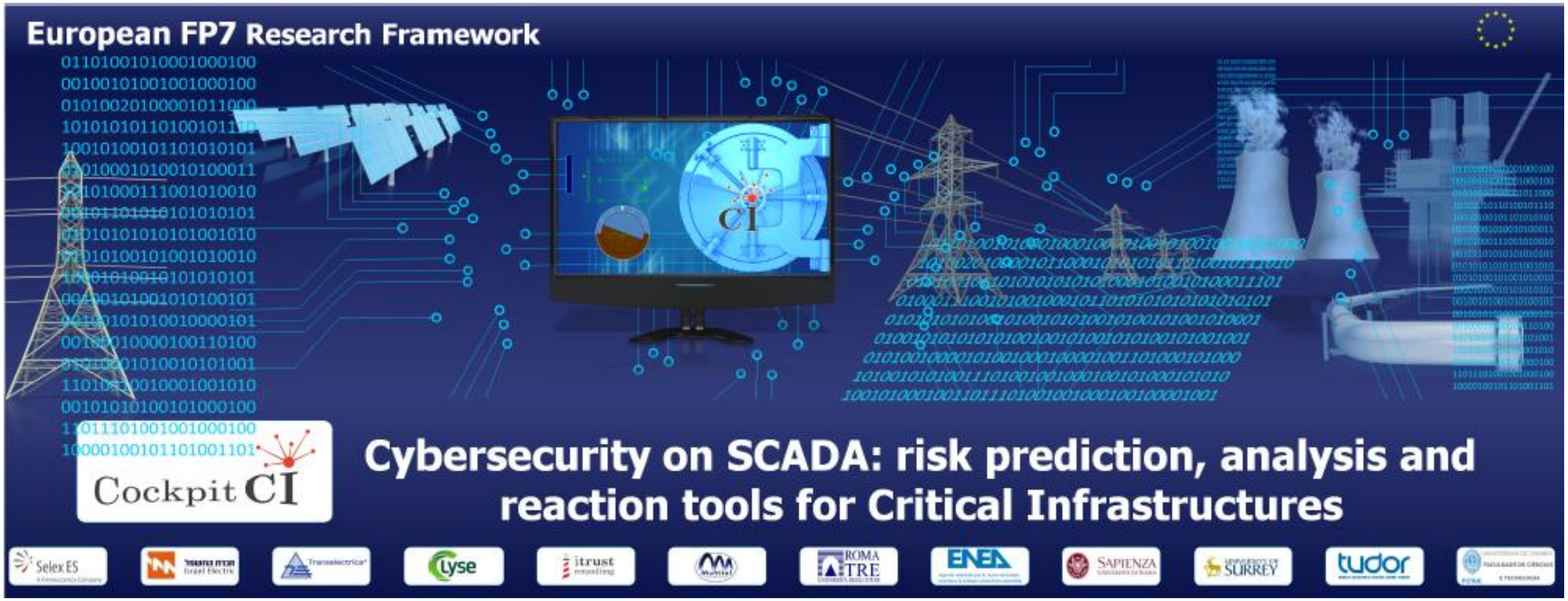

European FP7 Research Framework
Cockpit CI
Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures
Selex ES
Israel Electric
Transelectrica
Lyse
itrust
ROMA TRE
ENEA
SAPIENZA
UNIVERSITY OF SURREY
tudor

Luxembourg - March 10th, 2014

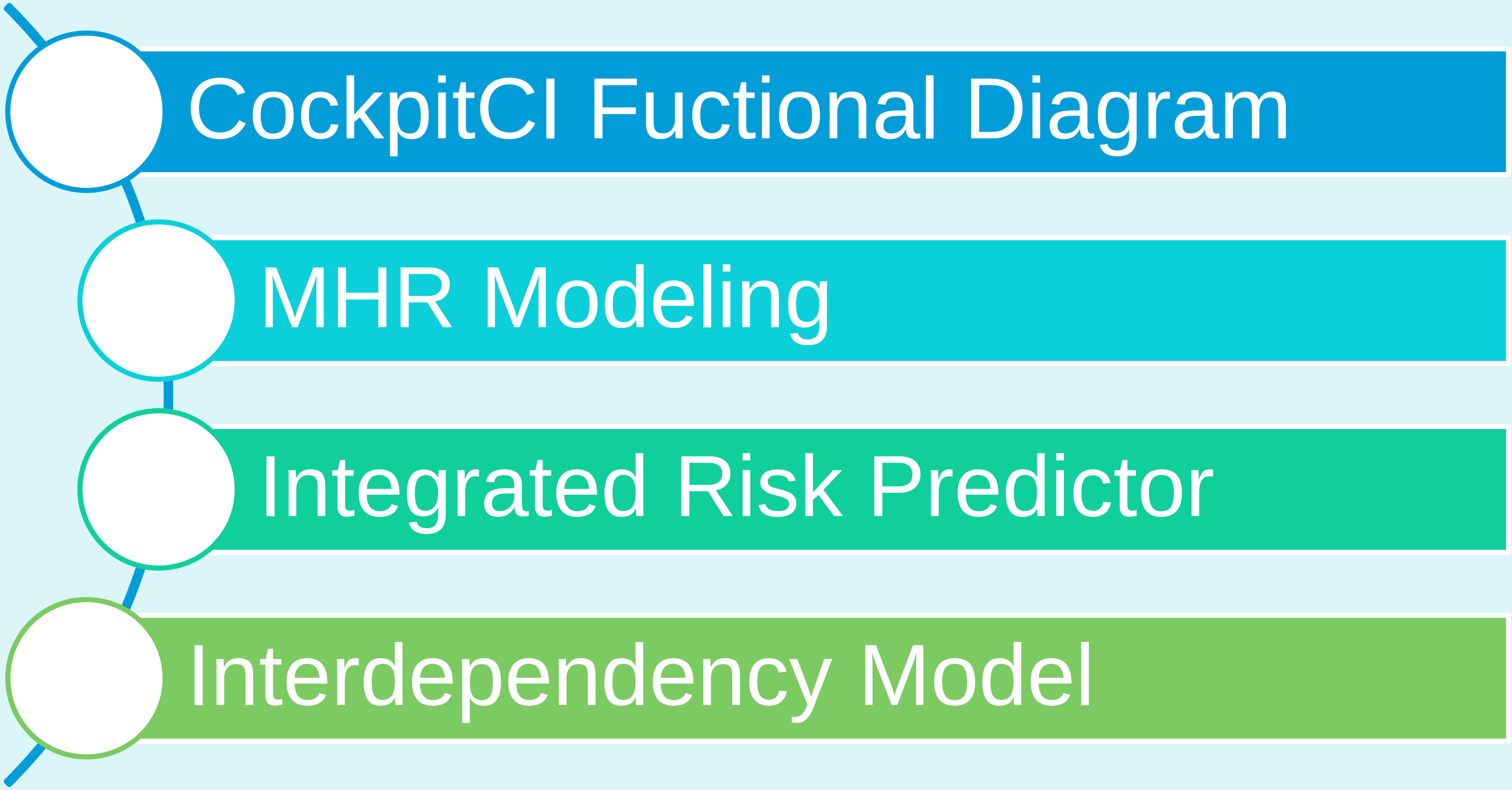
Integrated On-Line Risk Prediction System

