber state scenario:

Element	Up	Degraded	Down
1 (FIU_MOSCAD_local)	0.4	0.4	0.2
0 (FIU_MOSCAD_remote)	0.6	0.3	0.1

Number of simulations: 50

Indicator: Tn	Segment number						
	1	2	3	4	5	6	7
Tn, min (“true”)	12.50	21.06	23.74	25.78	25.80	36.42	22.46
Tn, min (simulation)	11.18	18.63	21.15	23.05	23.0	33.58	20.54
Confidence interval, α = 0.05	4.97	9.16	8.79	8.10	8.59	8.60	6.25
Confidence interval, %	44.4	49.2	41.6	35.1	37.4	25.6	30.4
Difference with true value, %	10.56	11.53	10.90	10.60	10.86	7.78	8.53

Cockpit CI

Monte-Carlo simulations, static security state

Cyber state scenario:

Element	Up	Degraded	Down
1 (FIU_MOSCAD_local)	0.4	0.4	0.2
0 (FIU_MOSCAD_remote)	0.6	0.3	0.1

Number of simulations: 200

Indicator: Tn	Segment number						
	1	2	3	4	5	6	7
Tn, min ("true")	12.50	21.06	23.74	25.78	25.80	36.42	22.46
Tn, min (simulation)	13.76	23.40	25.85	27.65	27.89	38.60	23.91
Confidence interval, α = 0.05	2.95	5.45	5.29	4.96	5.26	5.31	3.76
Confidence interval, %	21.5	23.3	20.4	18.0	18.9	13.8	15.7
Difference with true value, %	10.1	11.3	8.92	7.25	8.10	5.98	6.48

Cockpit CI

Monte-Carlo simulations, static security state

Cyber state scenario:

Element	Up	Degraded	Down
1 (FIU_MOSCAD_local)	0.4	0.4	0.2
0 (FIU_MOSCAD_remote)	0.6	0.3	0.1

Number of simulations: 500

Indicator: Tn	Segment number						
	1	2	3	4	5	6	7
Tn, min (“true”)	12.50	21.06	23.74	25.78	25.80	36.42	22.46
Tn, min (simulation)	12.61	21.08	24.41	26.95	26.84	37.21	23.42
Confidence interval, α = 0.05	1.70	3.15	3.06	2.95	3.09	3.10	2.24
Confidence interval, %	13.5	14.9	12.6	11.0	11.5	8.32	9.56
Difference with true value, %	0.92	0.11	2.84	4.52	4.04	2.18	4.28

Cockpit CI

Conclusion and perspectives

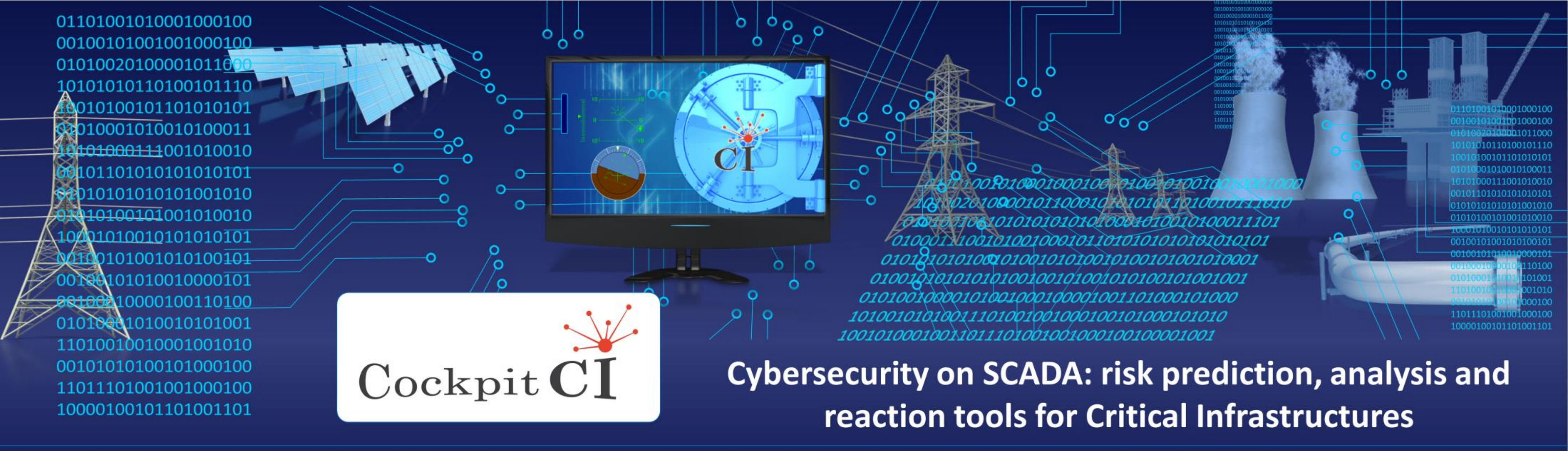
Developed modeling framework and implemented simulation model have proven the feasibility of QoS indicators calculation for such a complex heterogeneous system under cyber attack

The input/output data of the model are clearly identified, so the model can be integrated in the whole CockpitCI tool, making a part of Integrated Risk Predictor

Simulation Monte-Carlo in case of dynamic cyber security state (cyber attack in progress)

On-line model receiving elements state rankings from IDS, IRP, … and calculating Tn for current situation

Cockpit CI



Integrated On-Line Risk Prediction
Mixing together risk alerts and forcing a reaction

4th CockpitCI Workshop (Bucharest 16.09.2014)

Stefano Panzieri

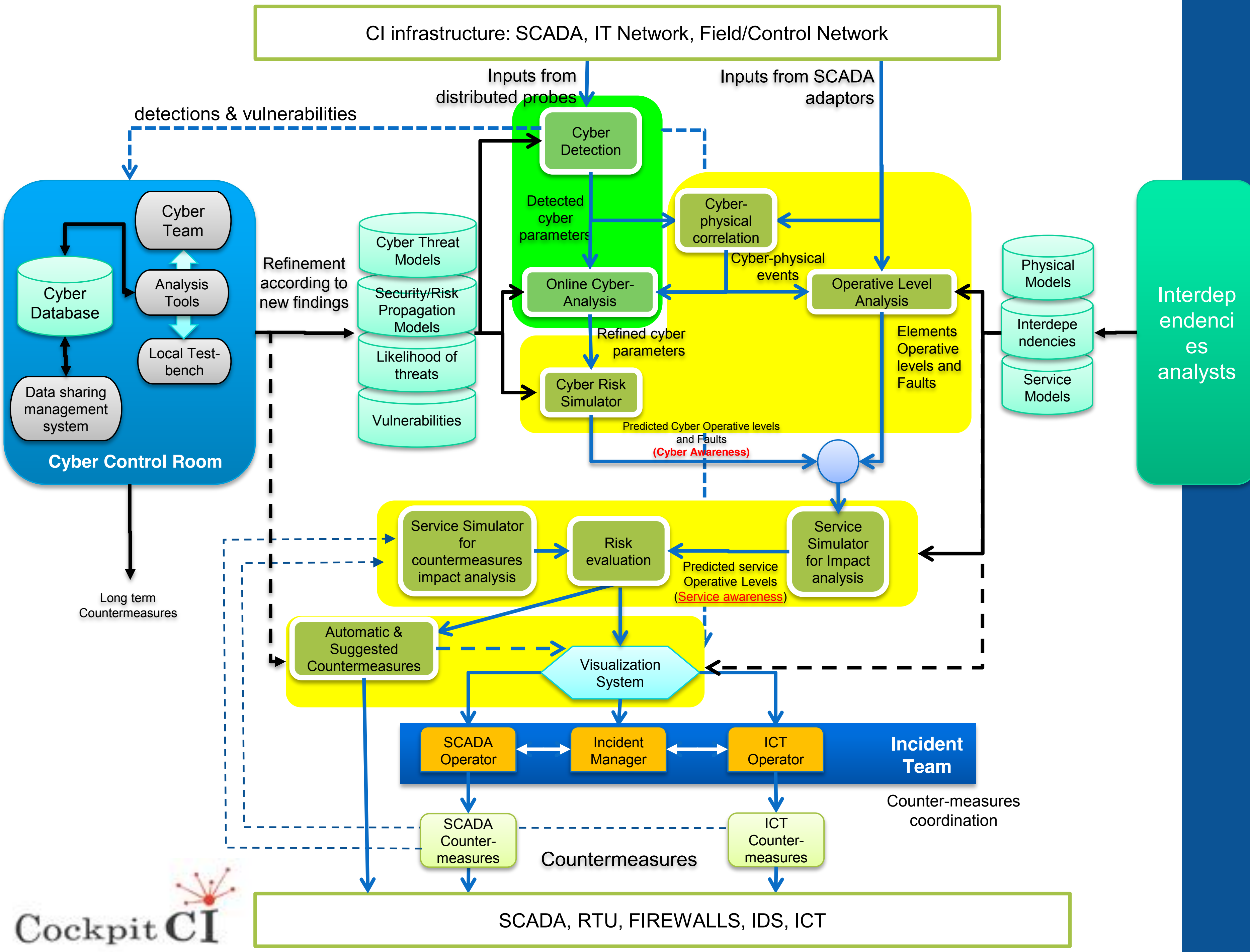
University of Roma TRE

Information Society

CockpitCI Functional Diagram

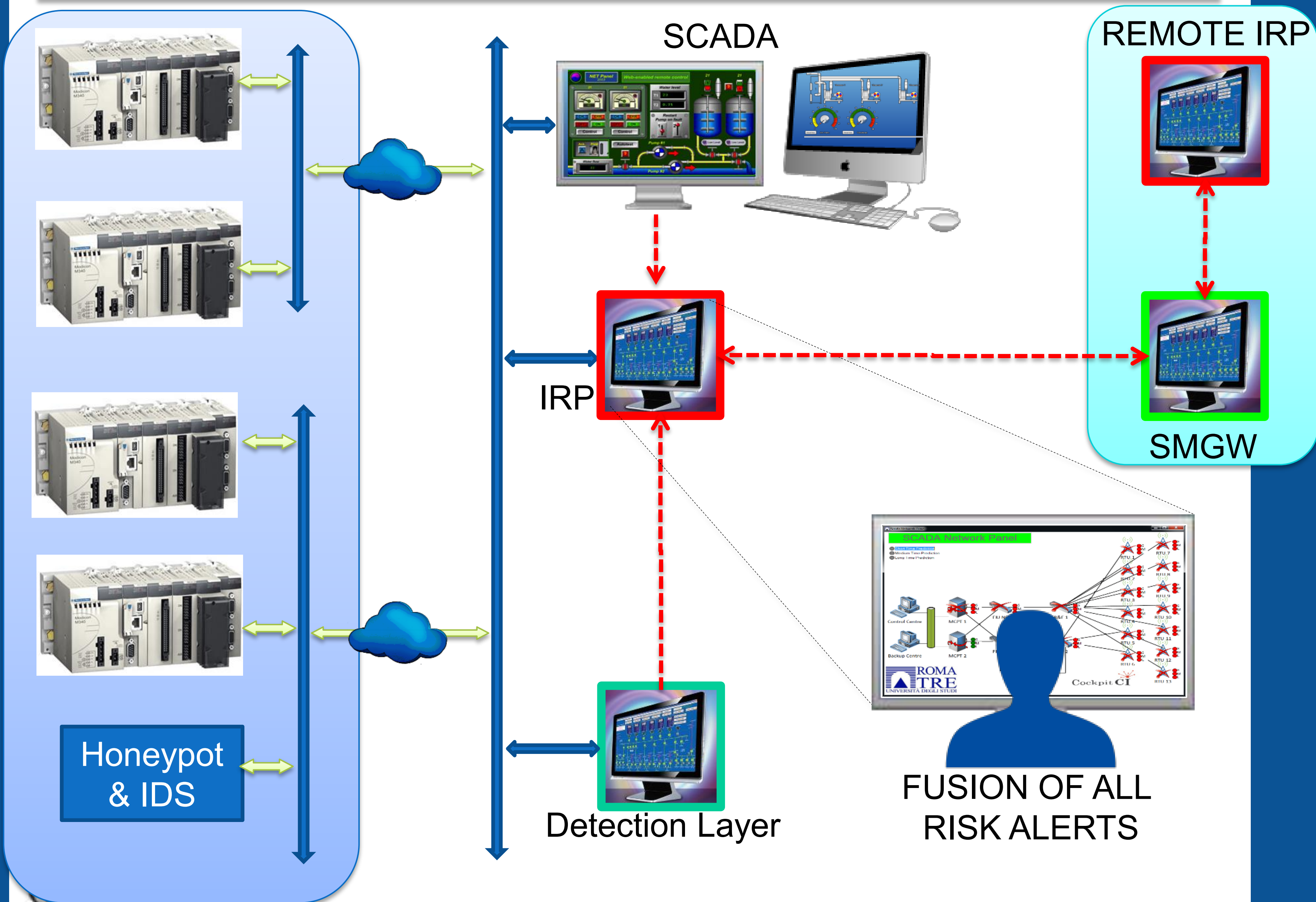
CockpitCI Functional Diagram

Cockpit CI



CI infrastructure: SCADA, IT Network, Field/Control Network
Inputs from distributed probes
Inputs from SCADA adaptors
detections & vulnerabilities
Cyber Detection
Detected cyber parameters
Cyber-physical correlation
Cyber-physical events
Online Cyber-Analysis
Operative Level Analysis
Refined cyber parameters
Elements Operative levels and Faults
Cyber Risk Simulator
Predicted Cyber Operative levels and Faults
(Cyber Awareness)
Cyber Team
Analysis Tools
Local Test-bench
Cyber Database
Data sharing management system
Cyber Control Room
Refinement according to new findings
Cyber Threat Models
Security/Risk Propagation Models
Likelihood of threats
Vulnerabilities
Physical Models
Interdependencies
Service Models
Interdependencies analysts
Long term Countermeasures
Service Simulator for countermeasures impact analysis
Risk evaluation
Service Simulator for Impact analysis
Predicted service Operative Levels (Service awareness)
Automatic & Suggested Countermeasures
Visualization System
SCADA Operator
Incident Manager
ICT Operator
Incident Team
Counter-measures coordination
SCADA Counter-measures
ICT Counter-measures
Countermeasures
SCADA, RTU, FIREWALLS, IDS, ICT
Cockpit CI

IRP & Detection Layer & Secure Mediation GW

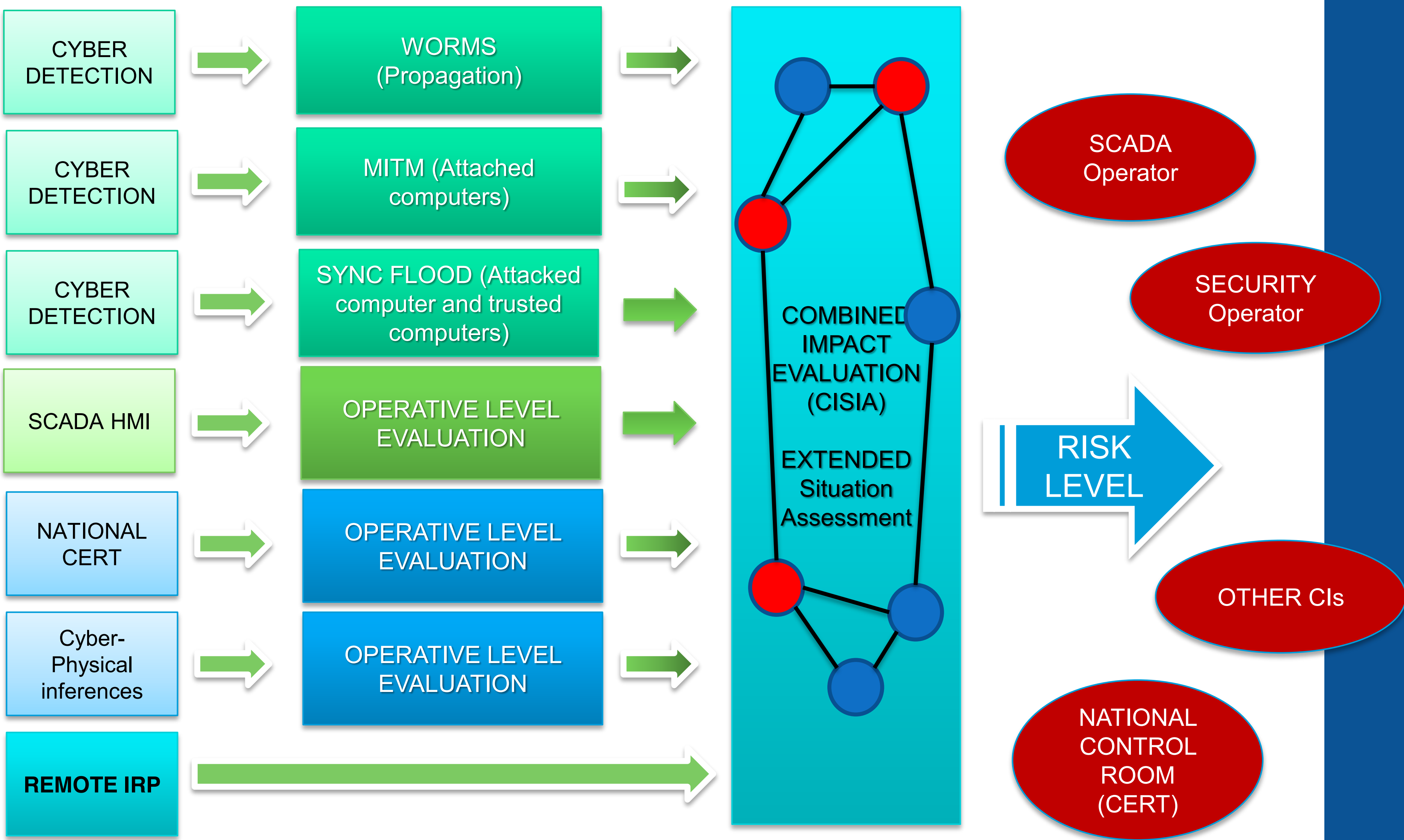


Integrated Risk Predictor

Integrated Risk Predictor

Cockpit CI

FROM HOLISTIC ASSESSMENT TO COMBINED IMPACT EVALUATION

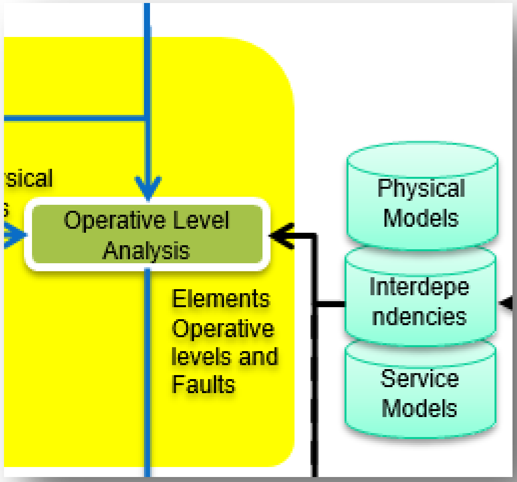


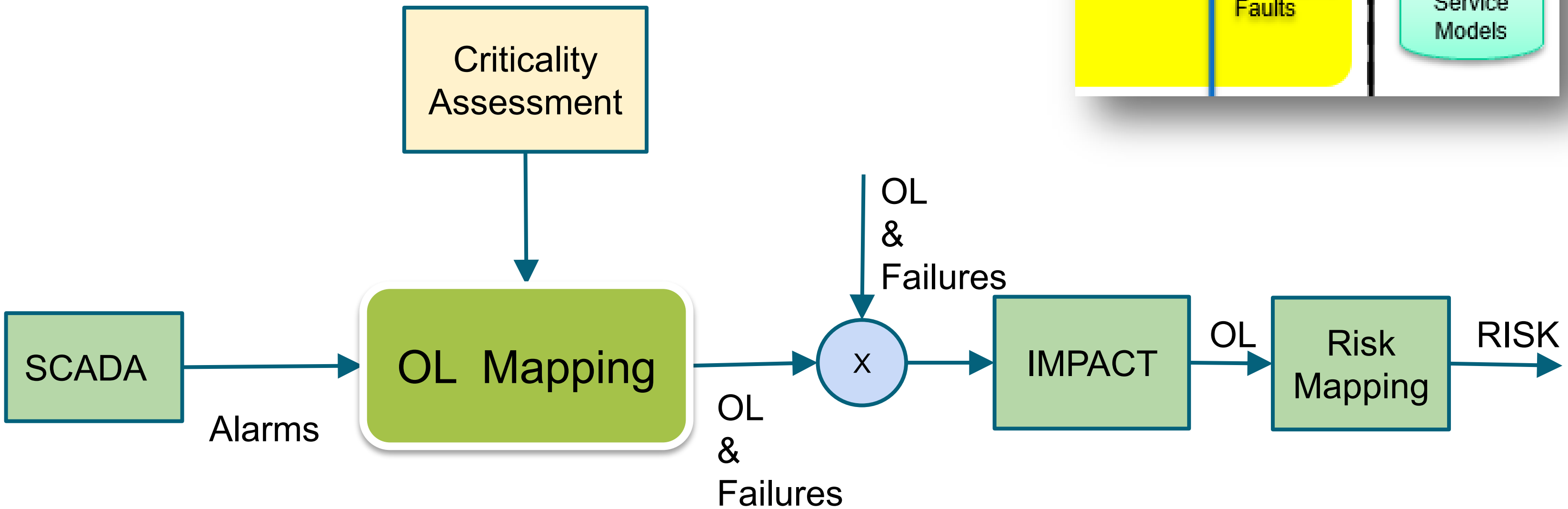
Holistic estimation

Reductionistic decomposition for cascading effects evaluation

Cockpit CI

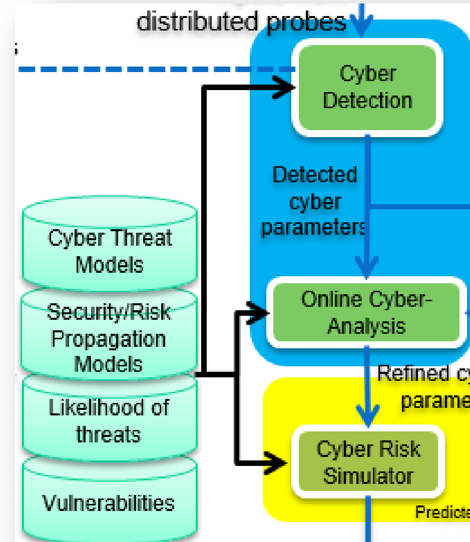
SCADA ALARMS → OPERATIVE LEVELS & FAILURES

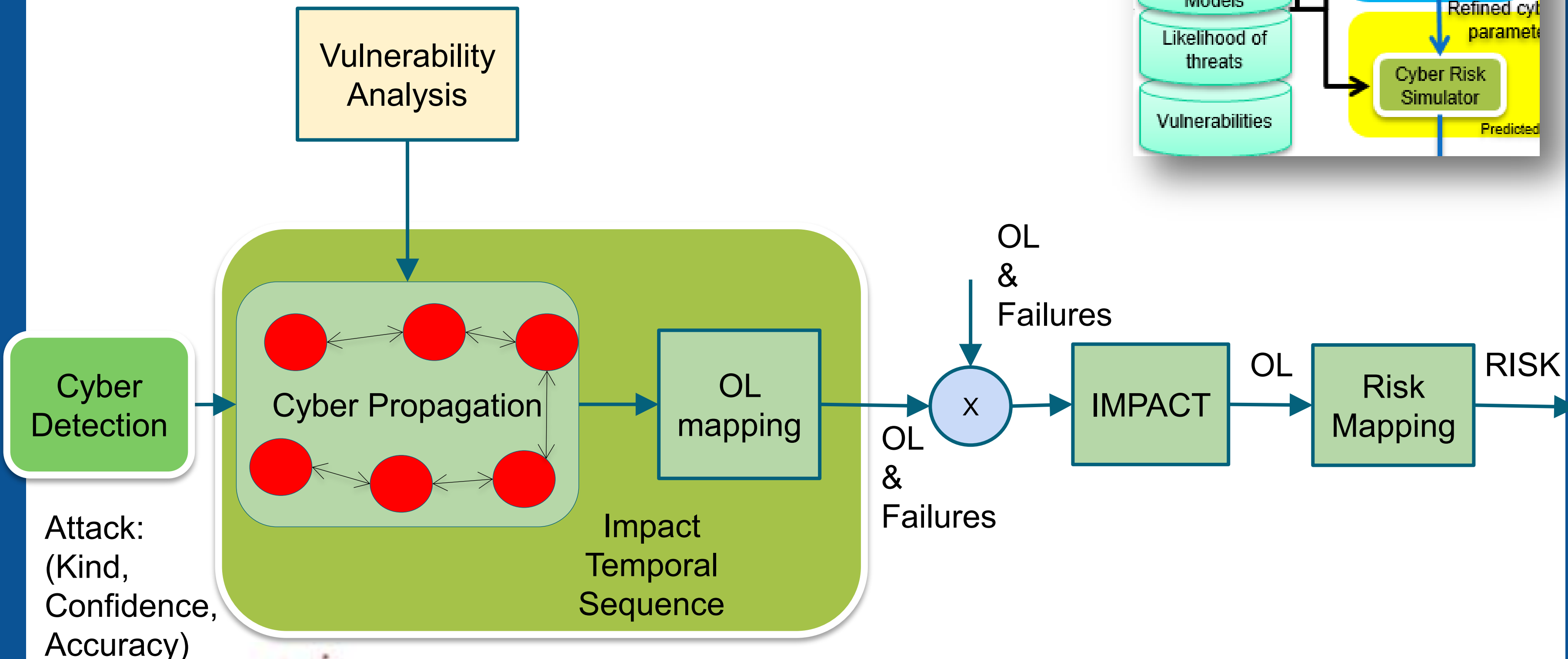




Cockpit CI

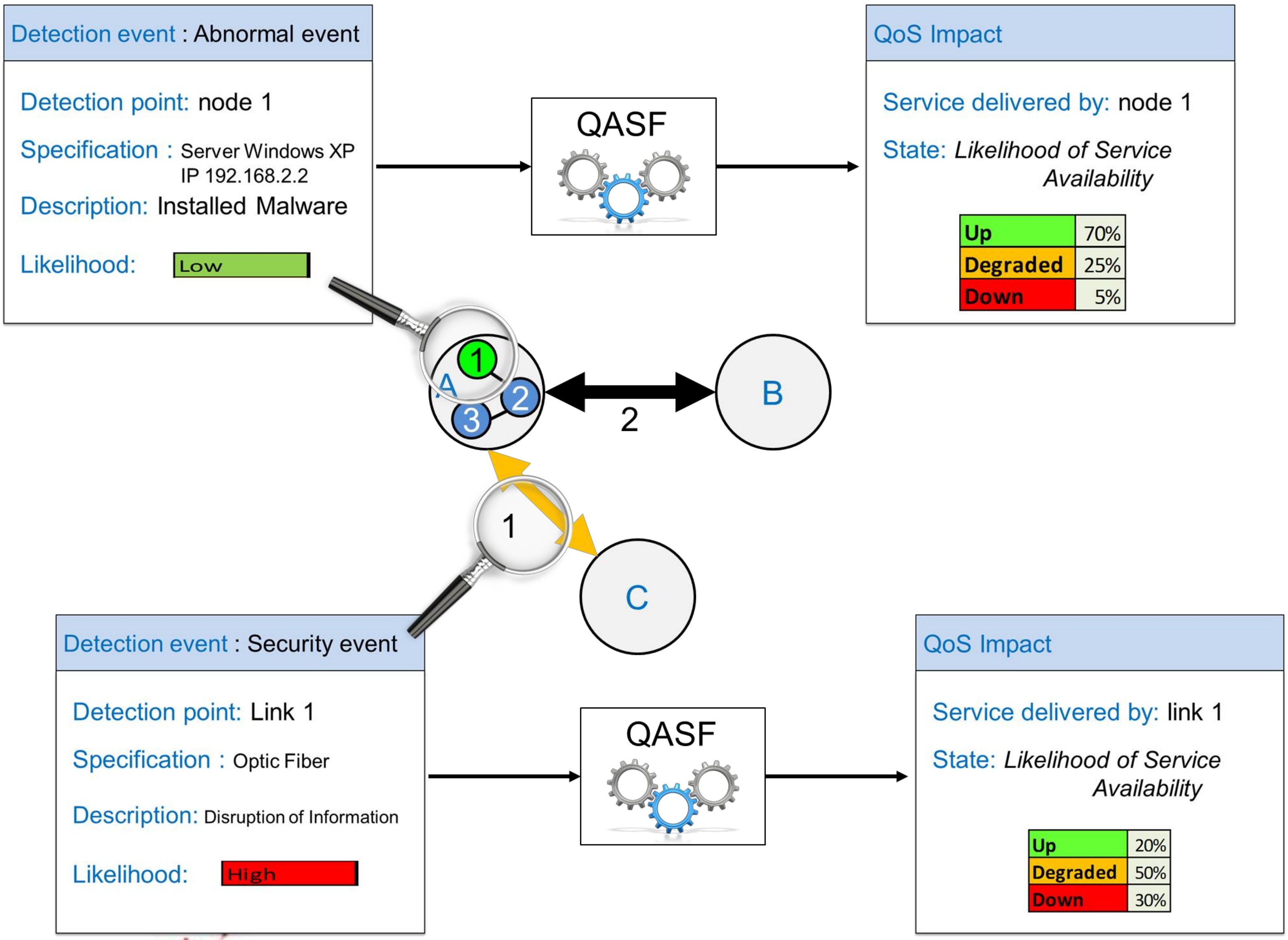
CYBER ALERTS → OPERATIVE LEVELS & FAILURES





Cockpit CI

QoS Assessment Security Factors



Cockpit CI

		Abnormal event				Security event				Security Incident			
Likelihood of Impact on QoS of the node		Up	Degraded	Down	Total	Up	Degraded	Down	Total	Up	Degraded	Down	Total
Installed malware	Low	70%	25%	5%	100%	40%	40%	20%	100%	5%	50%	45%	100%
	Medium	55%	35%	10%	100%	20%	50%	30%	100%	0%	30%	70%	100%
	High	35%	50%	15%	100%	5%	40%	55%	100%	0%	15%	85%	100%