Integrated On-Line Risk Prediction System

Cockpit CI

prof. Stefano Panzieri

ROMA TRE
UNIVERSITÀ DEGLI STUDI



CockpitCI Fuctional Diagram

MHR Modeling

Integrated Risk Predictor

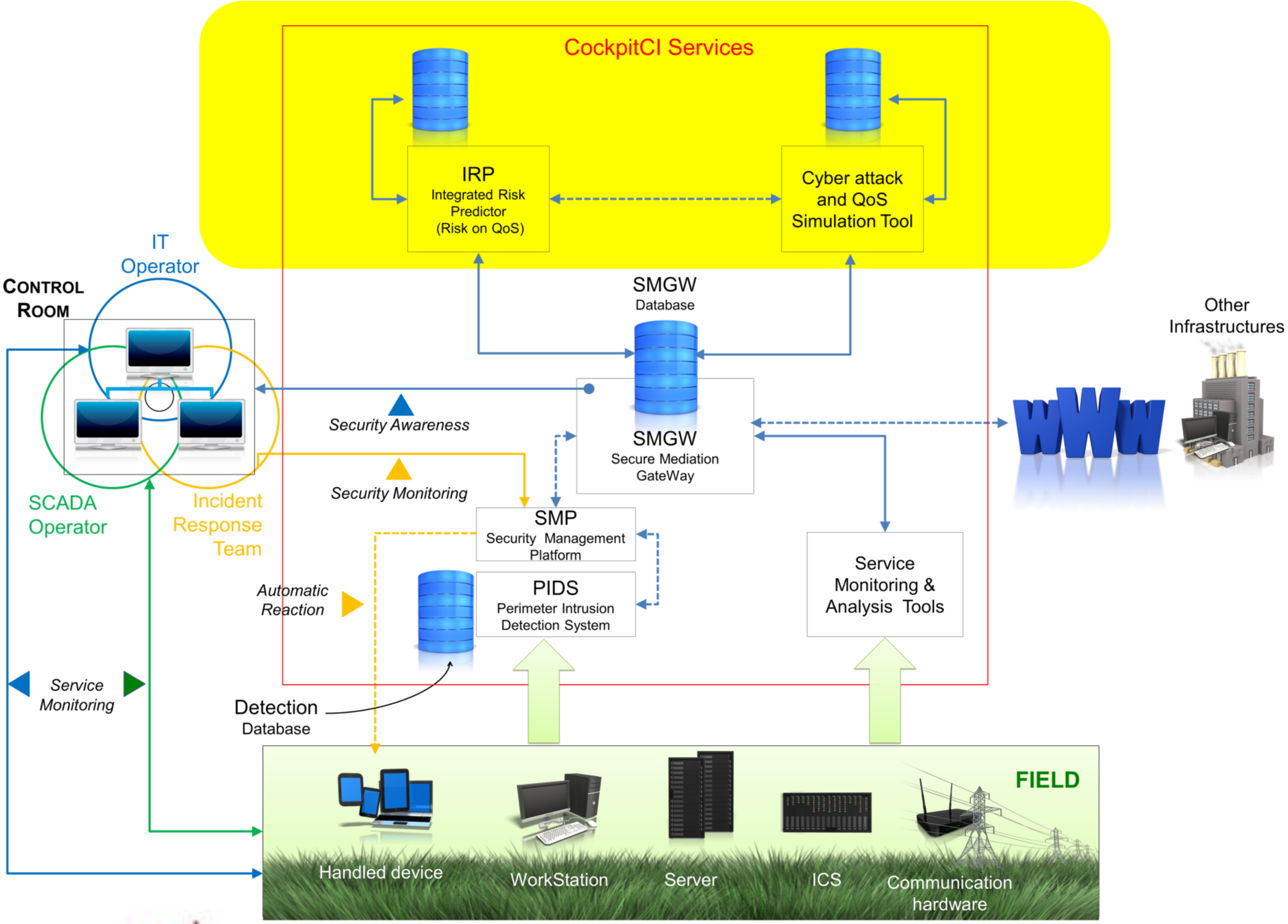
Interdependency Model

Outline

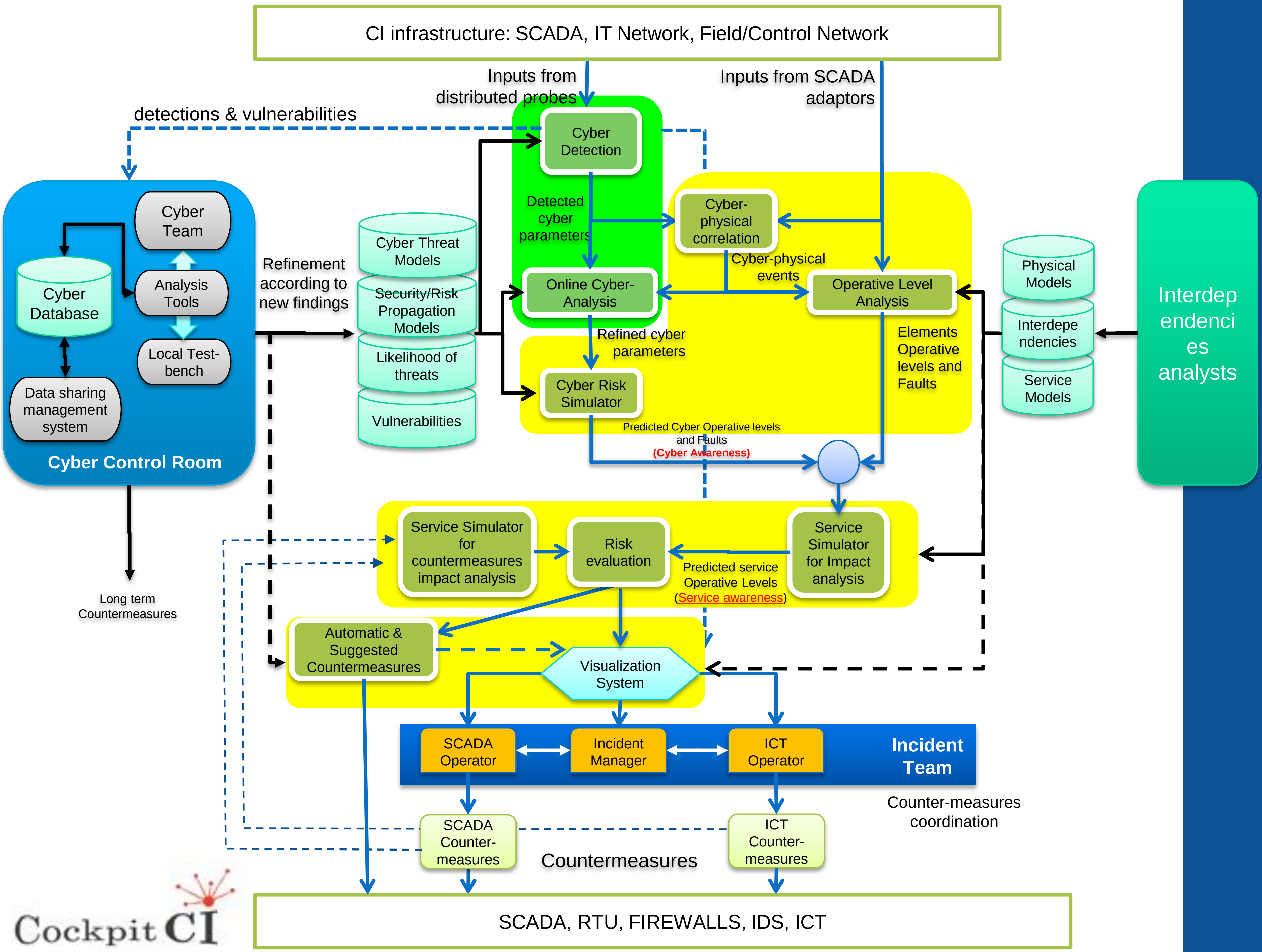
Cockpit CI

CockpitCI Functional Diagram

CockipCI



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

Cyber Risk Simulator

Elements Operative levels and Faults

Predicted Cyber Operative levels and Faults (Cyber Awareness)

Cyber Team

Analysis Tools

Cyber Database

Local Test-bench

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

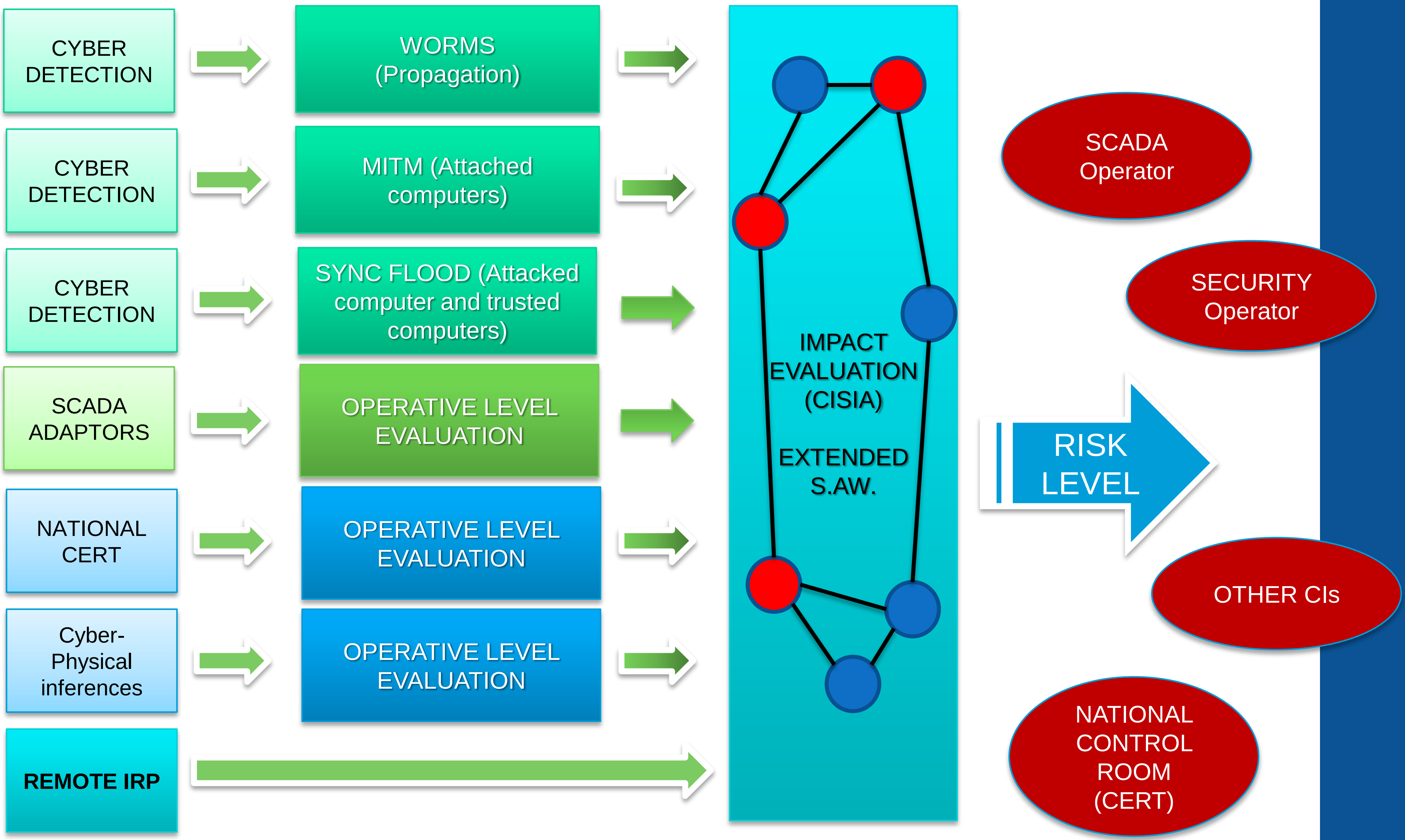
SCADA, RTU, FIREWALLS, IDS, ICT

Cockpit CI

Integrated Risk Predictor

Cockpit CI

FROM HOLISTIC ASSESSMENT TO COMBINED IMPACT EVALUATION



CYBER DETECTION → WORMS (Propagation) →

CYBER DETECTION → MITM (Attached computers) →

CYBER DETECTION → SYNC FLOOD (Attacked computer and trusted computers) →

SCADA ADAPTORS → OPERATIVE LEVEL EVALUATION →

NATIONAL CERT → OPERATIVE LEVEL EVALUATION →

Cyber-Physical inferences → OPERATIVE LEVEL EVALUATION →

REMOTE IRP →

IMPACT EVALUATION (CISIA)

EXTENDED S.AW.

RISK LEVEL

SCADA Operator

SECURITY Operator

OTHER CIs

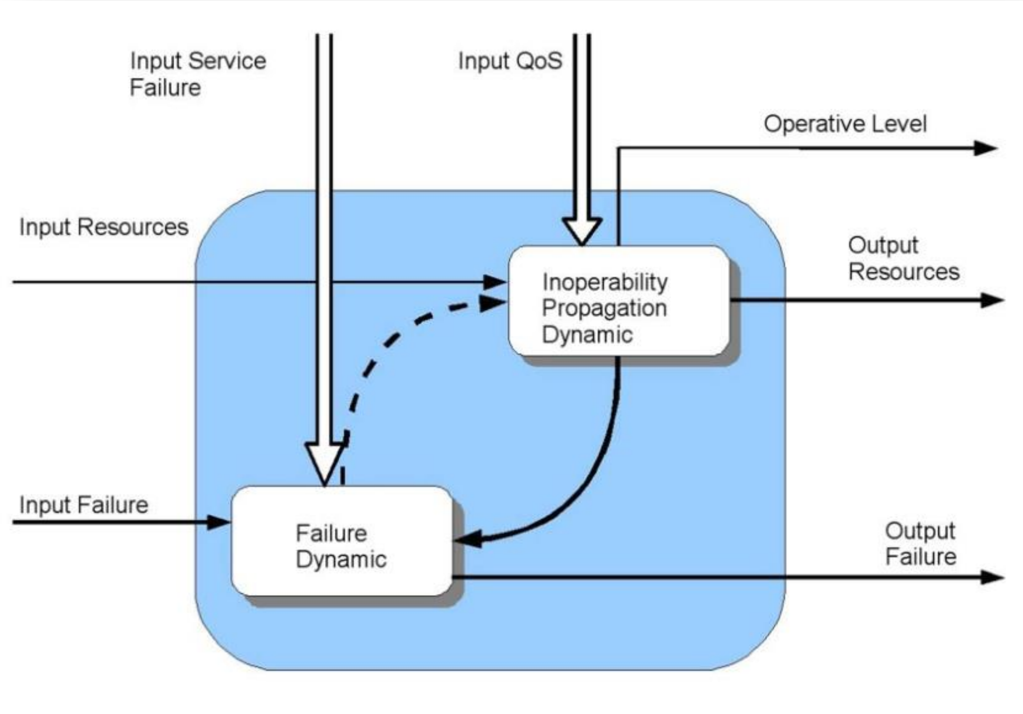
NATIONAL CONTROL ROOM (CERT)