For each type of Node/Component/Link				Detection Analysis Level											
				Abnormal event				Security event				Security Incident			
		Likelihood of Impact on QoS of the node		Up	Degraded	Down	Total	Up	Degraded	Down	Total	Up	Degraded	Down	Total
Cyber Attack Detection at node level – Operational Impact	1	Misuses of resources	Low	80%	10%	10%	100%	70%	20%	10%	100%	0%	60%	40%	100%
			Medium	30%	30%	40%	100%	25%	35%	40%	100%	0%	50%	50%	100%
			High	10%	40%	50%	100%	5%	45%	50%	100%	0%	40%	60%	100%
	2	User compromise	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	3	Root compromise	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	4	Web compromise	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	5	Installed malware	Low	70%	25%	5%	100%	40%	40%	20%	100%	5%	50%	40%	95%
			Medium	55%	35%	10%	100%	20%	50%	30%	100%	0%	30%	70%	100%
			High	35%	50%	15%	100%	5%	40%	55%	100%	0%	15%	85%	100%
	6	DOS	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	7	Timeliness degradation	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
Cyber Attack Detection at node level – Informational Impact	8	Distortion of information	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	9	Disruption of Information	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	10	Destruction of Information	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
	11	Disclosure of information	Low				0%				0%				0%
			Medium				0%				0%				0%
			High				0%				0%				0%
Cyber Attack Detection at node level – Vulnerability	12	Software /firmware	Low												0%
			Medium												0%
			High												0%
	13	Hardware	Low												0%
			Medium												0%
			High												0%

Likelihood of cyber attack

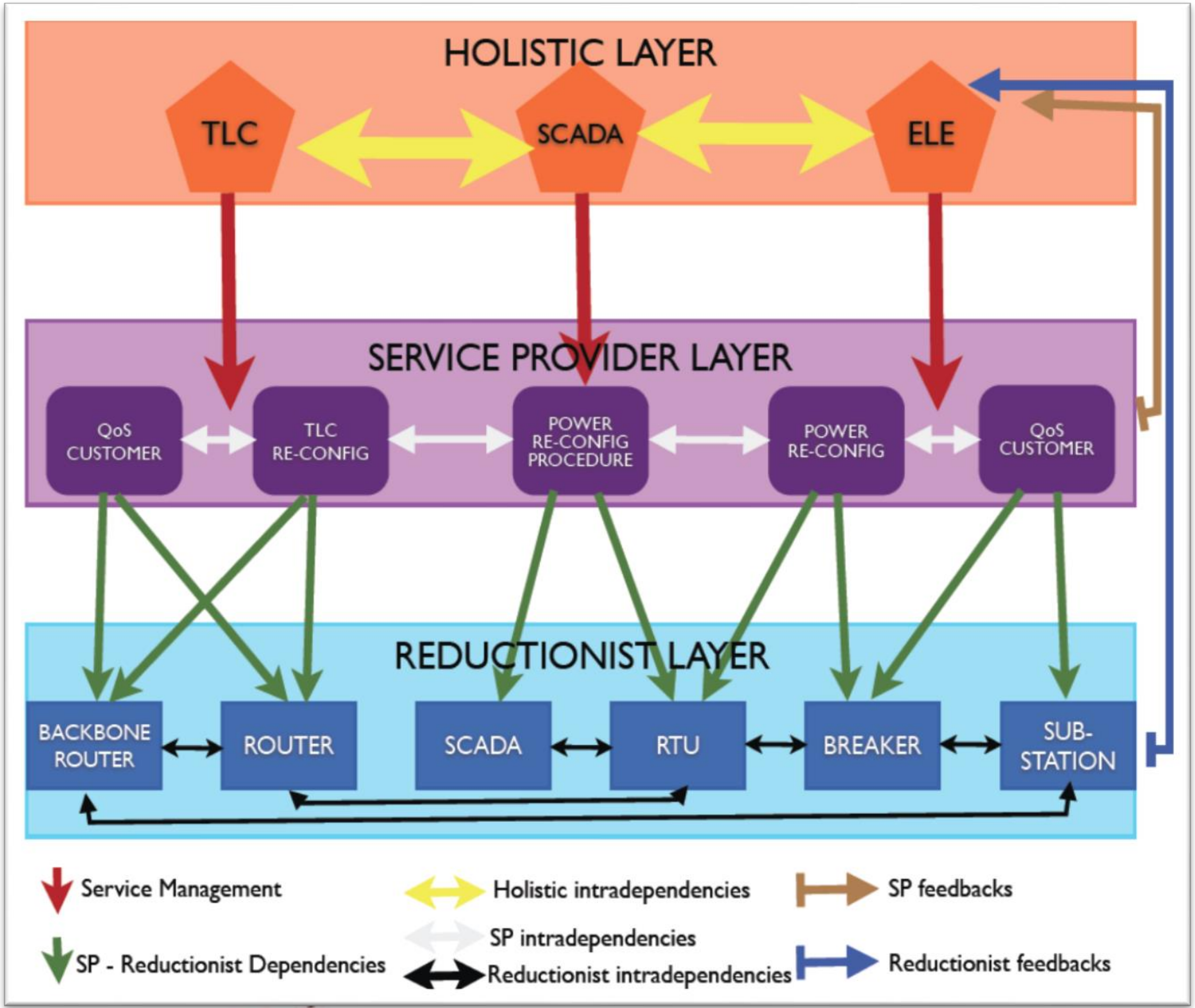
Cockpit CI

Physical / Logical / Geographic / Cyber

Interdependency Model

Cockpit CI

THE MIXED HOLISTIC-REDUCTIONISTIC MODELLING PERSPECTIVE

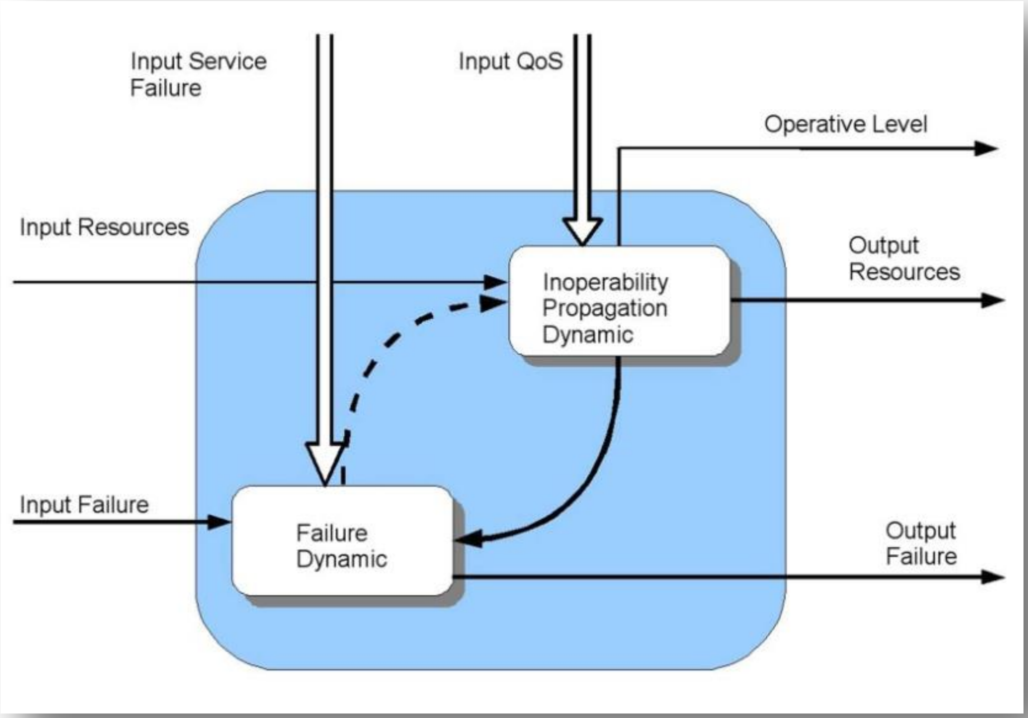


Behaviours (physical or logical or political) not emerging from Reductionistic layer

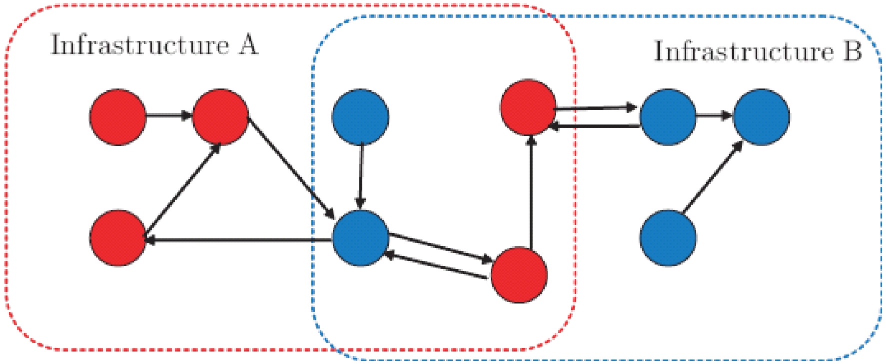
Expressions of both holistic and reductionistic models

Intra-Inter-Infrastructure homogeneous layer capturing interdependencies

CISIA: an agent based simulator

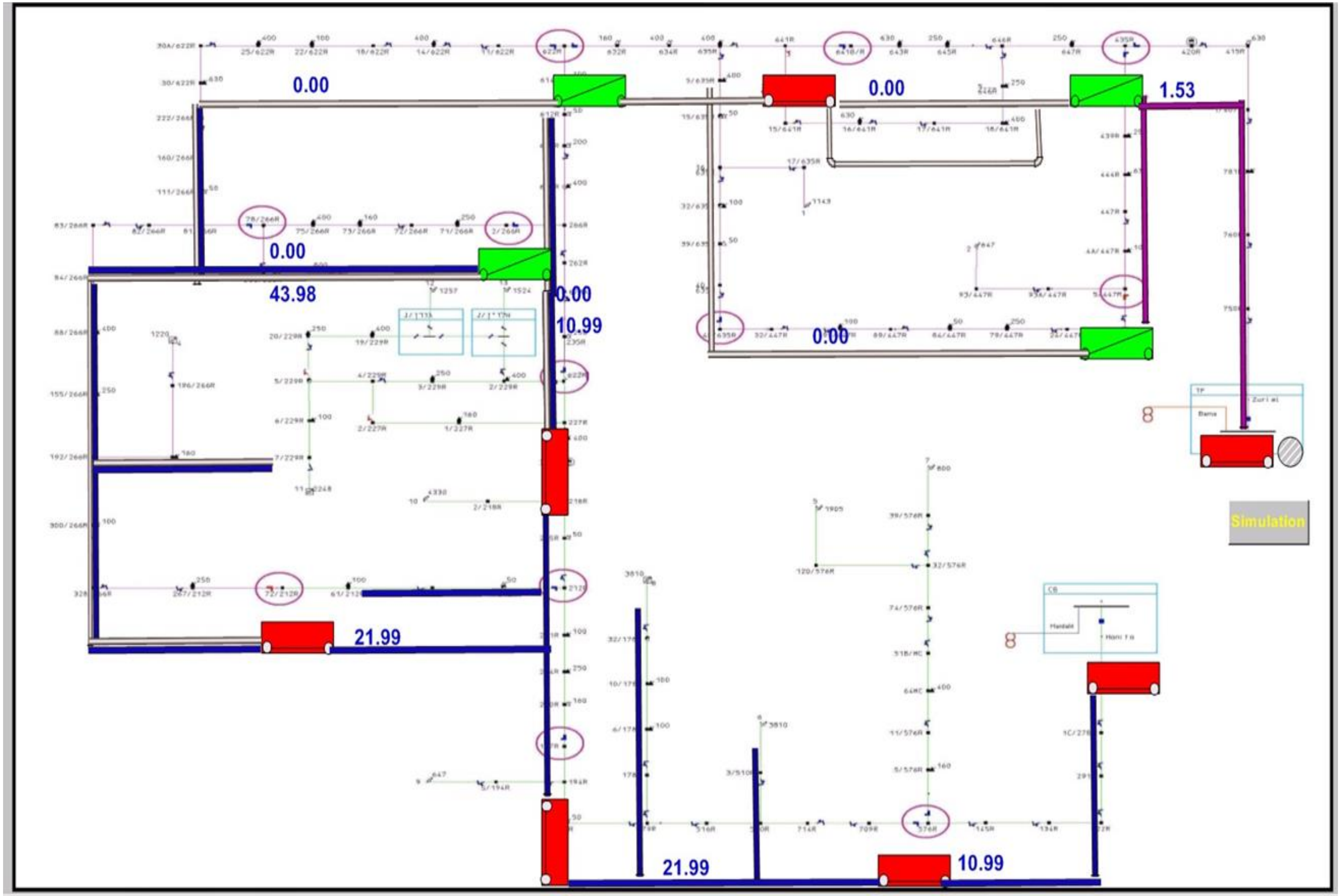


Reductionistic decomposition for cascading effects evaluation



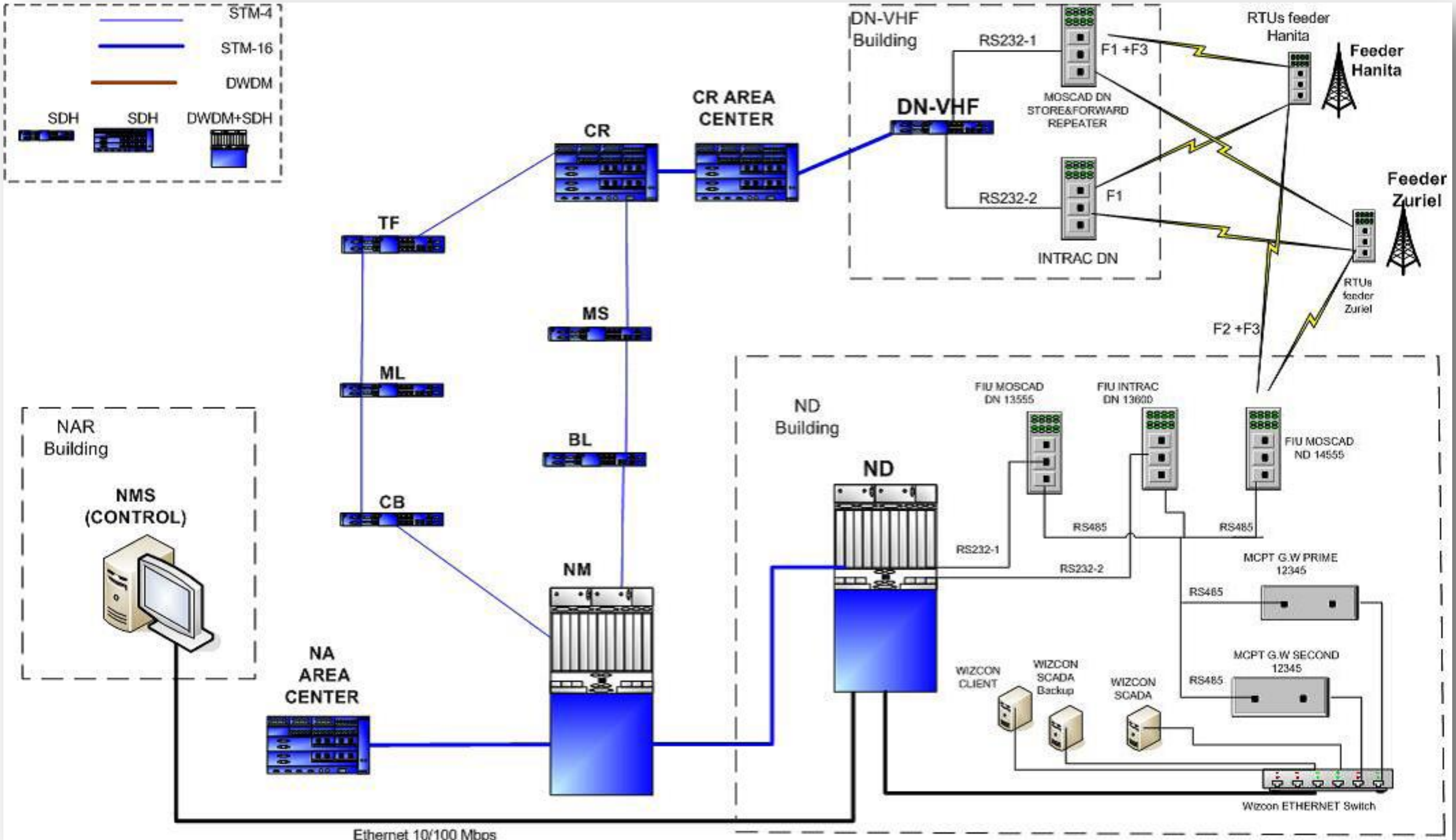
Cockpit CI

Medium Voltage Electric Grid



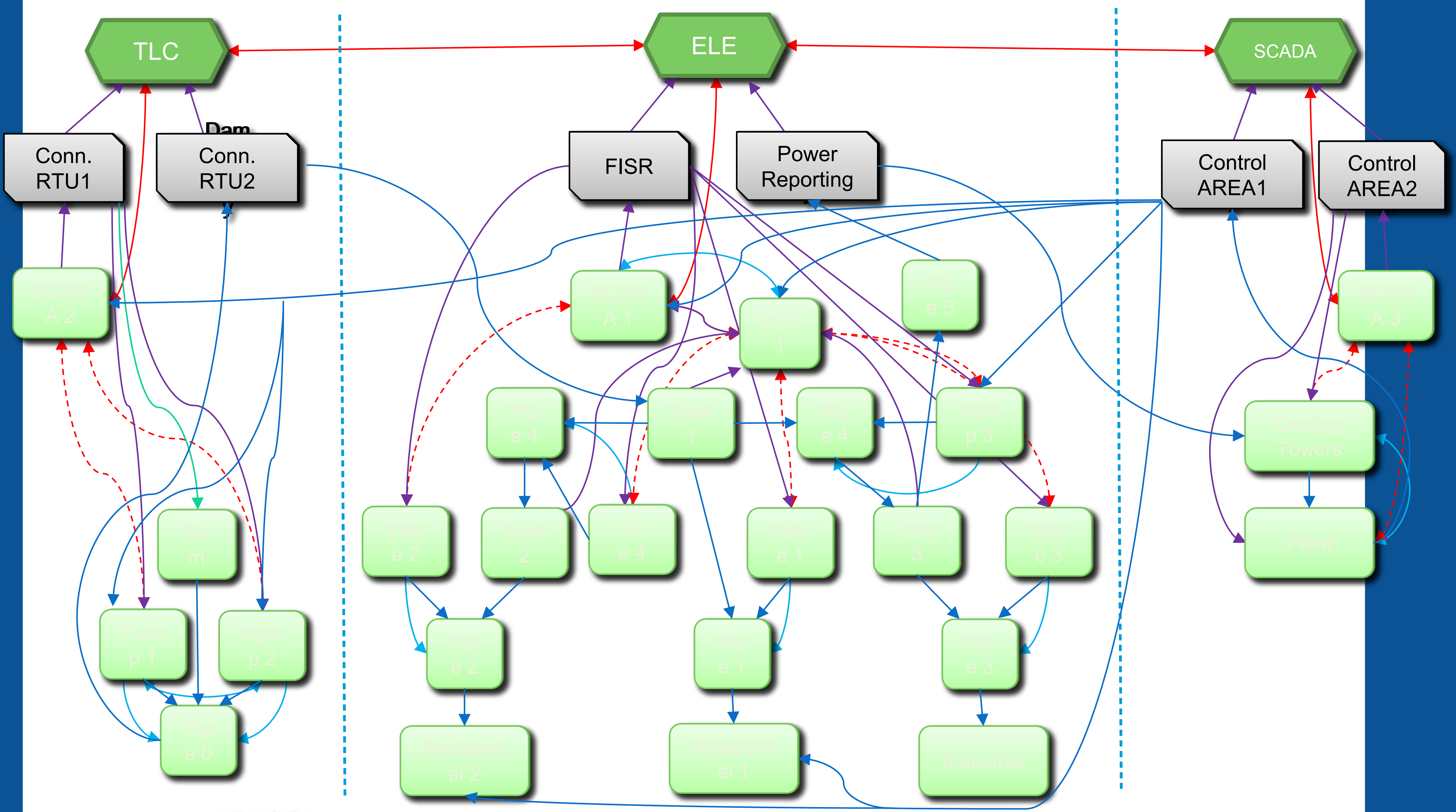
Cockpit CI

Interconnected telecommunication and SCADA network



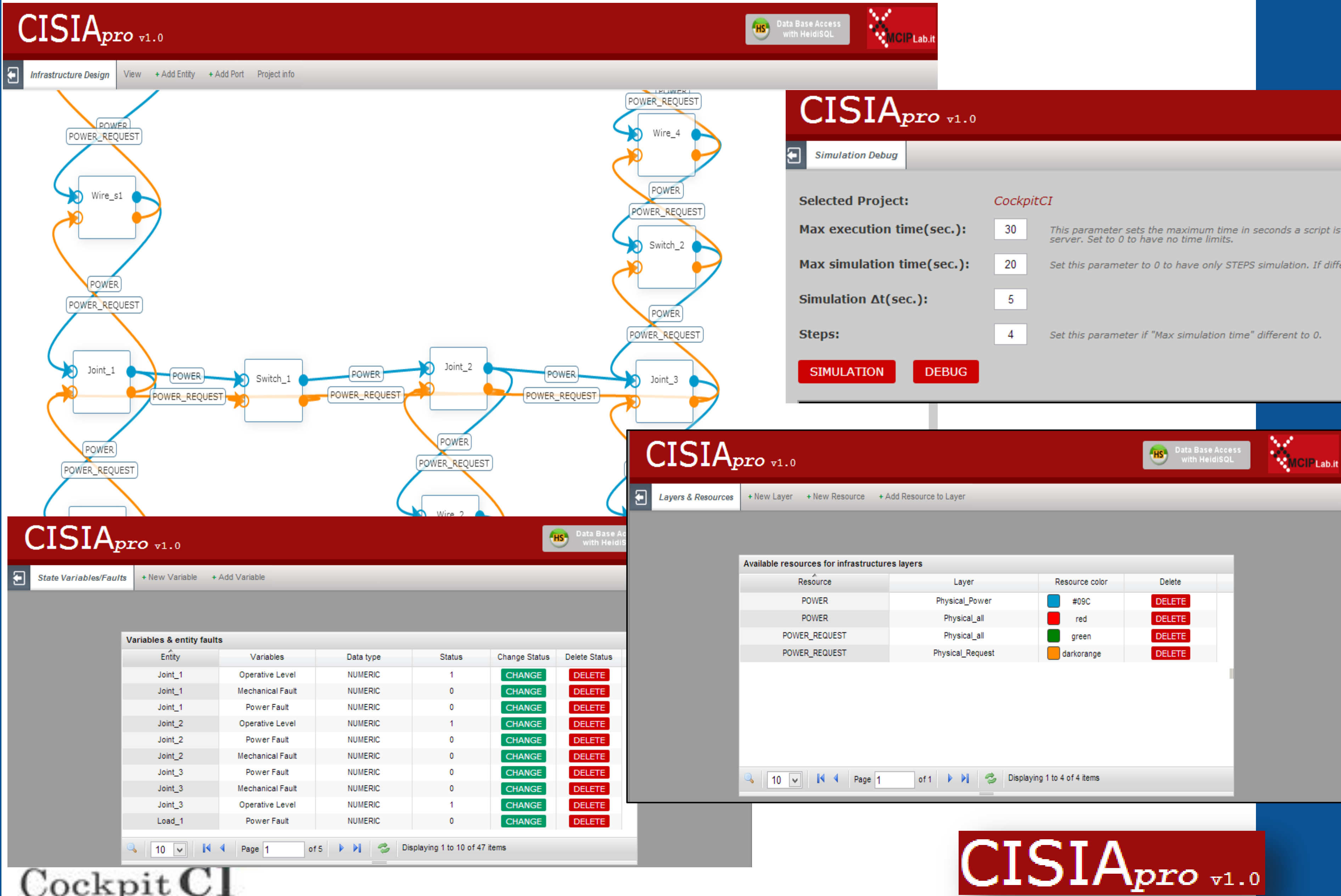
Cockpit CI

Interdependency modeling using MHR



Cockpit CI

CISIA*pro*: an output of CockpitCI project

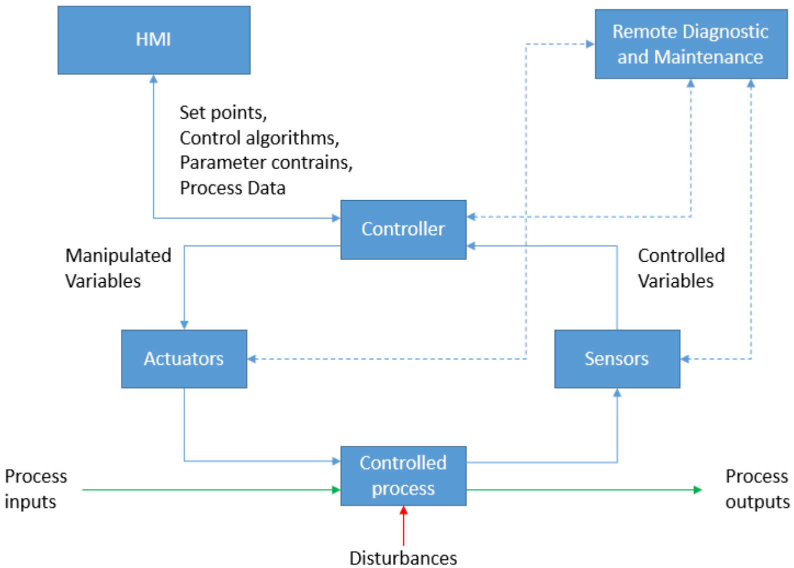


Smart Extension, Smart Cluster, Smart ICS

Smart RTU and Reaction Strategies

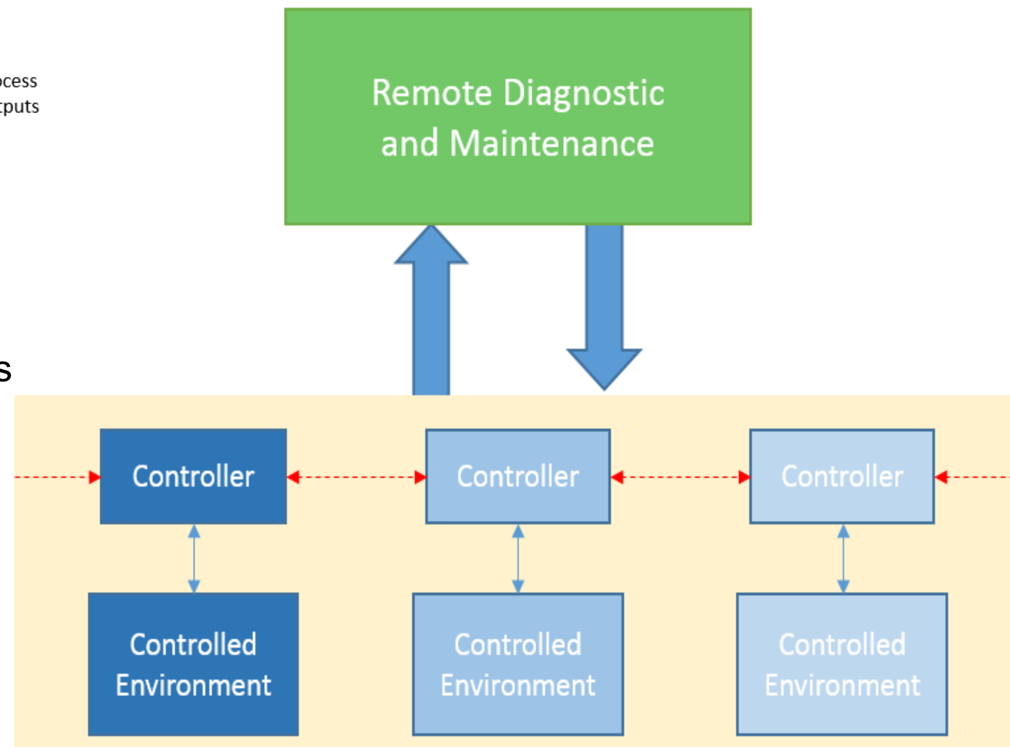
Cockpit CI

SMART Industrial Control Systems



Standard ICS

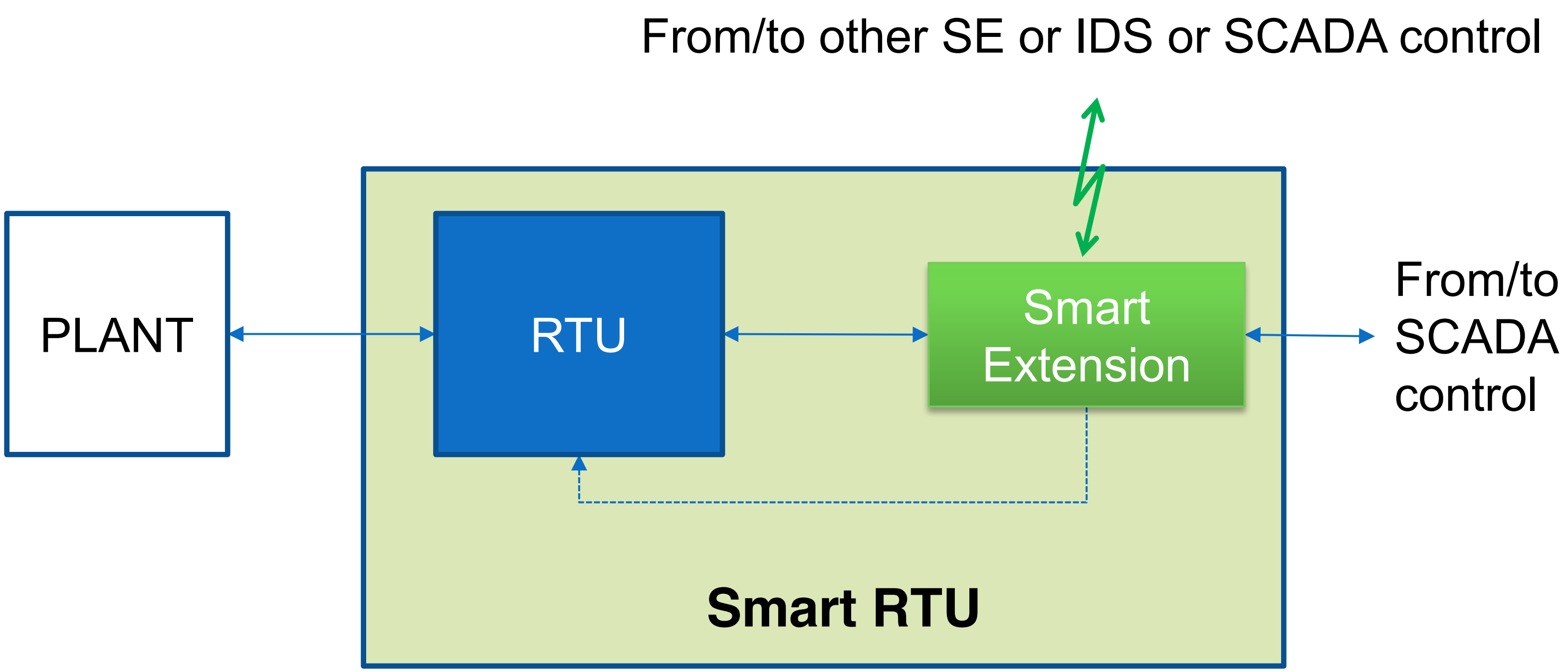
SMART ICS



- Process optimization
- Monitor and manage information on all levels
- Identify the optimal response strategies in case of attack or contingency
- Perform (or suggest to the operator) automatic reactions at global level
- Coordinate automatic reactions at local level