Cockpit CI

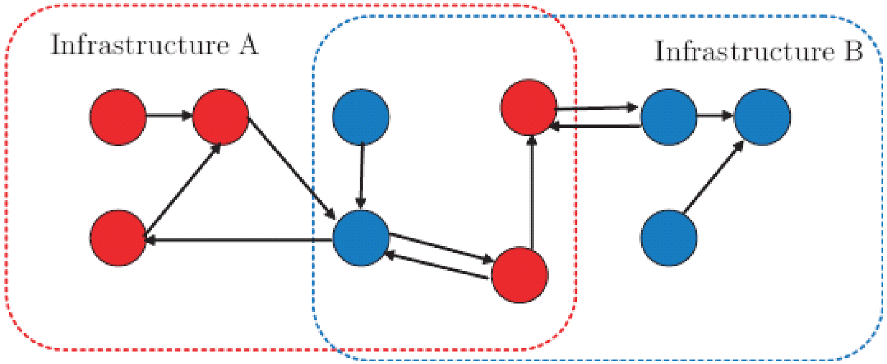
Holistic estimation

Reductionistic decomposition for cascading effects evaluation

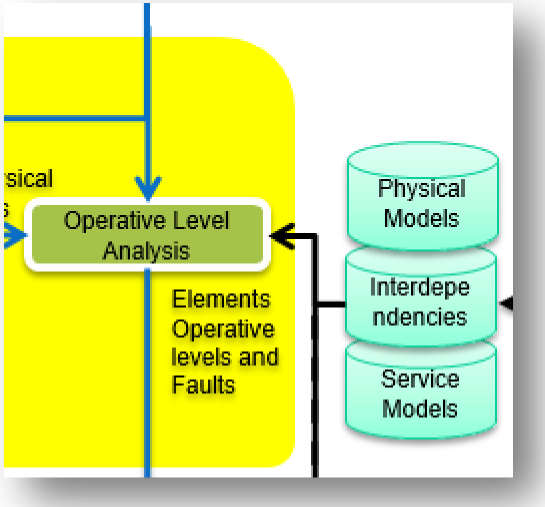
CISIA: an agent based simulator

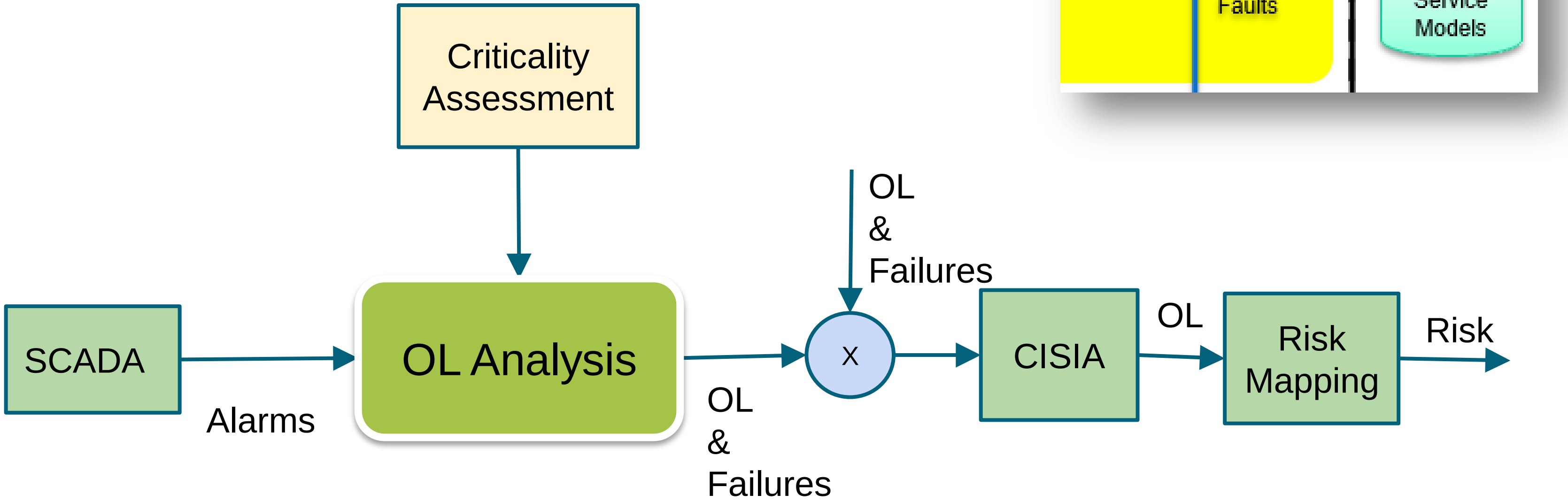


Reductionistic decomposition for cascading effects evaluation



SCADA ALARMS → OPERATIVE LEVELS & FAILURES





Criticality Assessment

SCADA

Alarms

OL Analysis

OL & Failures

OL & Failures

X

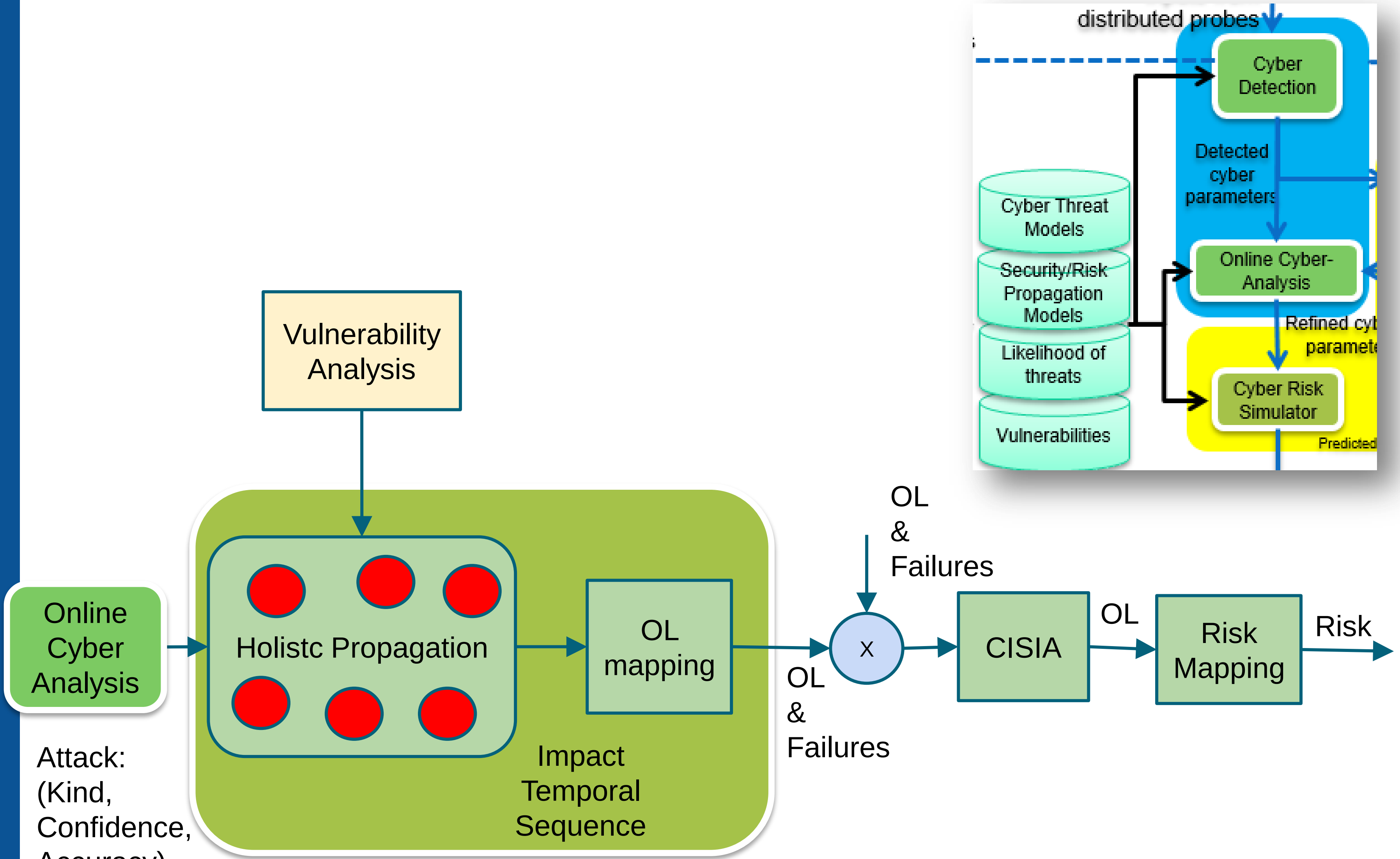
CISIA

OL

Risk Mapping

Risk

CYBER ALERTS → OPERATIVE LEVELS & FAILURES



distributed probes

Cyber Detection

Detected cyber parameters

Cyber Threat Models

Security/Risk Propagation Models

Likelihood of threats

Vulnerabilities

Online Cyber-Analysis

Refined cyb parame

Cyber Risk Simulator

Predicted

Vulnerability Analysis

Online Cyber Analysis

Holistc Propagation

OL mapping

Impact Temporal Sequence

OL & Failures

x

OL & Failures

CISIA

OL

Risk Mapping

Risk

Attack: (Kind, Confidence, Accuracy)