Cockpit CI

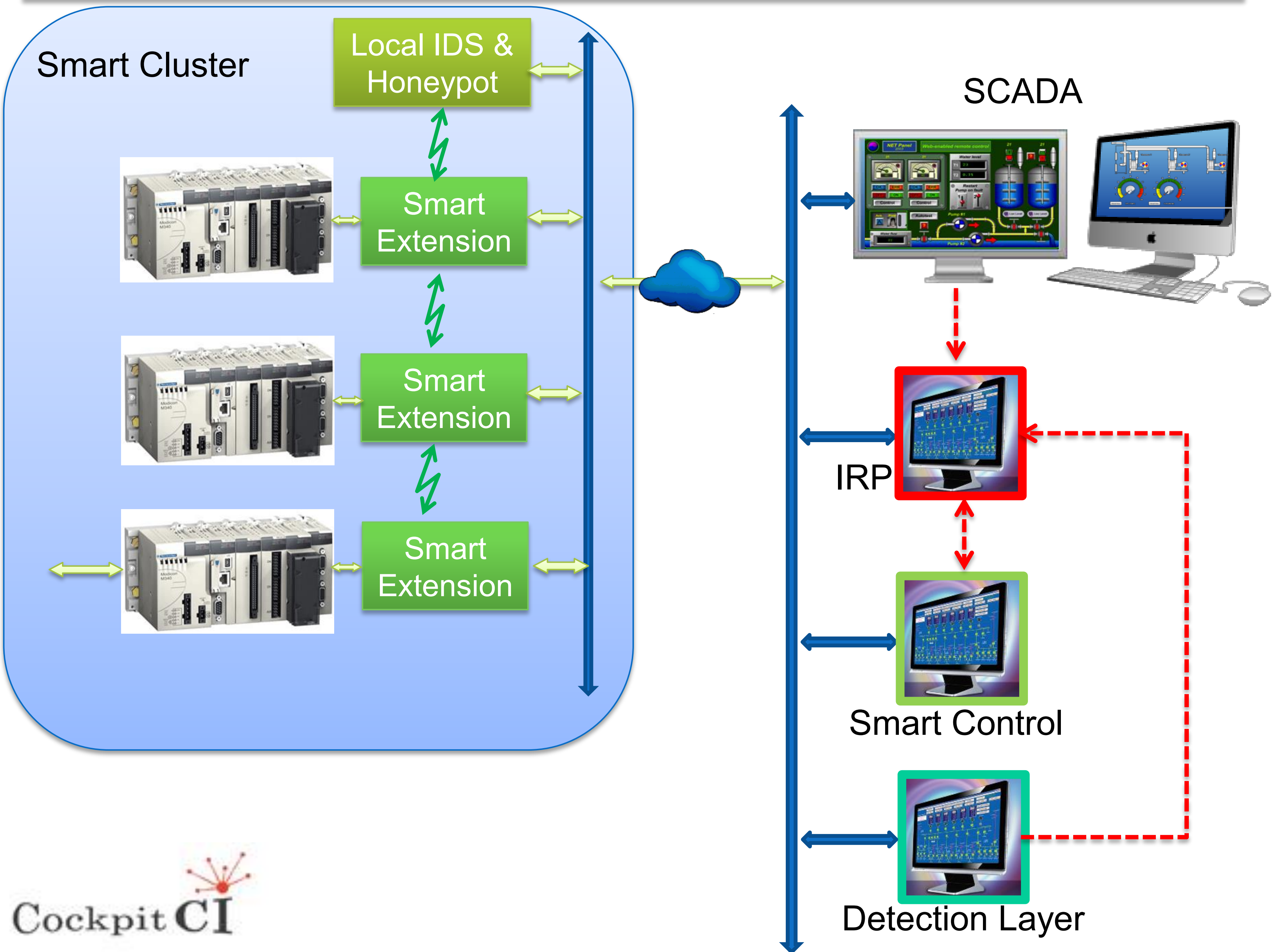
Smart Extension and Smart RTU



The Smart Extension is an application level commands' filter device, inserted in the SCADA communication channel. If the risk level of a cyber attack is increased, the Smart Extension may block inputs to the RTU (or reduce the accepted input messages to a minimum), in order to maintain a safe state.

Cockpit CI

Smart Ecosystem and Cluster Awareness



Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Selex ES A Finmeccanica Company · חברת החשמל Israel Electric · Transelectrica · Lyse · itrust consulting · Multitel · Roma Tre Università degli Studi · ENEA · CRAT · University of Surrey · tudor · Universidade de Coimbra FCTUC Faculdade de Ciências e Tecnologia

Any question ?

Information Society

Selex ES A Finmeccanica Company | Israel Electric | Transelectrica | Lyse | itrust consulting | Multitel | Roma Tre Università degli Studi | ENEA | CRAT | University of Surrey | Tudor | FCTUC Faculdade de Ciências e Tecnologia

Thank you for your attention

Information Society

Validation process peculiarities in the multinational R&D CIIP projects CockpitCI project

4^{th} CockpitCI Workshop (Bucharest 16.09.2014)

Dr. Leonid Lev

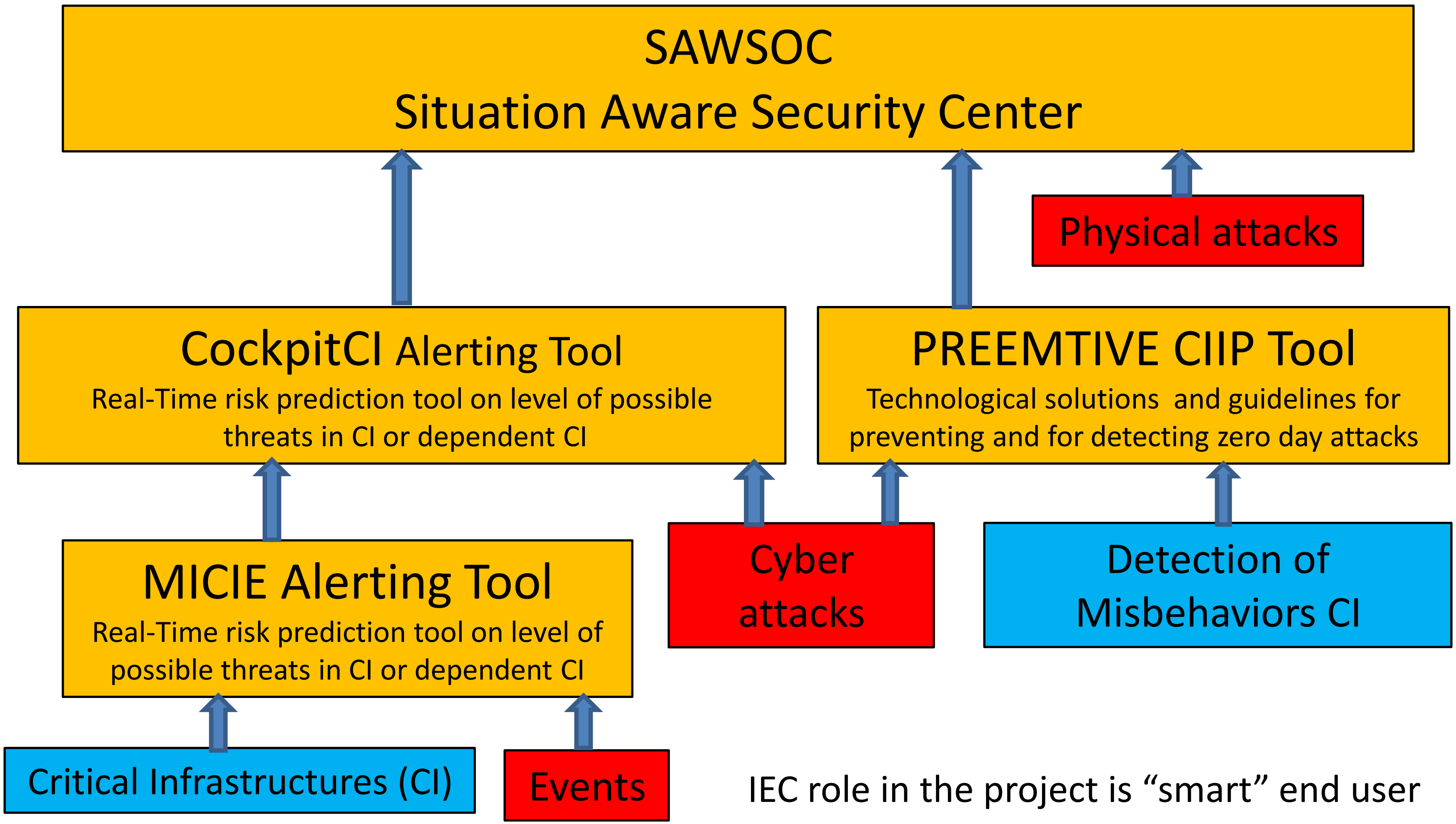
Israel Electric

Information Society

IEC FP7 Background

- IEC participates in FP7 since 2007
- IEC took part in more then 30 proposals in ICT, Security and Energy FP7 Calls
- IEC is a WP leader in 6 projects
- IEC cooperates with 50 partners from different European countries
- IEC received awards from Israel-Europe R&D Directorate for the FP

IECs’ involvement in CIIP Research Projects.



IEC role in the project is “smart” end user

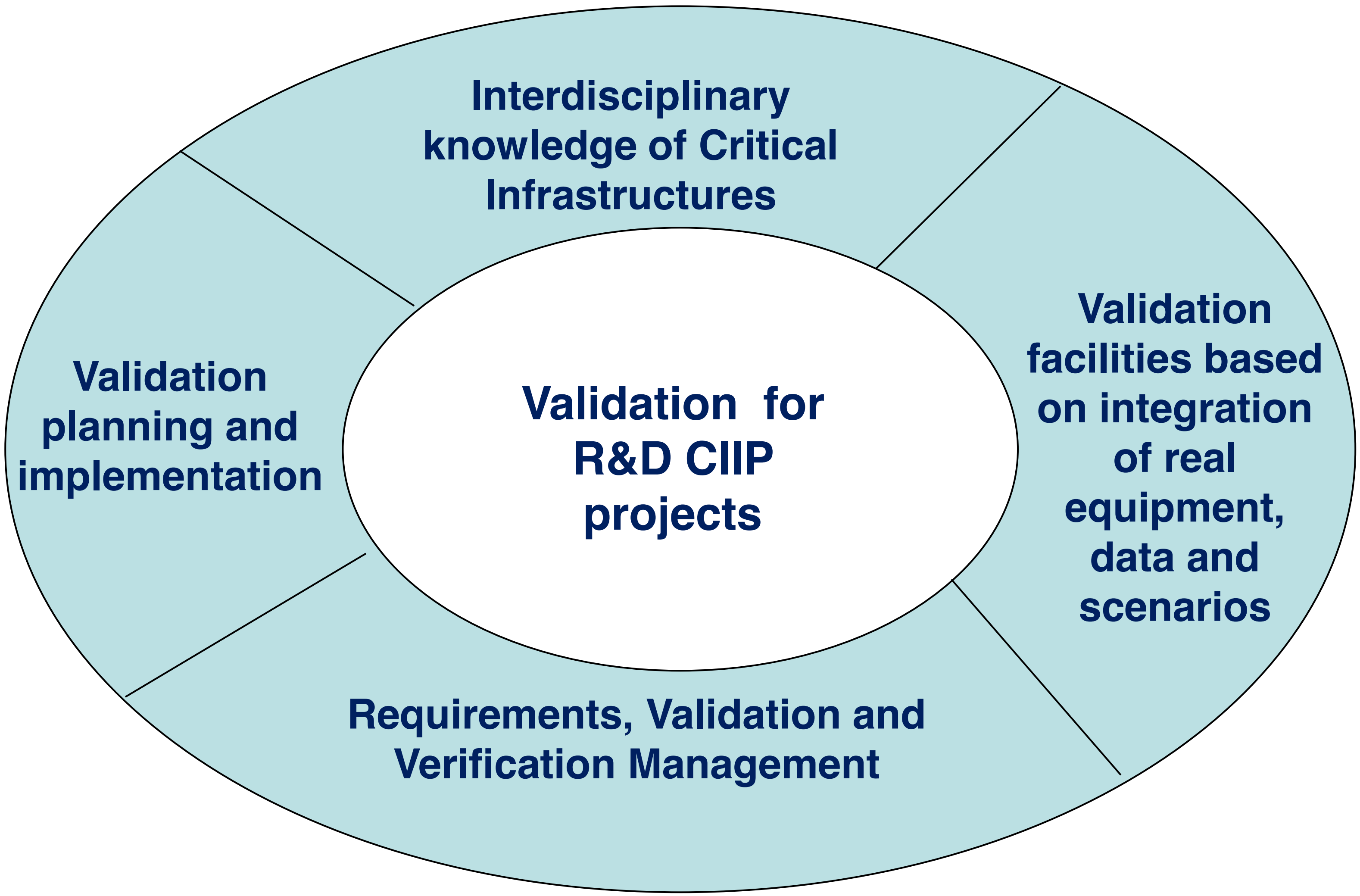
IEC Benefits from Participation in FP7

- **Exposure to trends and innovation**
- **Knowledge of new technologies**
- **Cooperation opportunities**
- **Professional image enhancement**

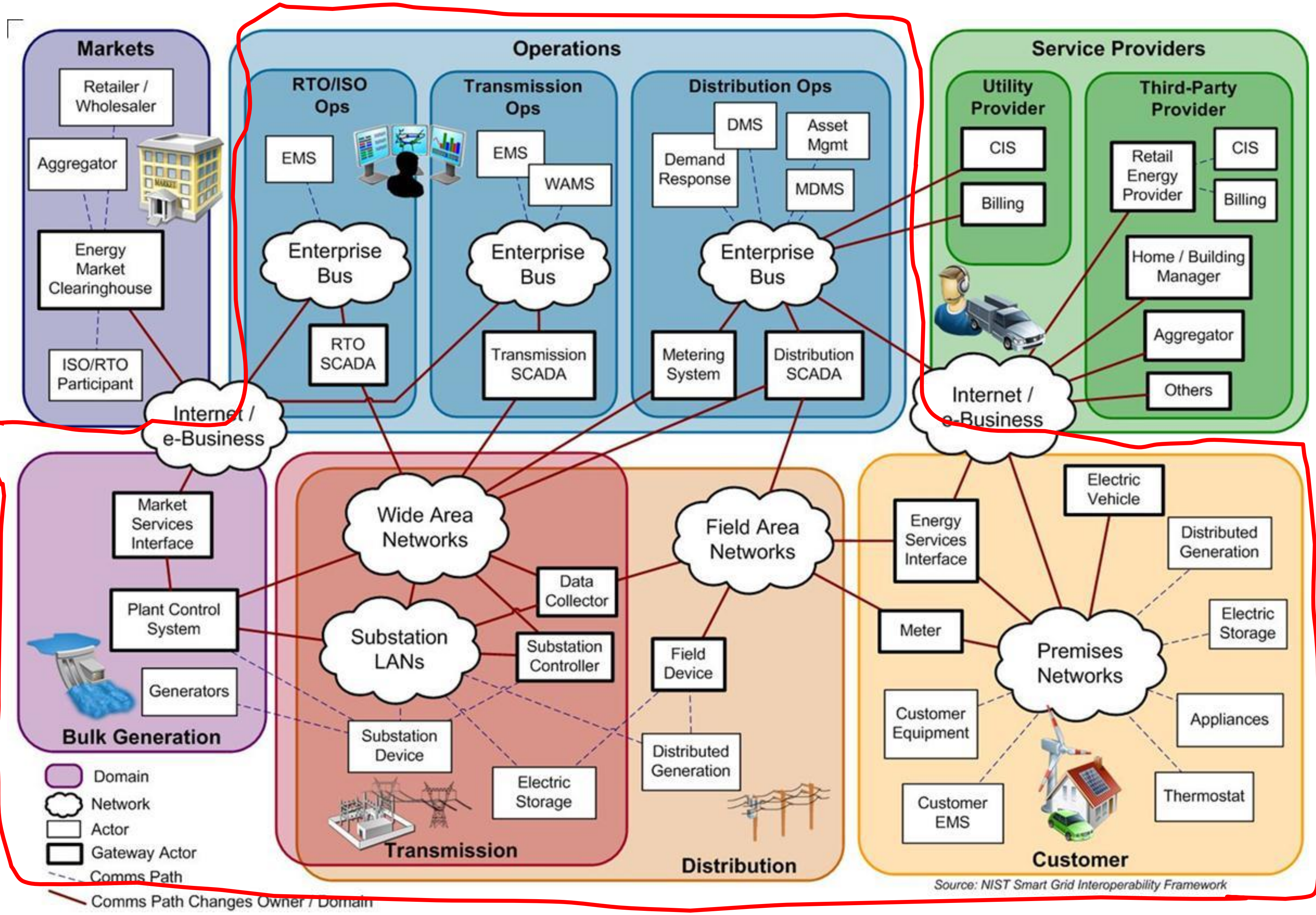
R&D projects validation.
How is it implemented now?