QoS Assessment Security Factors

Detection event : Abnormal event

Detection point: node 1

Specification : Server Windows XP
IP 192.168.2.2

Description: Installed Malware

Likelihood: Low

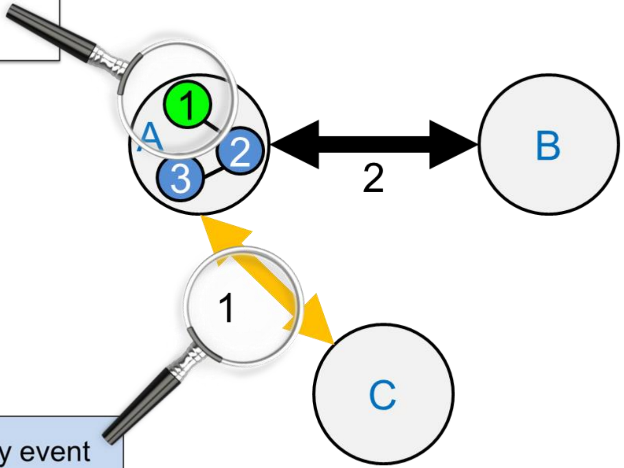
QASF

QoS Impact

Service delivered by: node 1

State: *Likelihood of Service Availability*

Up	70%
Degraded	25%
Down	5%



Detection event : Security event

Detection point: Link 1

Specification : Optic Fiber

Description: Disruption of Information

Likelihood: High

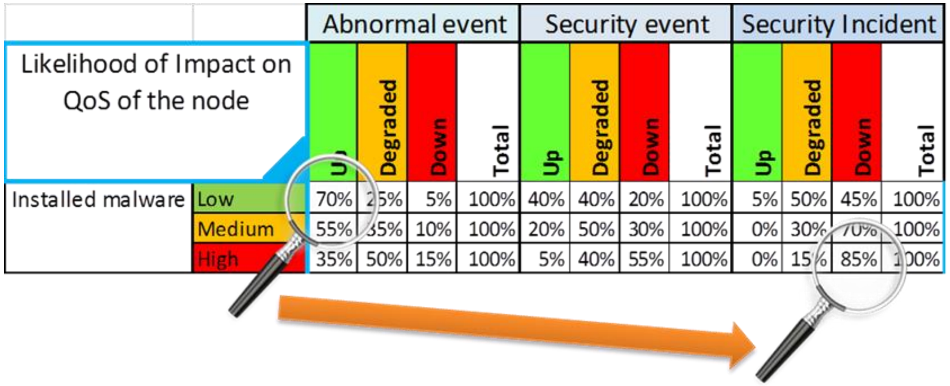
QASF

QoS Impact

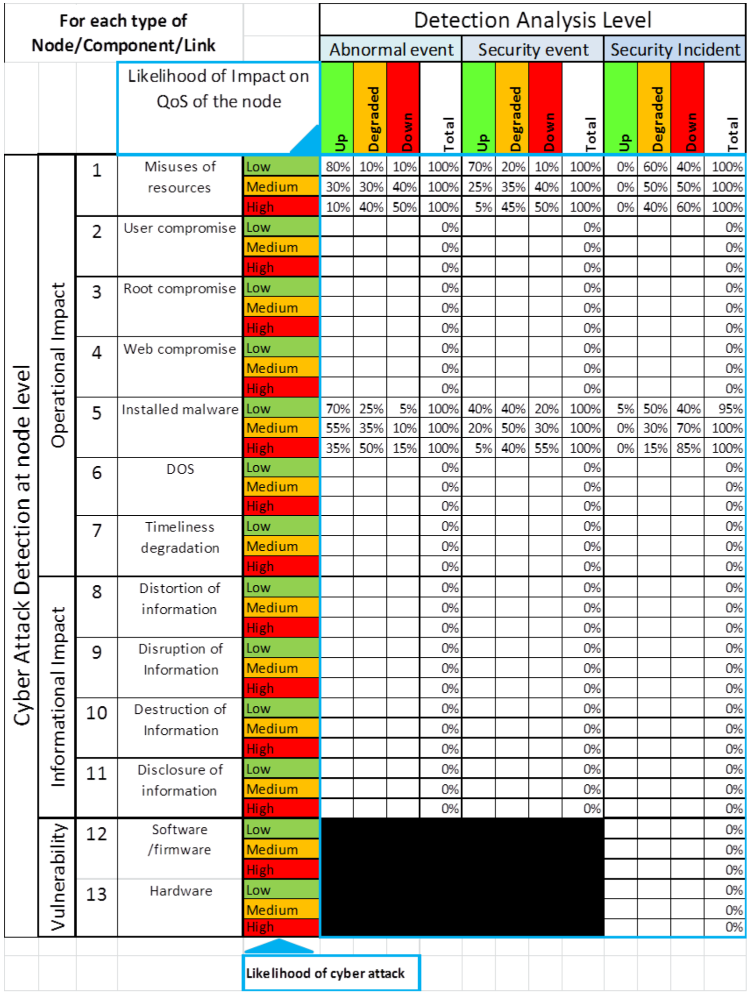
Service delivered by: link 1

State: *Likelihood of Service Availability*

Up	20%
Degraded	50%
Down	30%



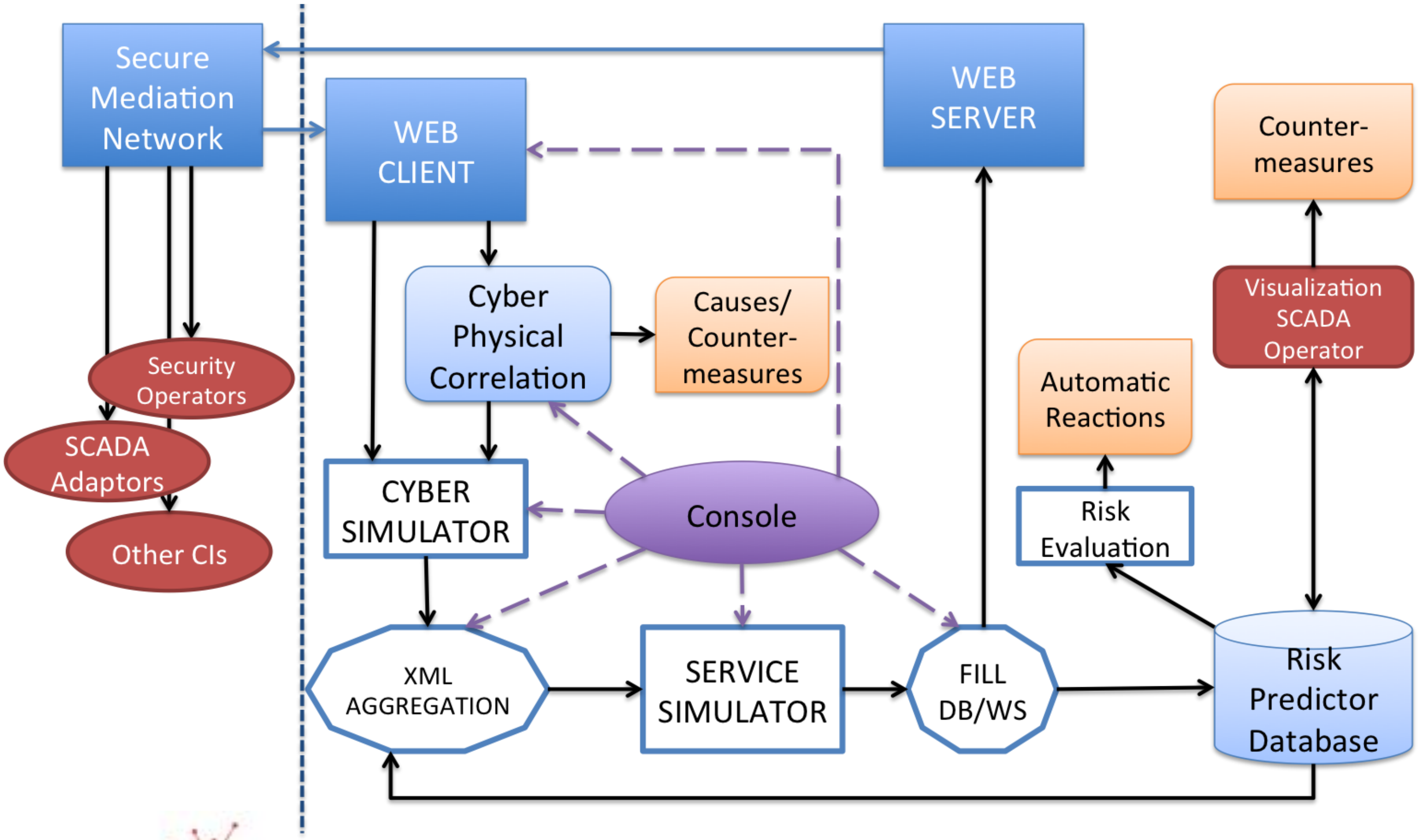
		Abnormal event				Security event				Security Incident			
Likelihood of Impact on QoS of the node		Up	Degraded	Down	Total	Up	Degraded	Down	Total	Up	Degraded	Down	Total
Installed malware	Low	70%	25%	5%	100%	40%	40%	20%	100%	5%	50%	45%	100%
	Medium	55%	35%	10%	100%	20%	50%	30%	100%	0%	30%	70%	100%
	High	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%
	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%
	Vulnerability	12	Software /firmware	Low												0%
				Medium												0%
				High												0%
		13	Hardware	Low												0%
				Medium												0%
				High												0%

Likelihood of cyber attack

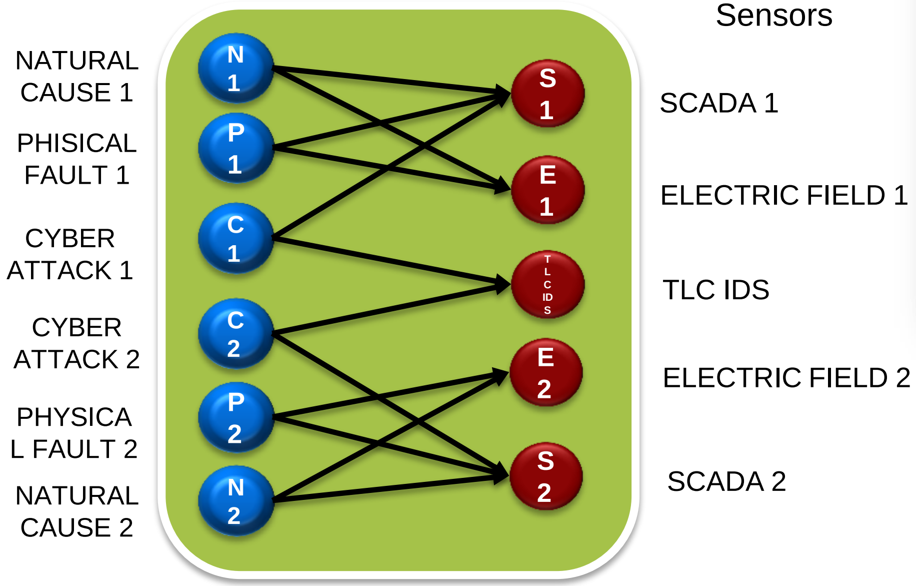
Risk Prediction Tool Architecture

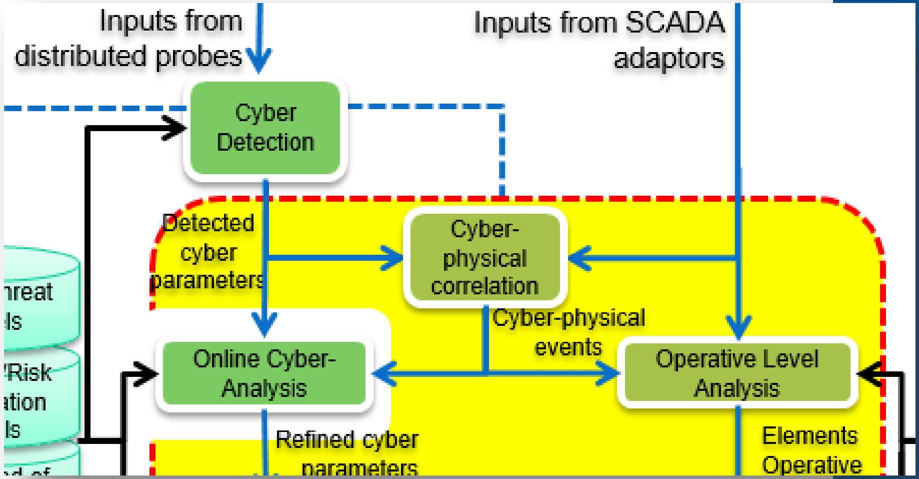


Cockpit CI

CYBER-PHYSICAL AWARENESS

Cyber-Physical Correlation





Cyber & Physical

From Cyber to Physical

WORMS (SIR **PROPAGATION**)

DOS ATTACK (PATHS and TARGETS)

HONEYPOT (NETWORK UNDER ATTACK)

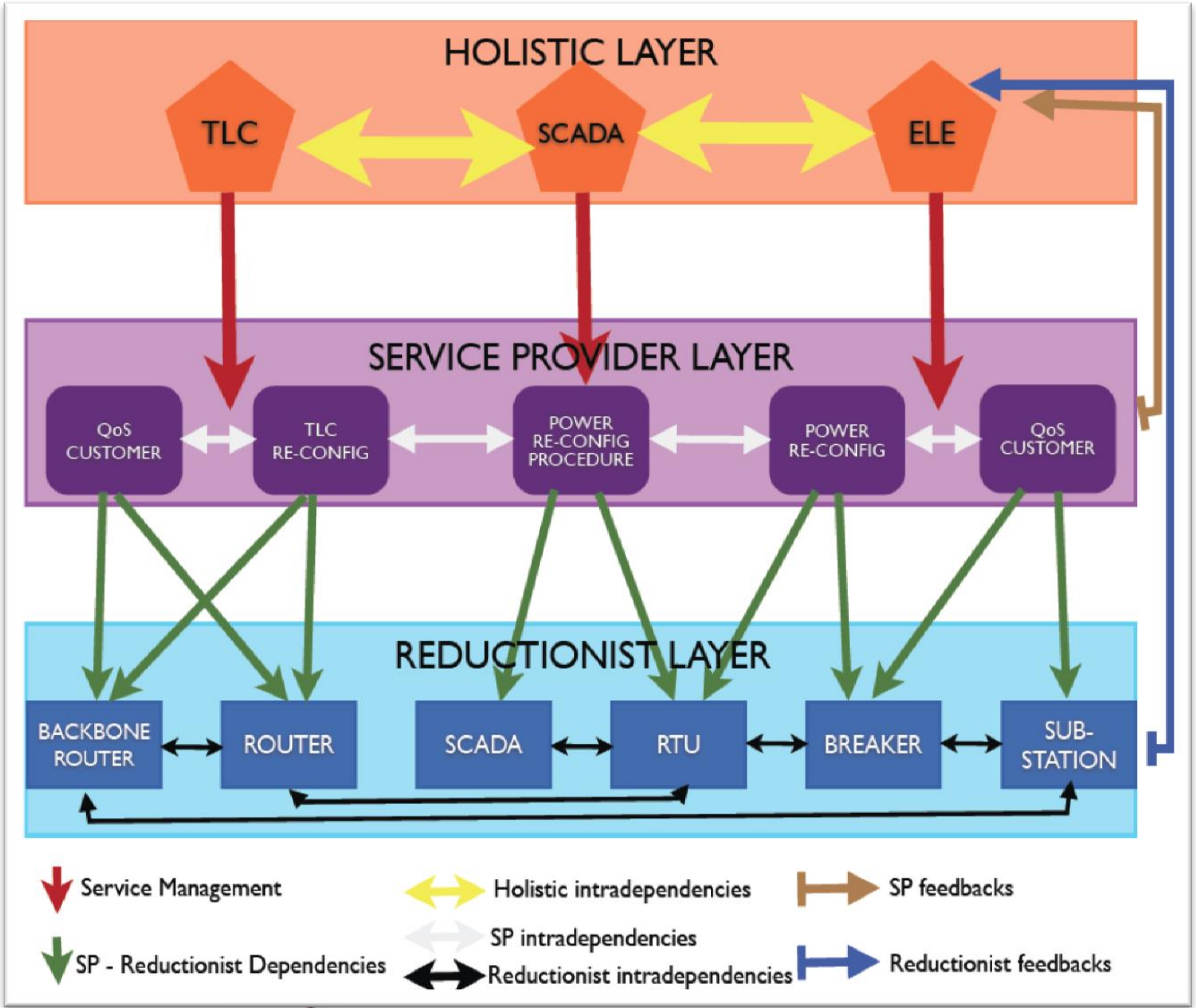
SHADOW RTUs (RTU ATTACKED)

Cockpit CI

CISIA IMPLEMENTATION INSIDE RISK PREDICTOR

MHR modelling

THE MIXED HOLISTIC-REDUCTIONISTIC MODELLING PERSPECTIVE



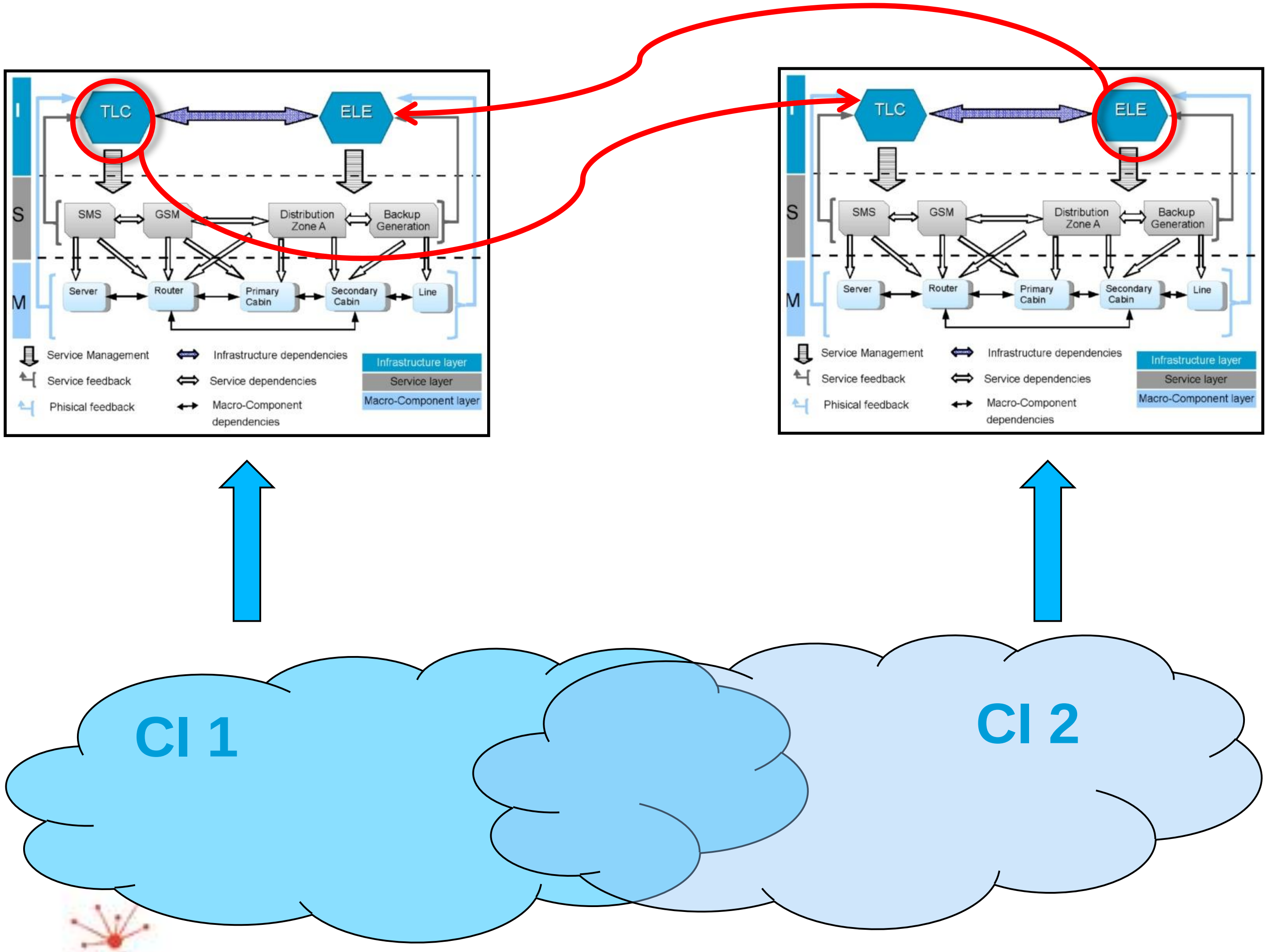
Behaviours (physical or logical or political) not emerging from Reductionistic layer