- Some end users are ready to provide small facility or training center. Usually they are not ready to install new applications or provide possibility of cyber attack.
- Laboratories based on PCs and some PLCs.
- Usually no real data or real scenarios are provided, even rarer the combination of real data and real scenarios could be provided.
- I do not know some end user who could provide the remote access to the real equipment, applications and communication networks.
- No single laboratory of the university or SME can create a seemingly infinite infrastructure capable of serving massive amounts of users at all times.

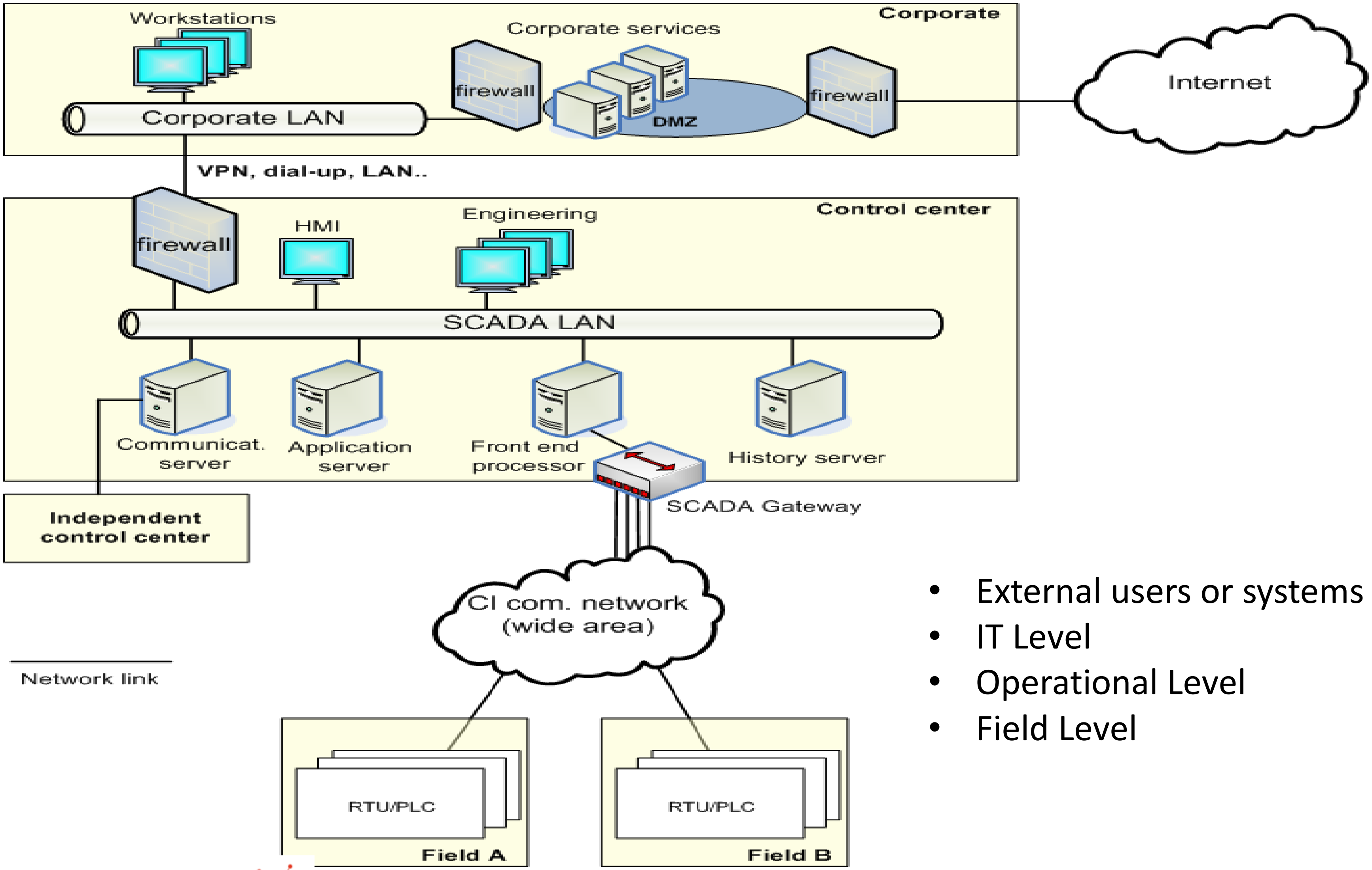
IEC Validation Concept for R&D projects



Typical Electrical Grid (NIST)



Generic Industrial Control System(ICS) Reference Architecture



- External users or systems
- IT Level
- Operational Level
- Field Level

What is IEC solution?

Develop facilities for design and validation of Industrial Control Systems (ICS) that will provide an architecture where resources and services can be transparently and dynamically managed, provisioned and relocated "without borders".

We call these facilities "Hybrid Environment for Design and Validation (HEDVa)

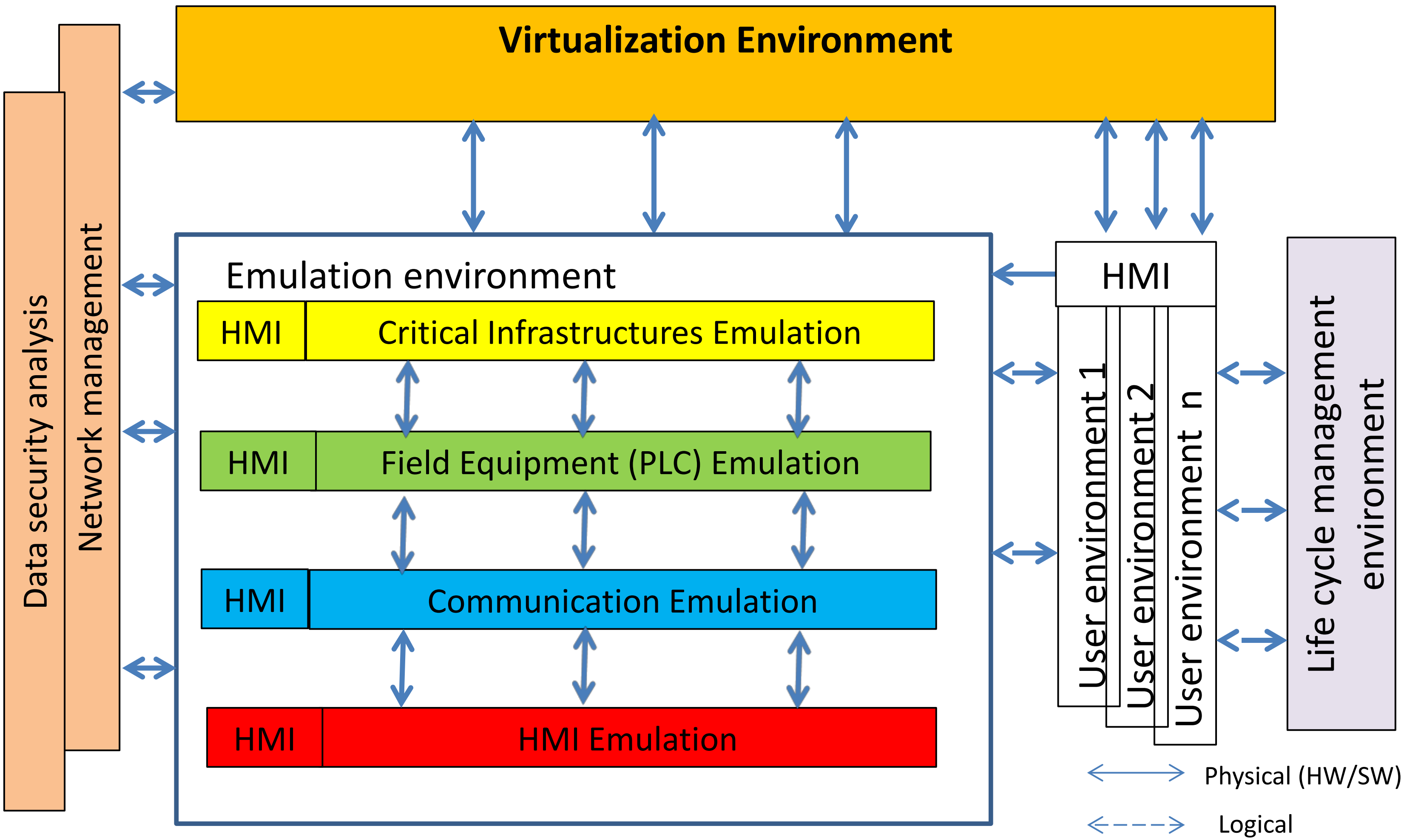
Concept Requirements

- ***General***
  - *Separation between Infrastructures' simulation and services*
  - *Multi-Site Capabilities*
  - *Service Orientation*
  - *Virtualization Technology Independence*
  - *Security*
- ***Infrastructures***
  - *Hybrid Infrastructures' simulation*
  - *Using real knowledge for infrastructures' scenarios implementation*
  - *Using historic data for infrastructures' scenarios implementation*
  - *Adaptive resource allocation*
  - *Migration and elasticity transparency*
  - *Local optimizations*
- ***Service Management***
  - *Flexible virtualization configurations*
  - *Resources allocation and management*
  - *Conflicts Resolution and Avoidance*
  - *Scenarios and date renewable possibility*

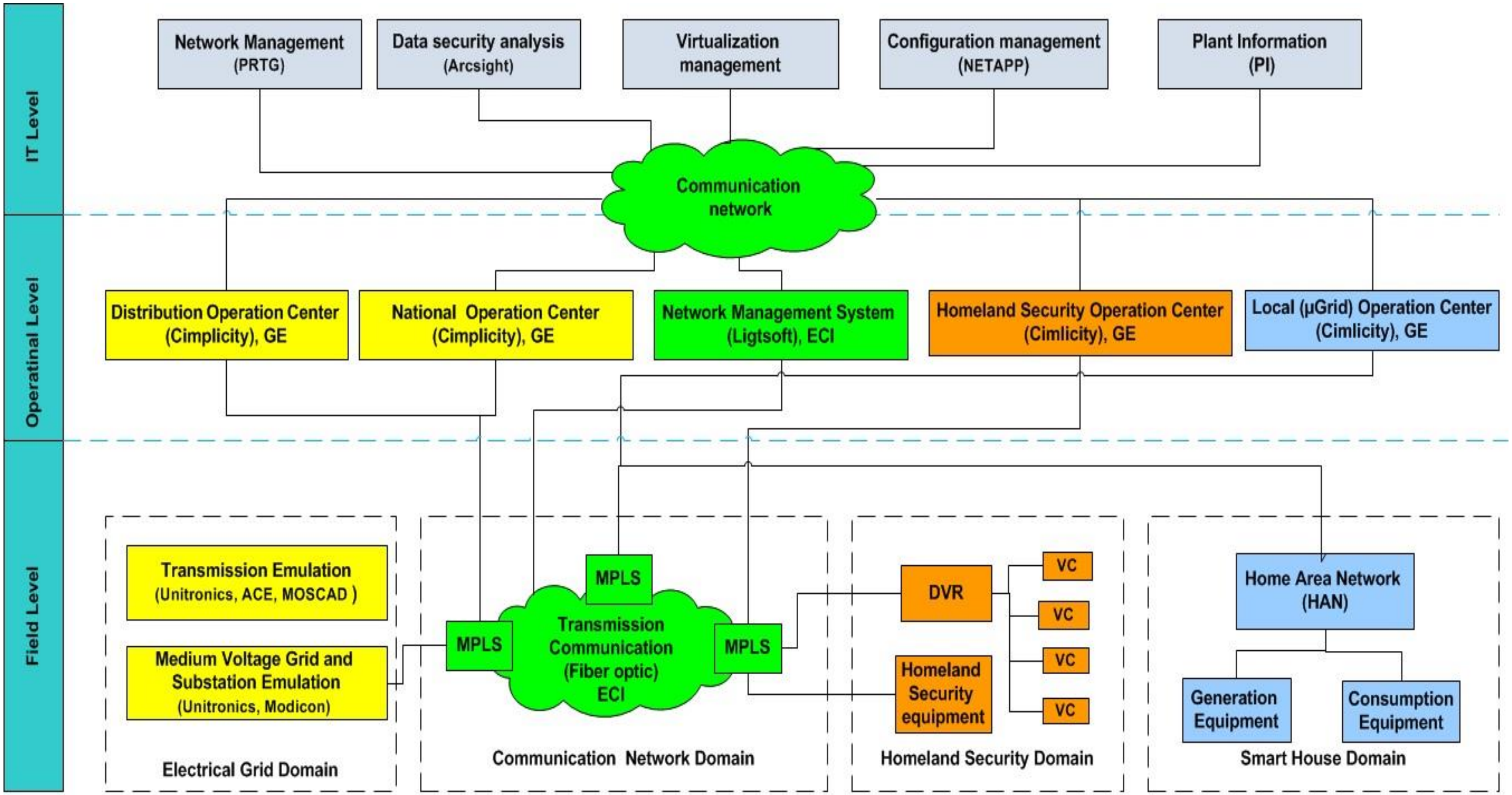
Provided Services

- Critical Infrastructures simulation based on real equipment, historical data and knowledge of operational processes,
- Configuration and maintenance of the “user environment” according to the user requirements,
- Parallel running of several “user environment” without any mutual interference,
- Remote access to specific “user environment”,
- Design and implementation of different reference scenarios including predefined faults and abnormal situations,
- Returning to the normal status of the “user environment” on every stage of design or validation process,
- Providing the environment data traffic and logs for analyses of abnormal situations,
- Requirements and tests management

Hybrid Design and Validation Environment (HEDVa) Concept



Industrial Control Systems (ICS) Emulation



- Critical infrastructures are emulated by real equipment, data and scenarios
- Operational level is emulated by real SCADA applications
- IT level presented by real equipment and applications
- Nothing is connected to operational systems or infrastructures

What Else?