Expressions of both holistic and reductionistic models

Intra-Inter-Infrastructure homogeneous layer capturing interdependencies

Cockpit CI

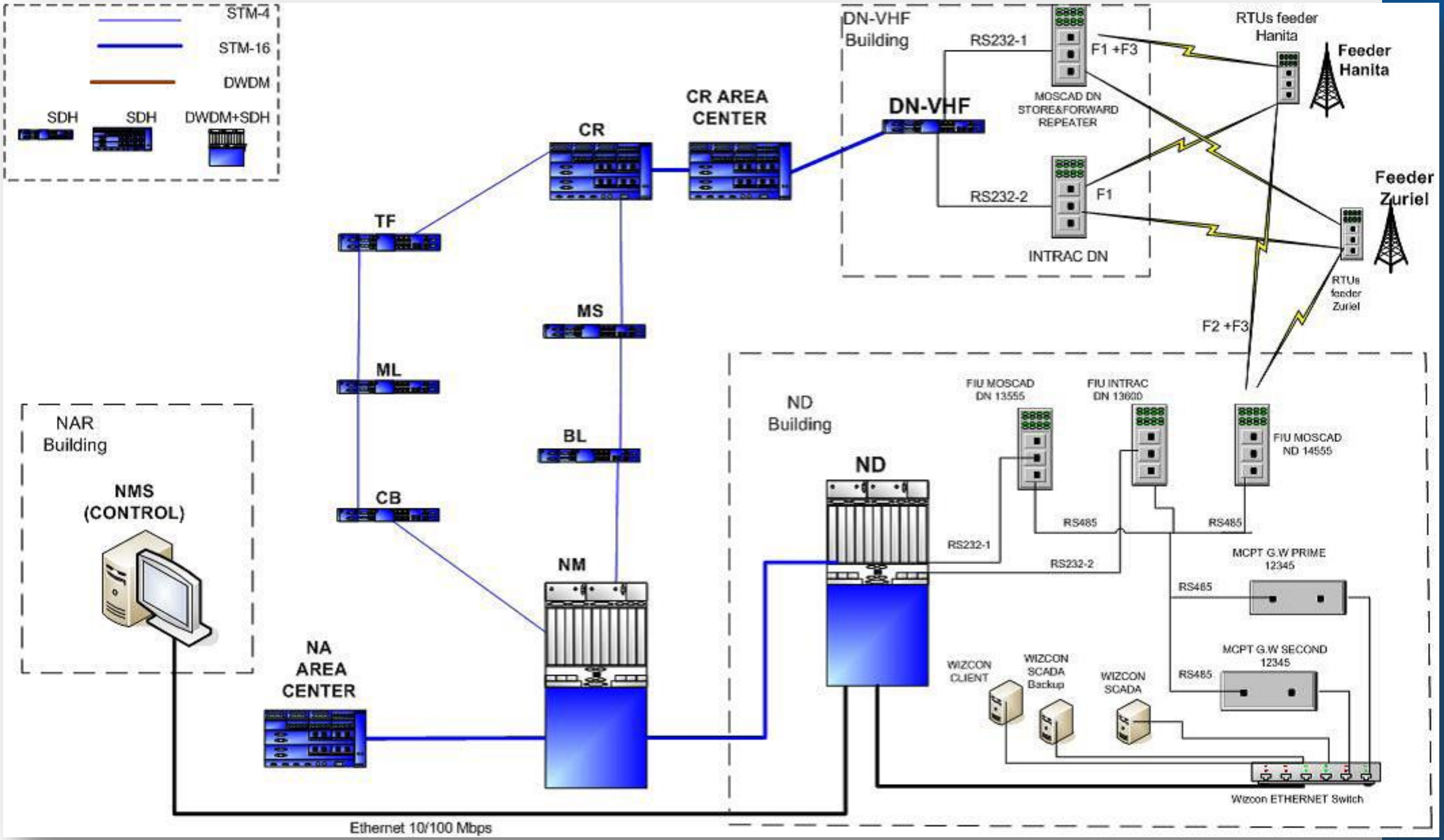
Distributed Estimator



Physical / Logical / Geographic / Cyber

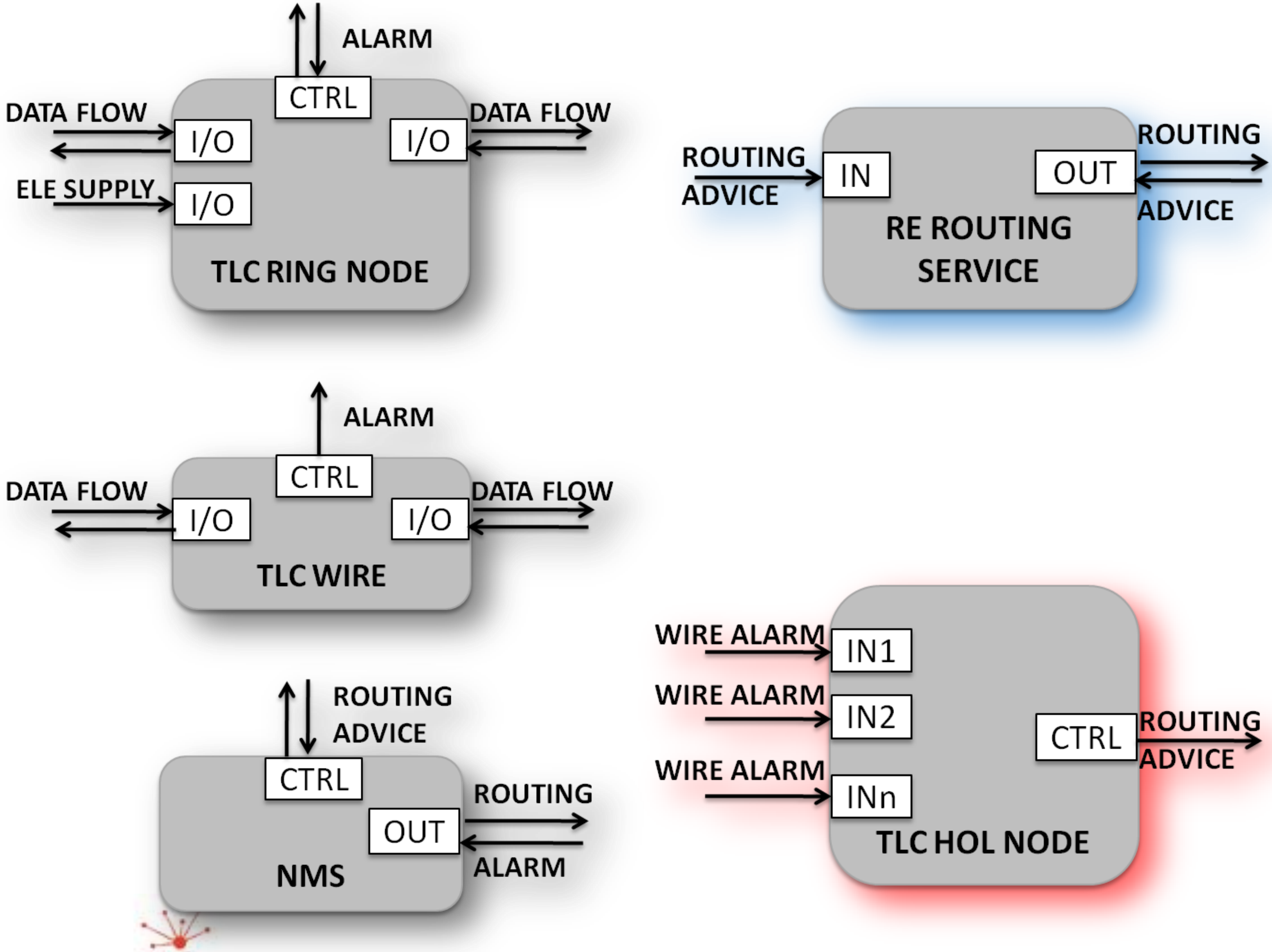
Interdependency Model

Interconnected telecommunication and SCADA network



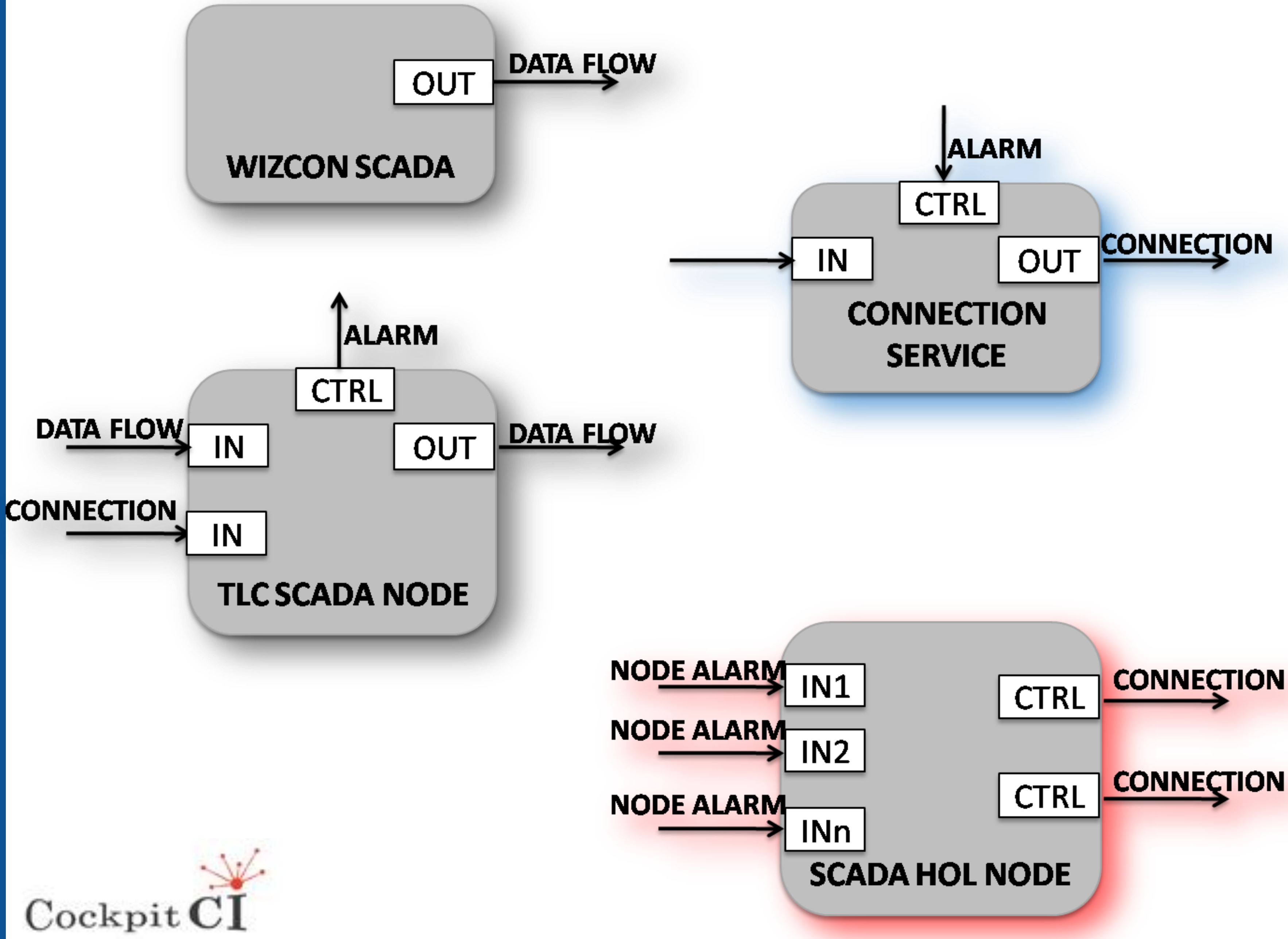
Cockpit CI

CISIA TLC Entities



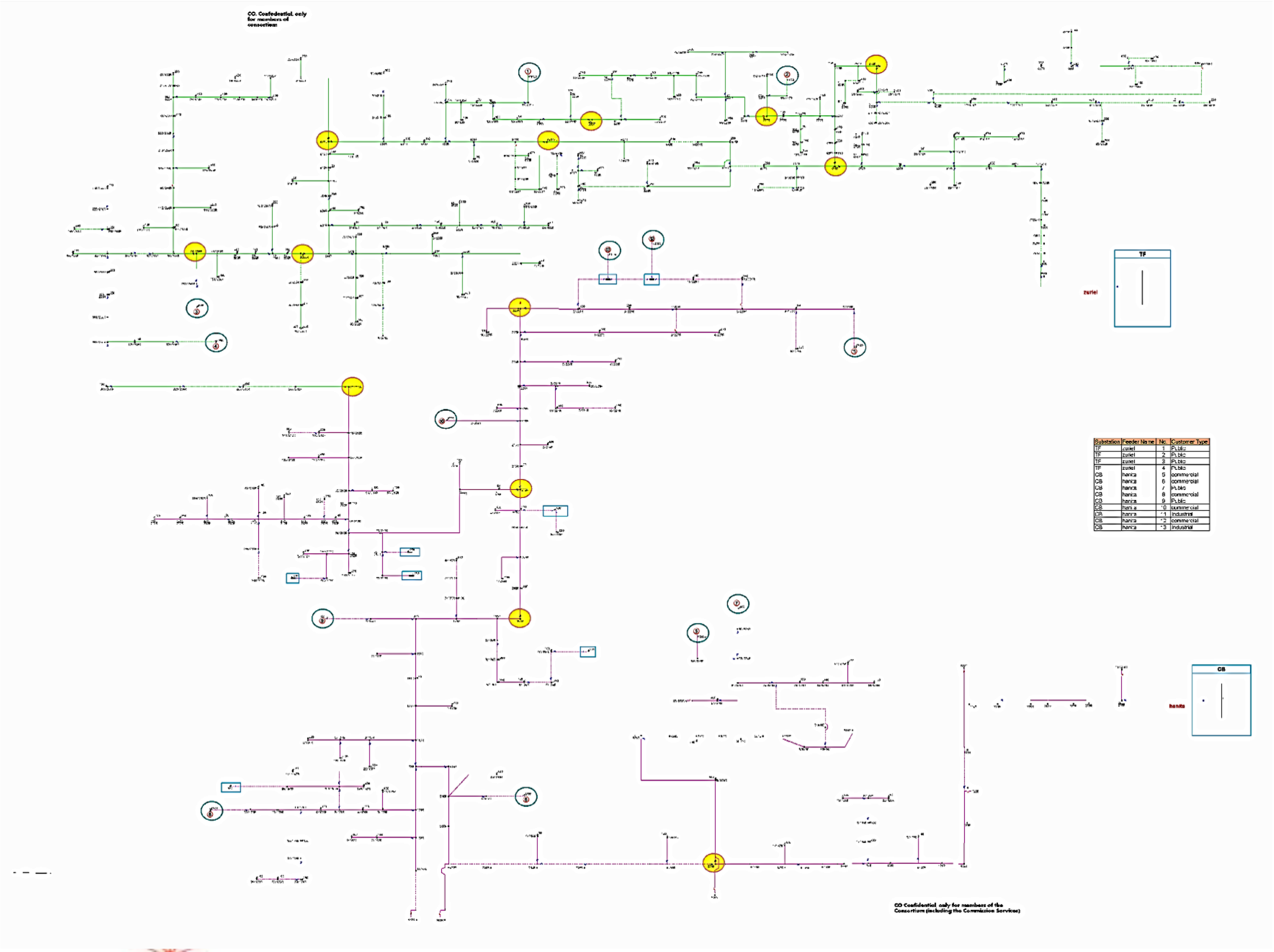
Cockpit CI

CISIA SCADA Entities



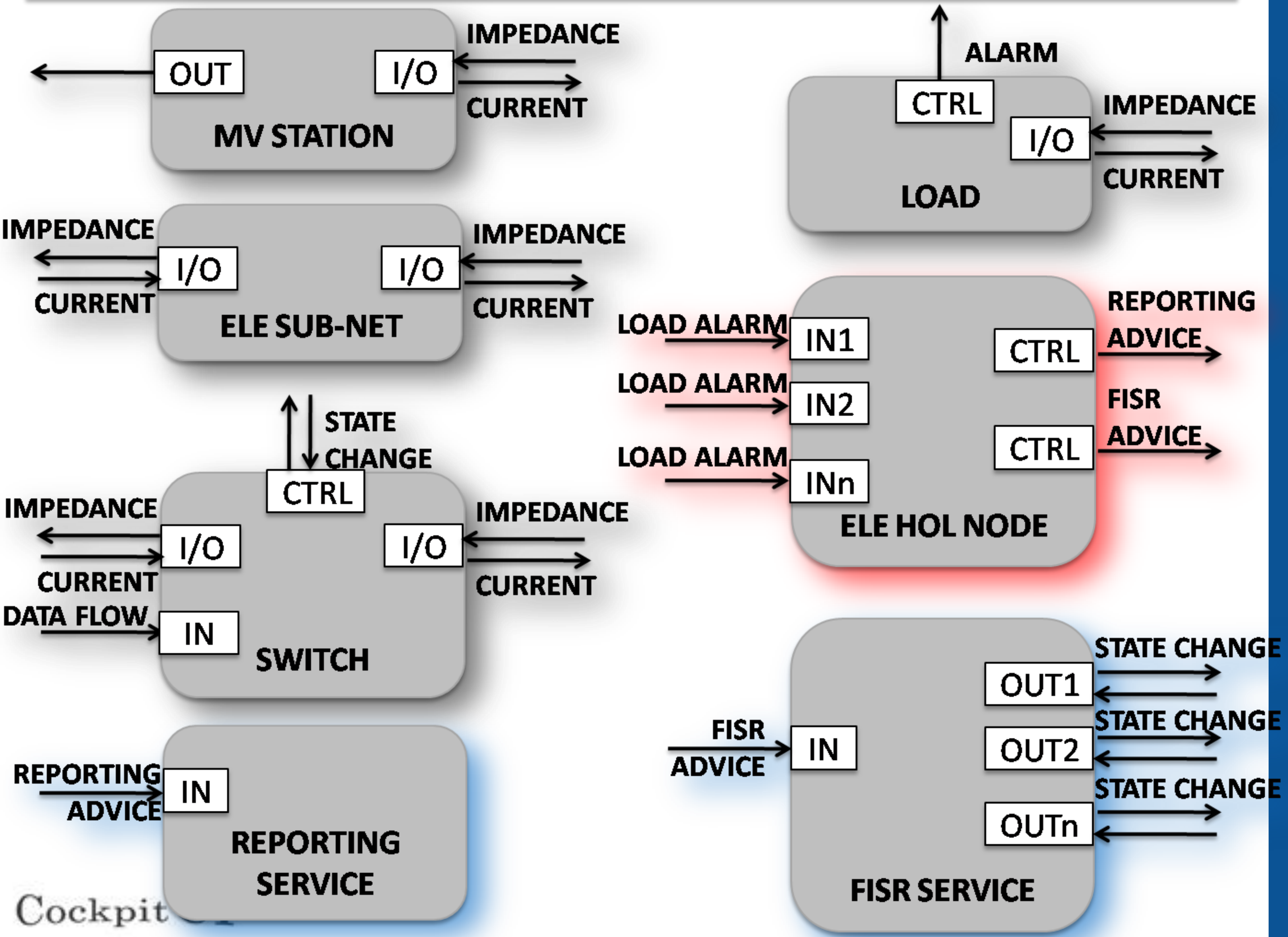
Cockpit CI

Medium Voltage electric grid


CO. Confidential, only for members of consortium
TF
zuriel
CB
hanita
1
2
3
4
5
6
7
8
9
10
11
12
13
CO Confidential, only for members of the Consortium (including the Commission Services)

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

CISIA ELE Entities



MV STATION
OUT
I/O
IMPEDANCE
CURRENT

ELE SUB-NET
IMPEDANCE
CURRENT
I/O
I/O
IMPEDANCE
CURRENT

SWITCH
STATE CHANGE
CTRL
IMPEDANCE
CURRENT
I/O
I/O
IMPEDANCE
CURRENT
DATA FLOW
IN

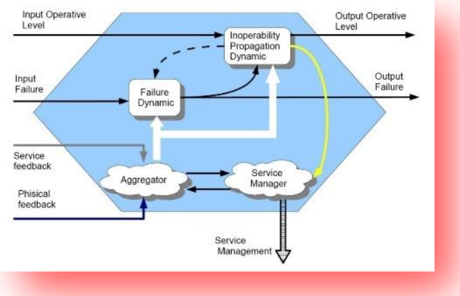
REPORTING SERVICE
REPORTING ADVICE
IN

LOAD
ALARM
CTRL
I/O
IMPEDANCE
CURRENT

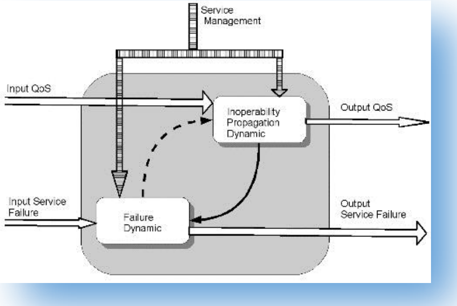
ELE HOL NODE
LOAD ALARM
IN1
LOAD ALARM
IN2
LOAD ALARM
INn
CTRL
REPORTING ADVICE
CTRL
FISR ADVICE

FISR SERVICE
FISR ADVICE
IN
OUT1
STATE CHANGE
OUT2
STATE CHANGE
OUTn
STATE CHANGE

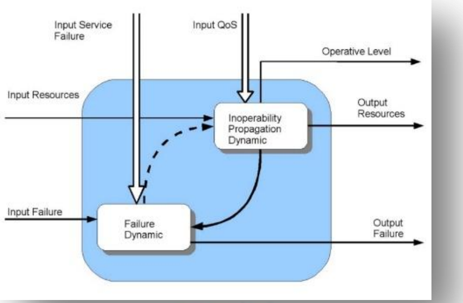
All the entities (202)



- TLC HOL NODE
- SCADA HOL NODE
- ELE HOL NODE

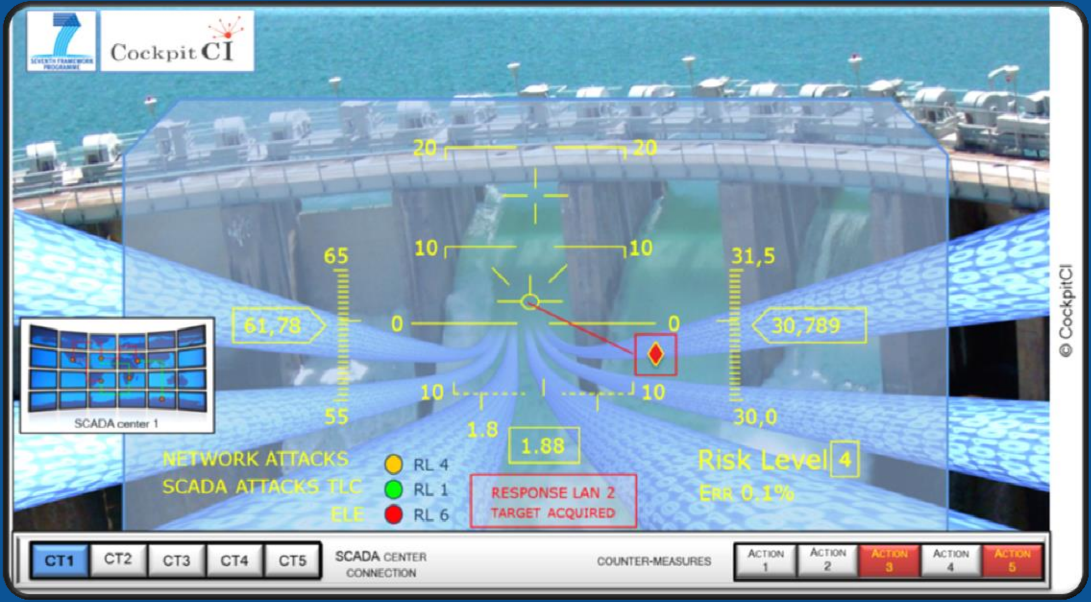


- RE_ROUTING SERVICE
- CONNECTION SERVICE
- REPORTING SERVCE
- FISR SERVICE



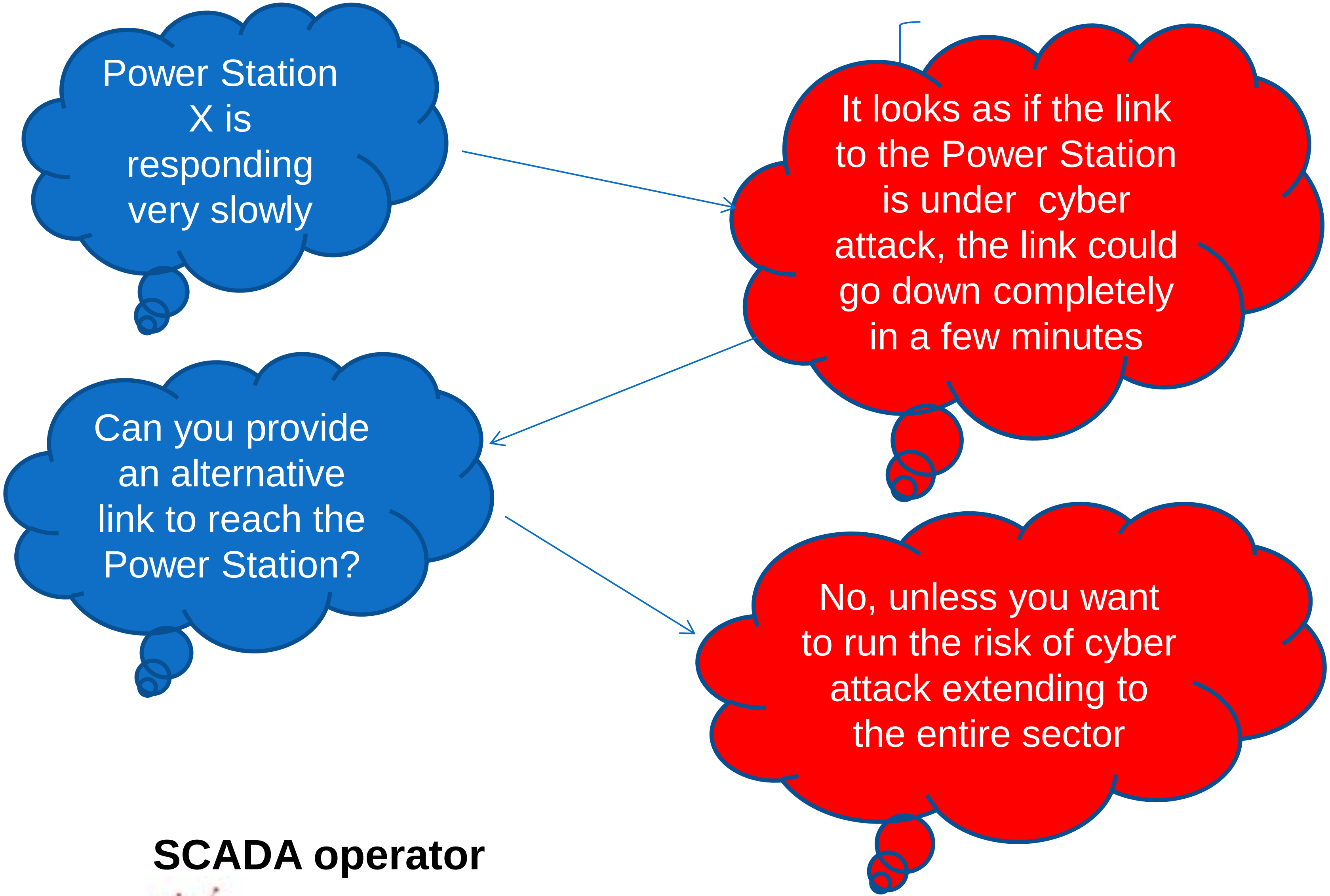
- TLC RING NODE
- TLC WIRE
- NMS
- WIZCON SCADA
- TLC SCADA NODE
- MV STATION
- ELE SUB-NET
- SWITCH
- LOAD

- 4 are the steps executed by CISIA
- 2184 are the total elements saved in the DB (OIs and Faults)
- 4 are the crisp values for each record in the DB
- 425 KB is the dimension of the output file for CISIA
- 5 are the input file for CISIA
- 326 KB is the overall amount of the input file for CISIA