- ✓ **Aware Situation Center**
  - **Security situation**
  - **Operational situation**
  - **Prediction and risks on-line analysis**
  - **Policies**

- ✓ **Validation of systems and tools for cyber security problems**
  - **IT**
  - **Communication**
  - **RTUs and other field equipment**

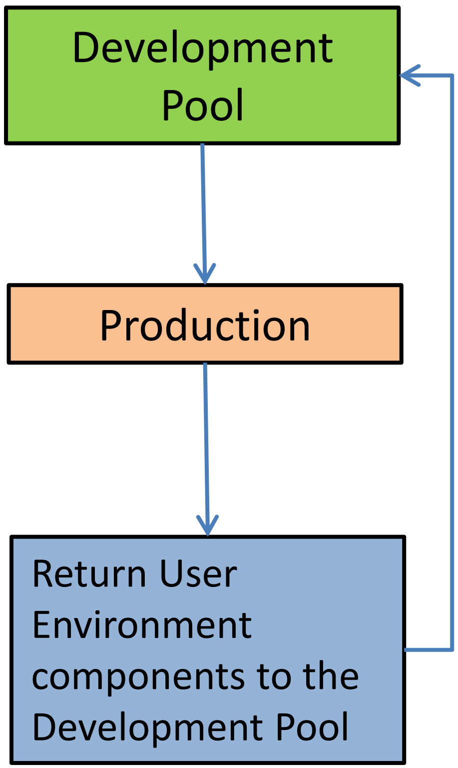
- ✓ **Services portfolio for development of new technologies**

- ✓ **Staff advanced studding**

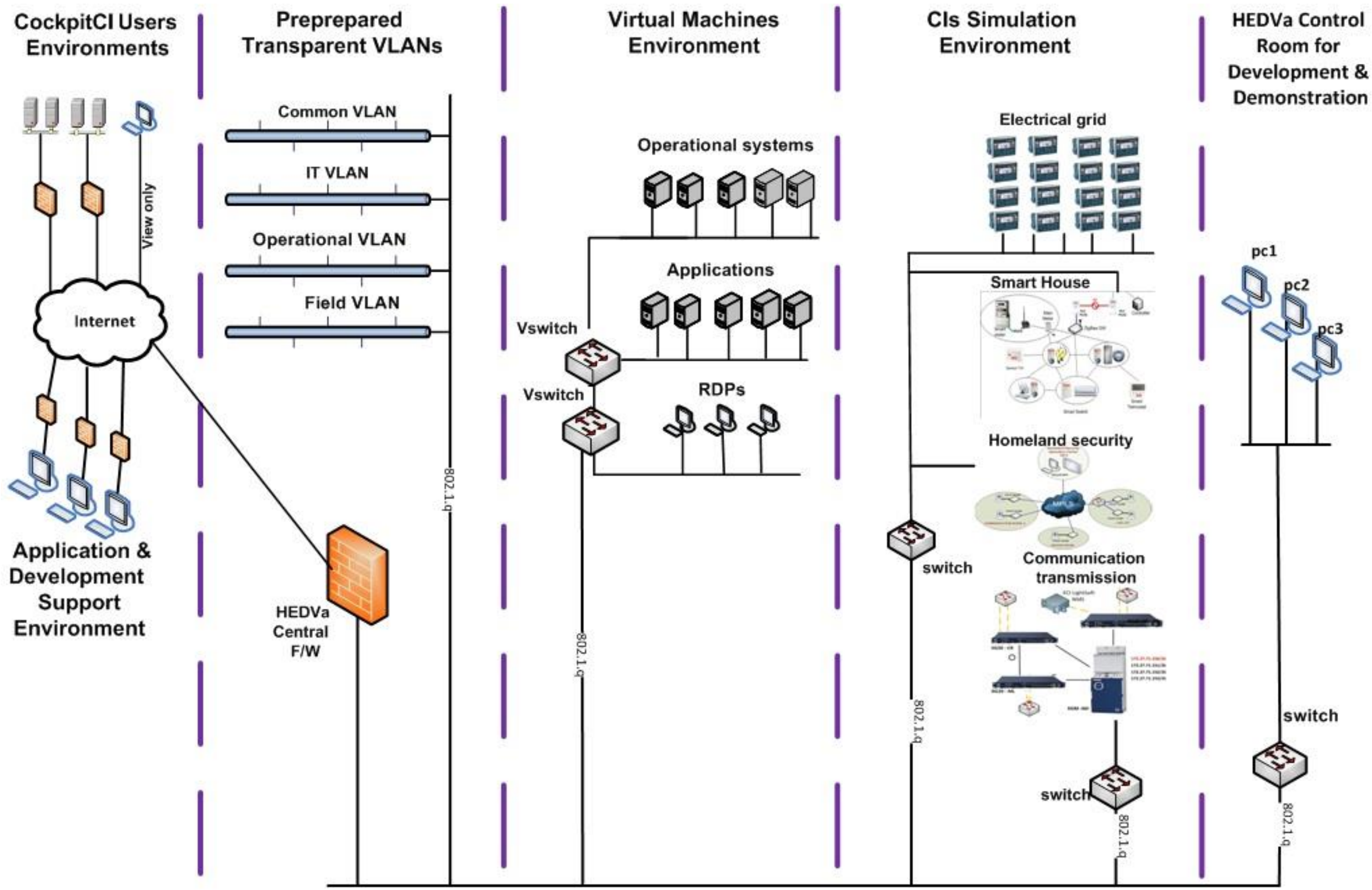
HEDVa Operational model

HEDVa services, applications or equipment could be stated in one of the three following operational modes:

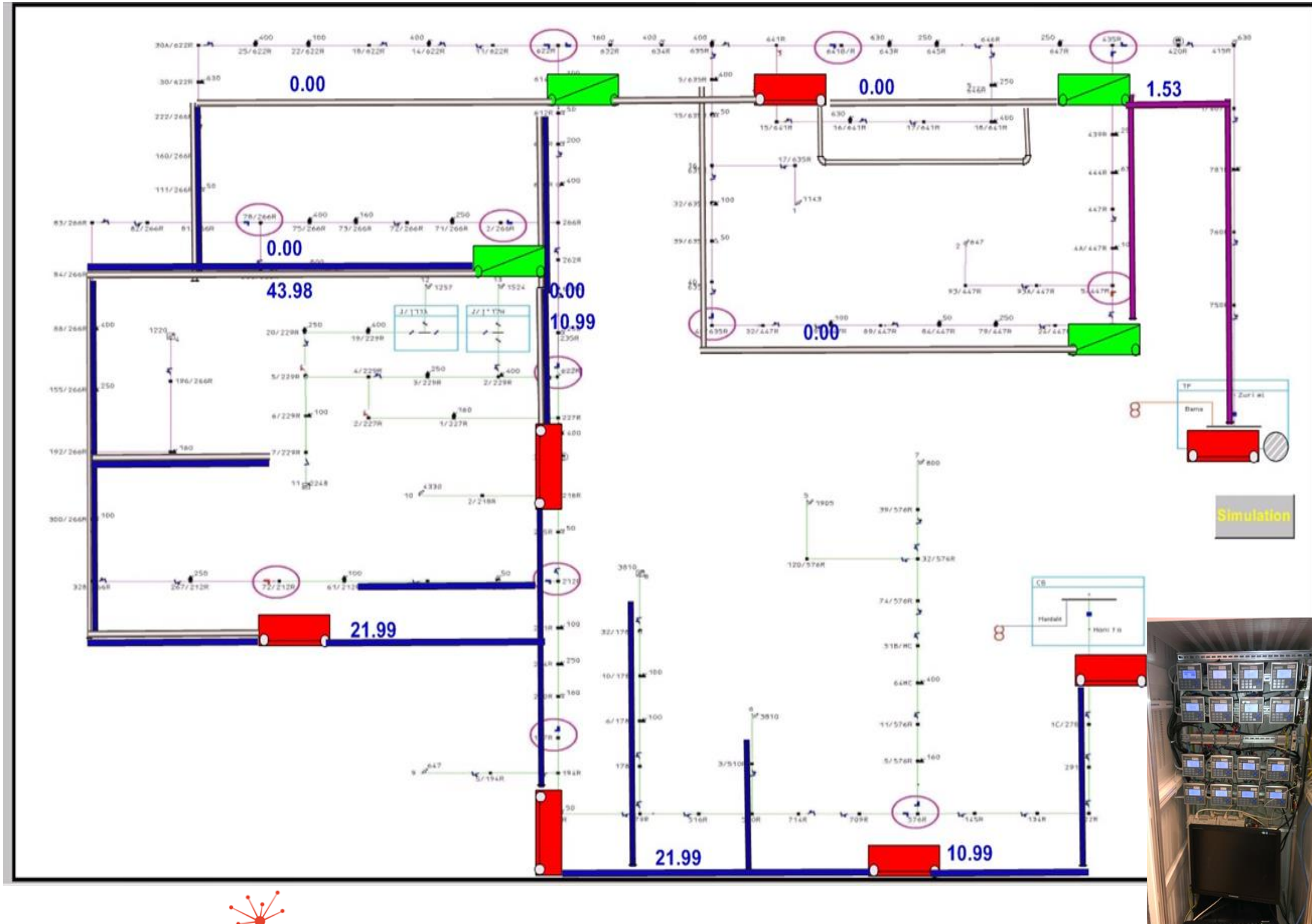
1. **Development Pool** mode proposed for development, testing and maintenance of HEDVa applications and equipment in v 1.0 that includes: emulators, simulators, HMI, interfaces, network configurations, virtualization (VMs, operational systems, SCADA,..)
2. **Production mode** proposes that required services, applications or equipment from the Development Pool are allocated in one of the Users' environment for integration, implementation or project product validation
3. **Return User Environment components to the Development Pool** proposes that all the user environment objectives are completed and all allocated services, applications, equipment and network configuration should be returned to the Development Pool in the v1.0



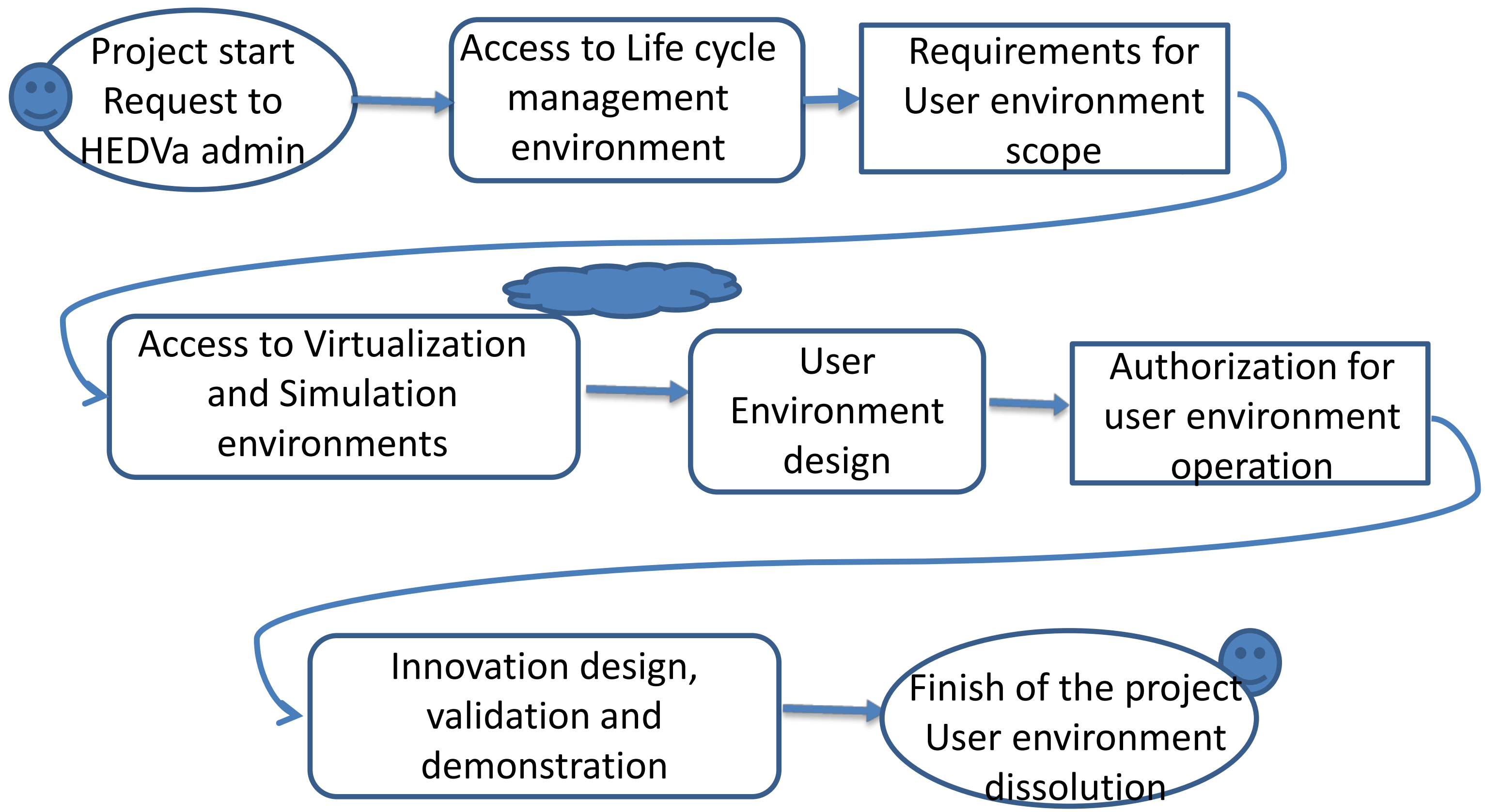
Development Pool



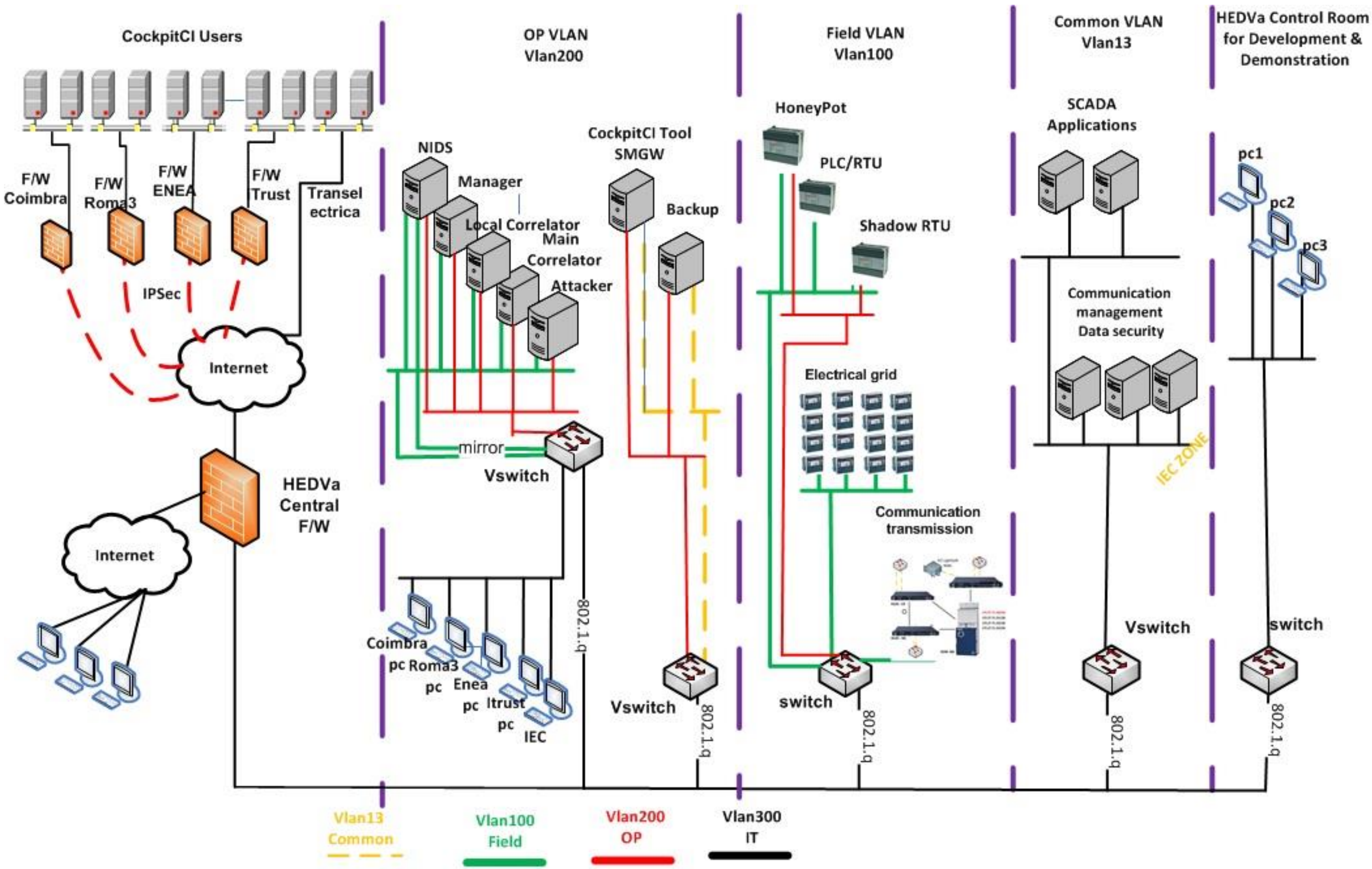
Electrical Grid Medium Voltage Emulator example

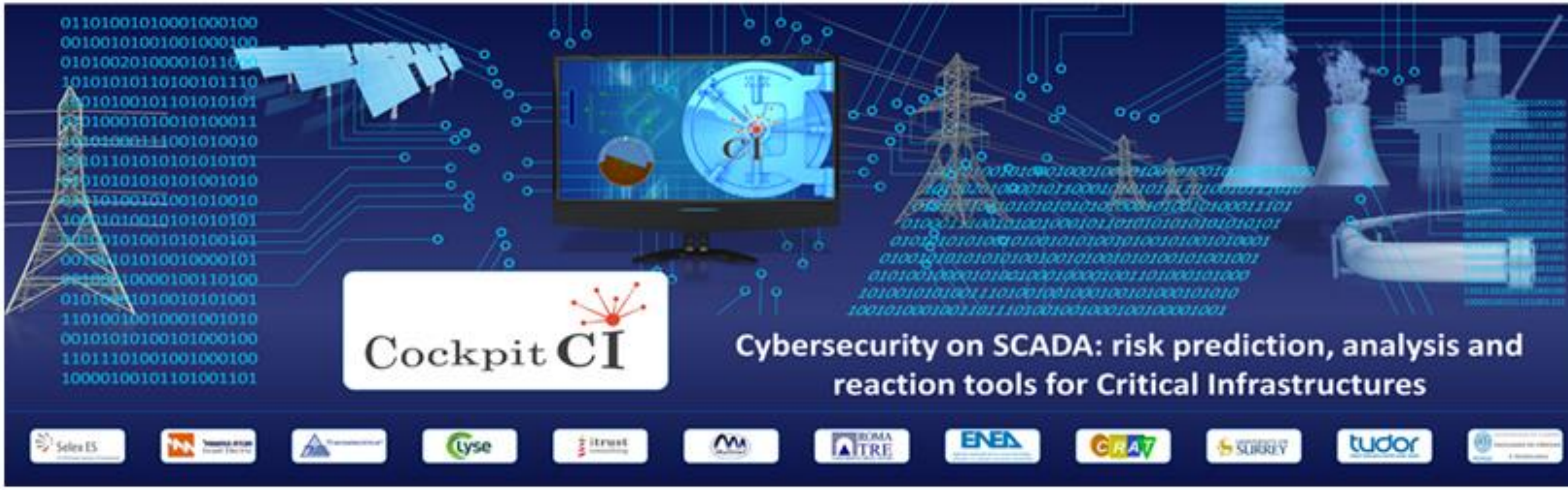


Production Stage: User environment Operation Flow



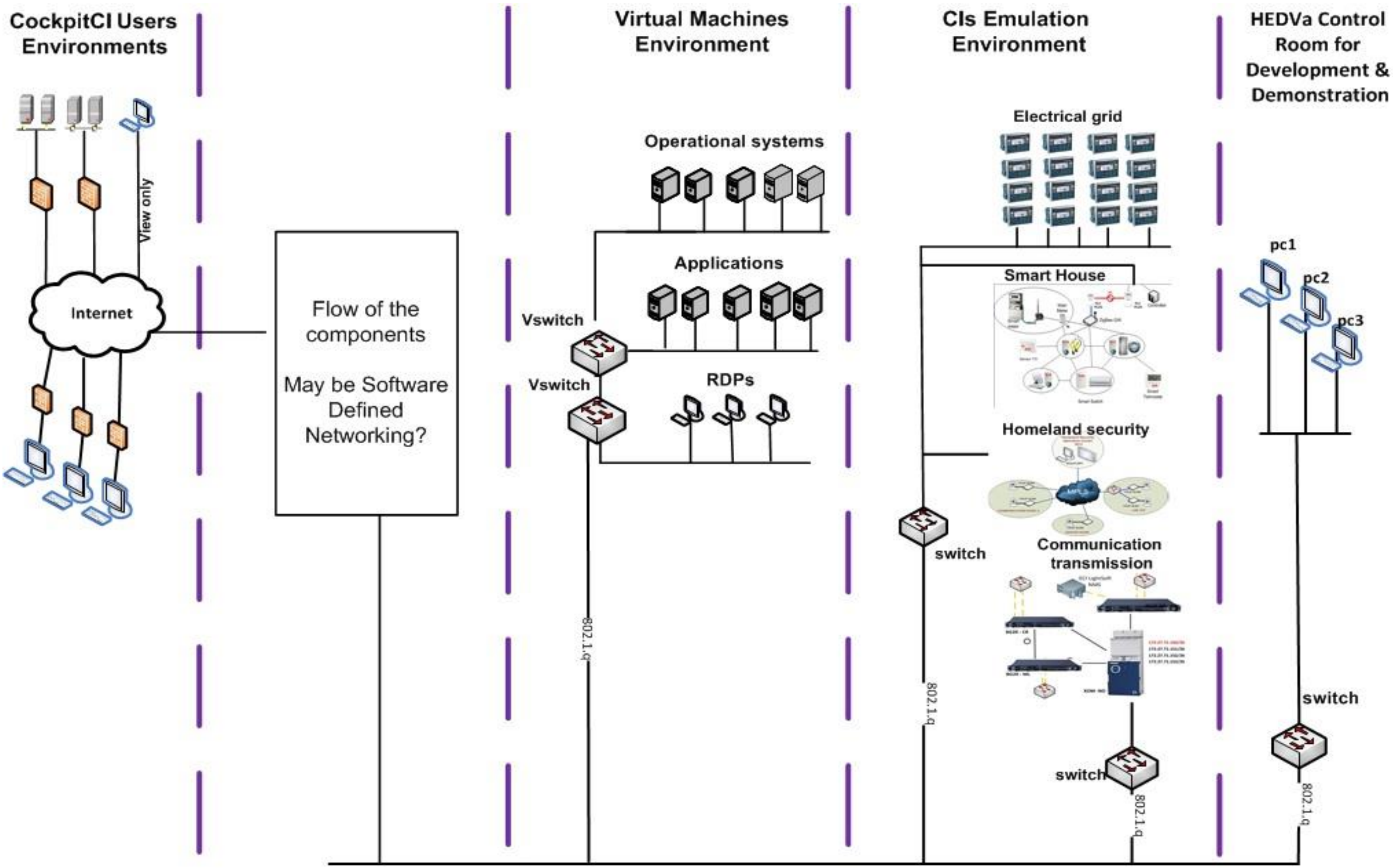
CockpitCI User Environment





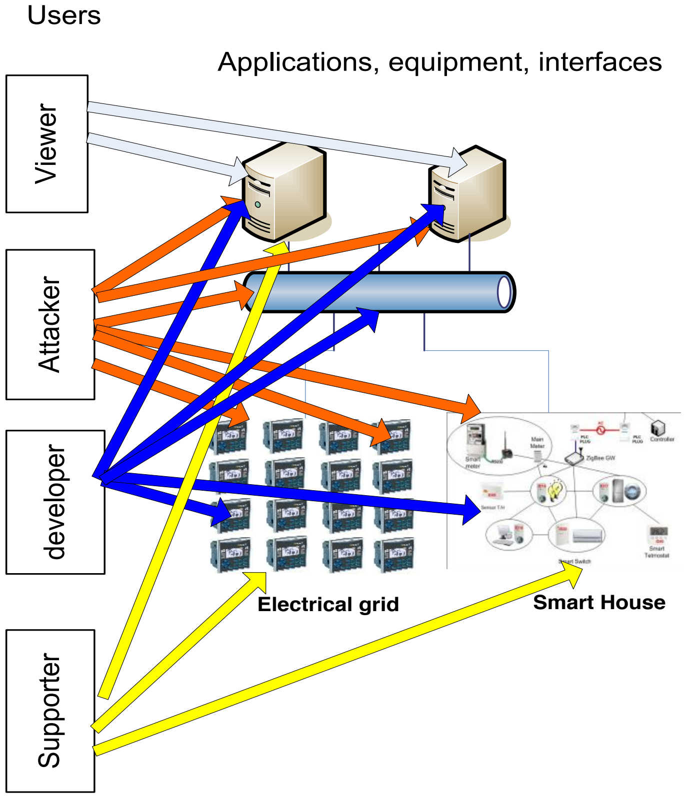
What is the next step?

Development Pool Vision

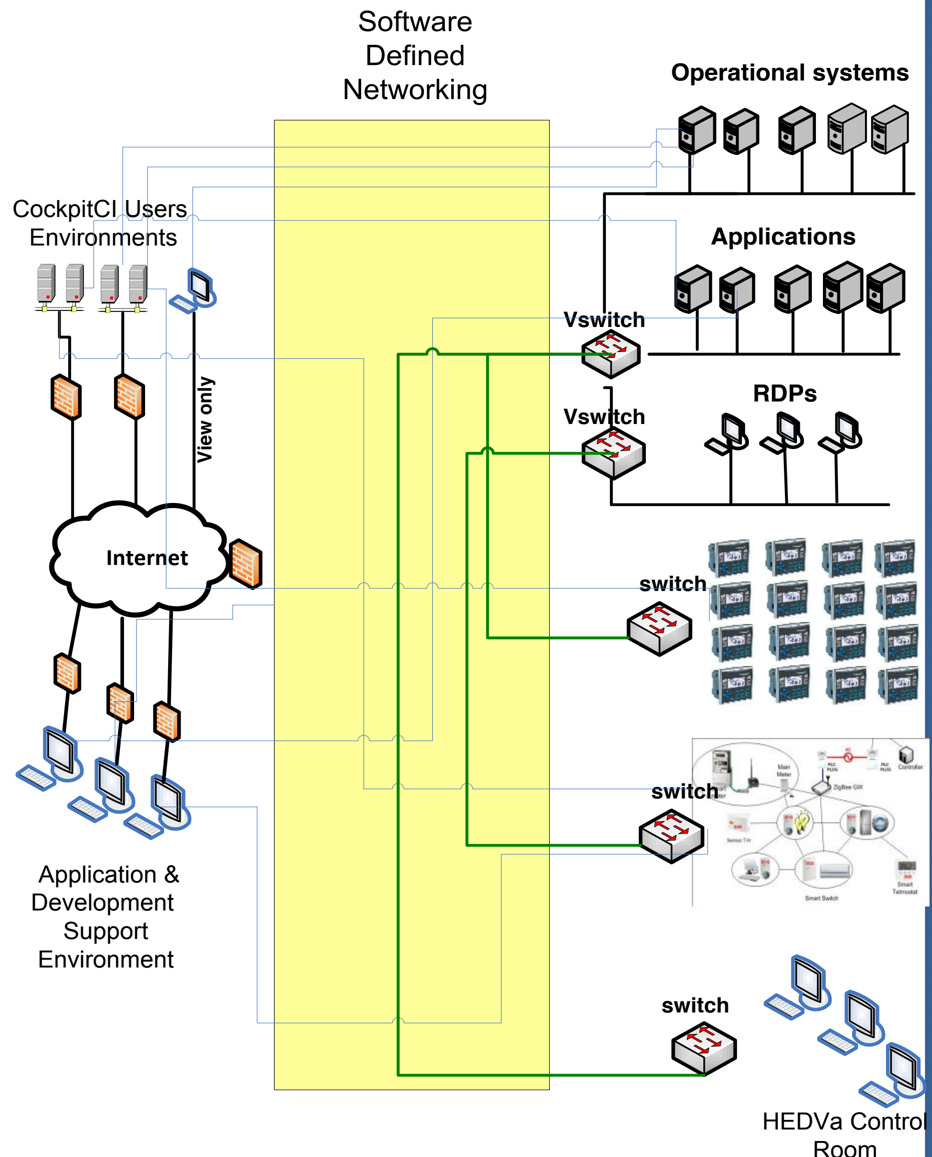


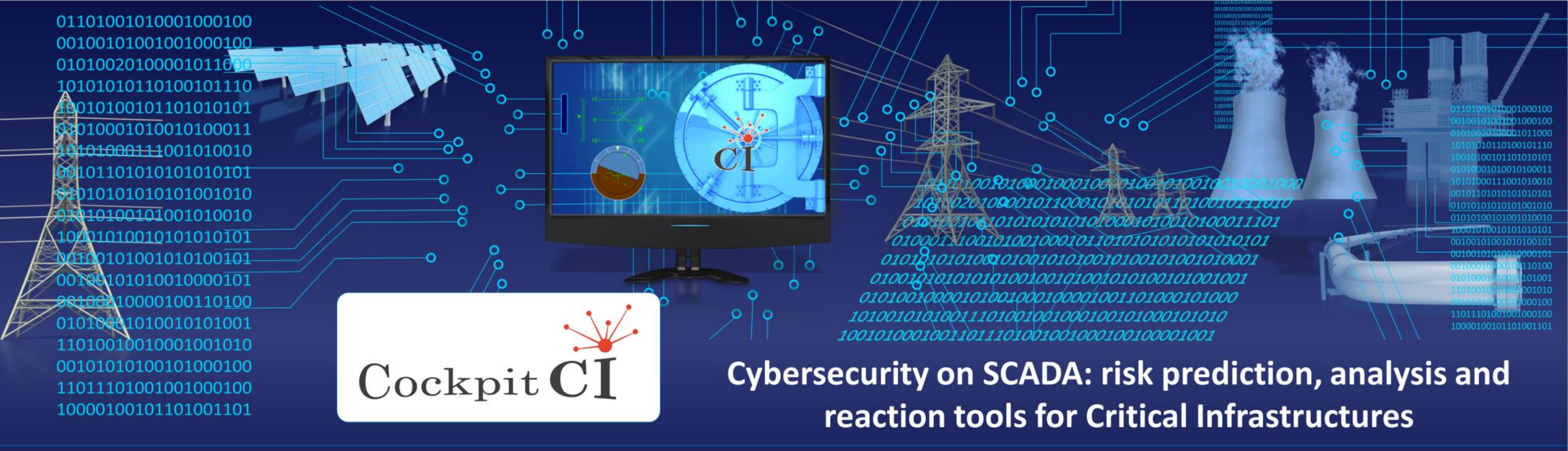
User Environment Development Vision

Use case



User Environment





Thank you for your attention

Information Society