Thank you for your attention

CockpitCI Operators: a possible dialogue (1)



Power Station X is responding very slowly

It looks as if the link to the Power Station is under cyber attack, the link could go down completely in a few minutes

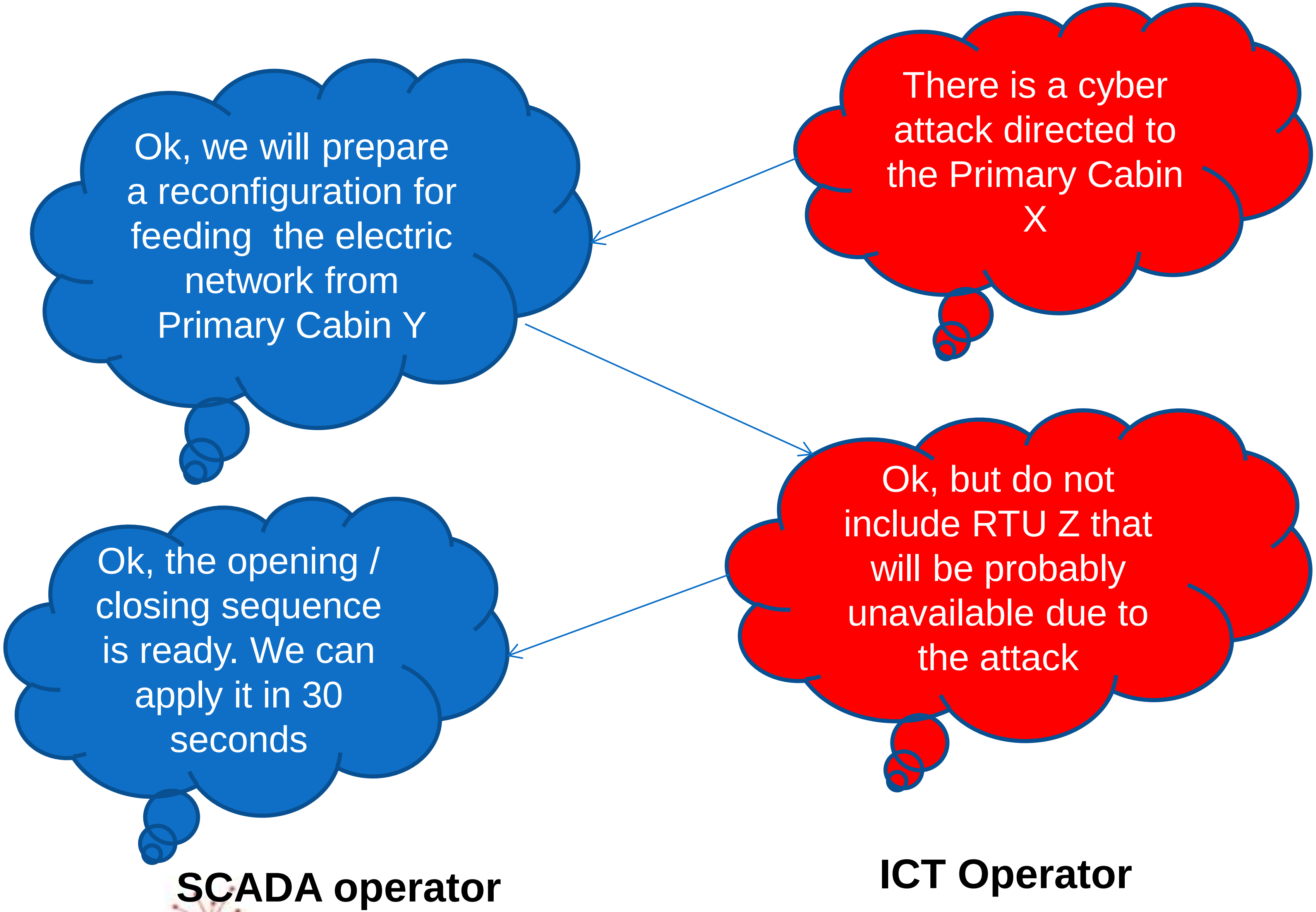
Can you provide an alternative link to reach the Power Station?

No, unless you want to run the risk of cyber attack extending to the entire sector

SCADA operator

ICT Operator

CockpitCI Operators: a possible dialogue (2)



There is a cyber attack directed to the Primary Cabin X

Ok, we will prepare a reconfiguration for feeding the electric network from Primary Cabin Y

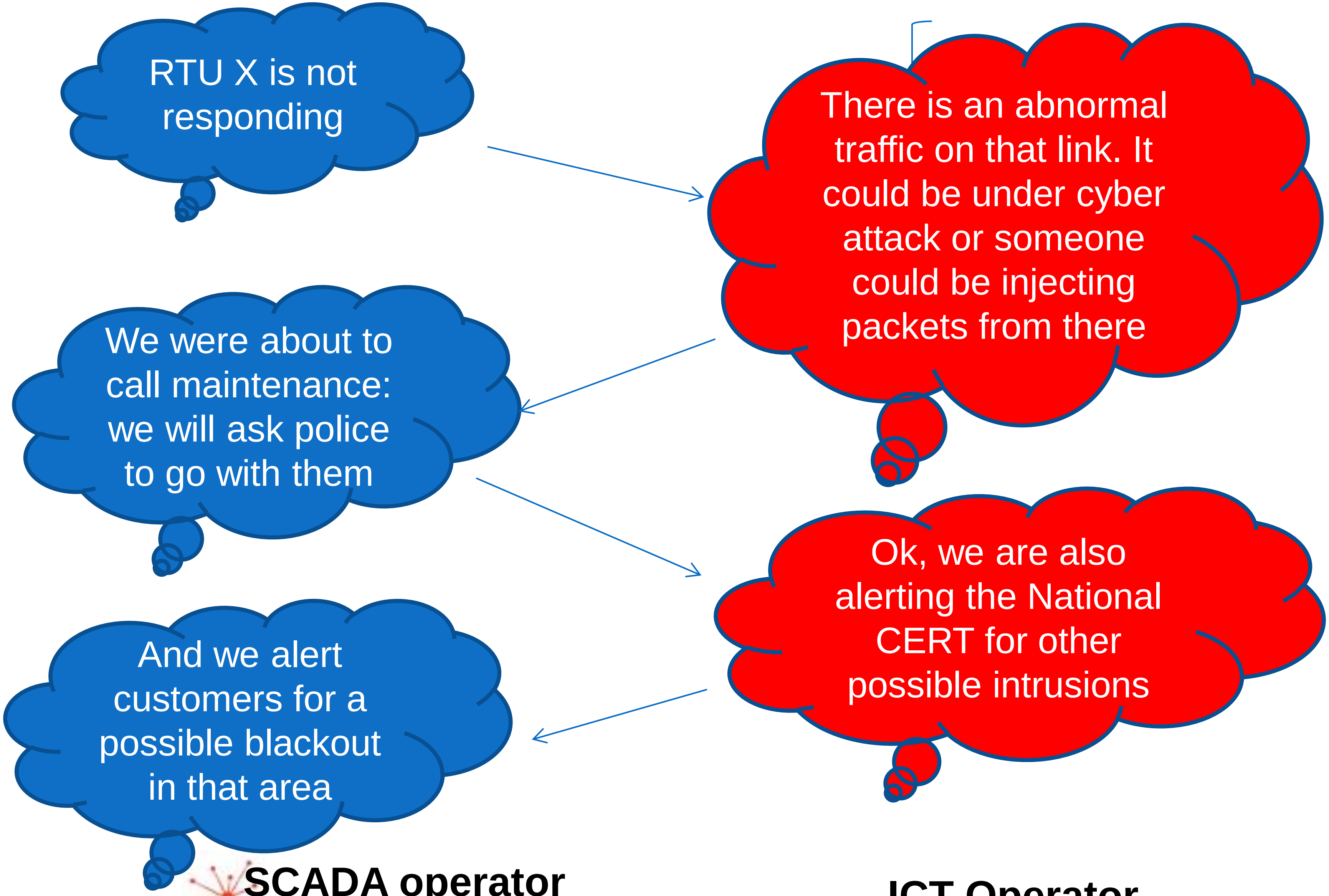
Ok, but do not include RTU Z that will be probably unavailable due to the attack

Ok, the opening / closing sequence is ready. We can apply it in 30 seconds

SCADA operator

ICT Operator

CockpitCI Operators: a possible dialogue (3)



RTU X is not responding

There is an abnormal traffic on that link. It could be under cyber attack or someone could be injecting packets from there

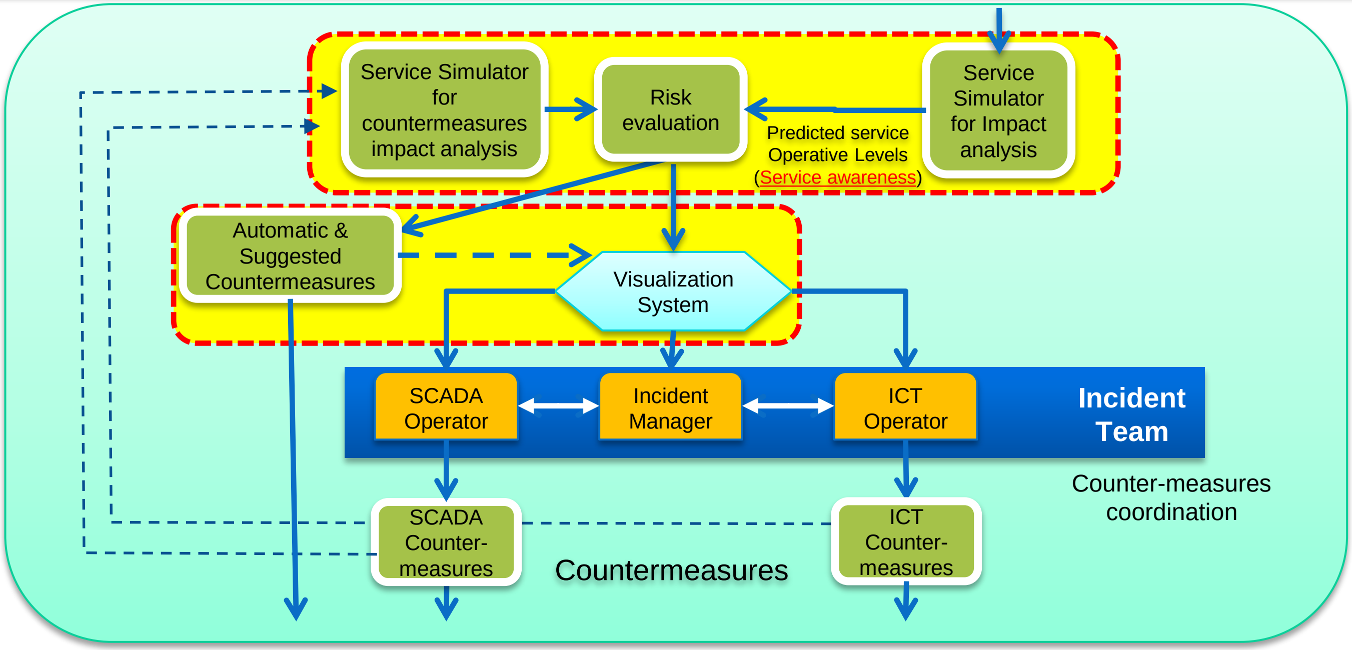
We were about to call maintenance: we will ask police to go with them

Ok, we are also alerting the National CERT for other possible intrusions

And we alert customers for a possible blackout in that area

Cockpit CI

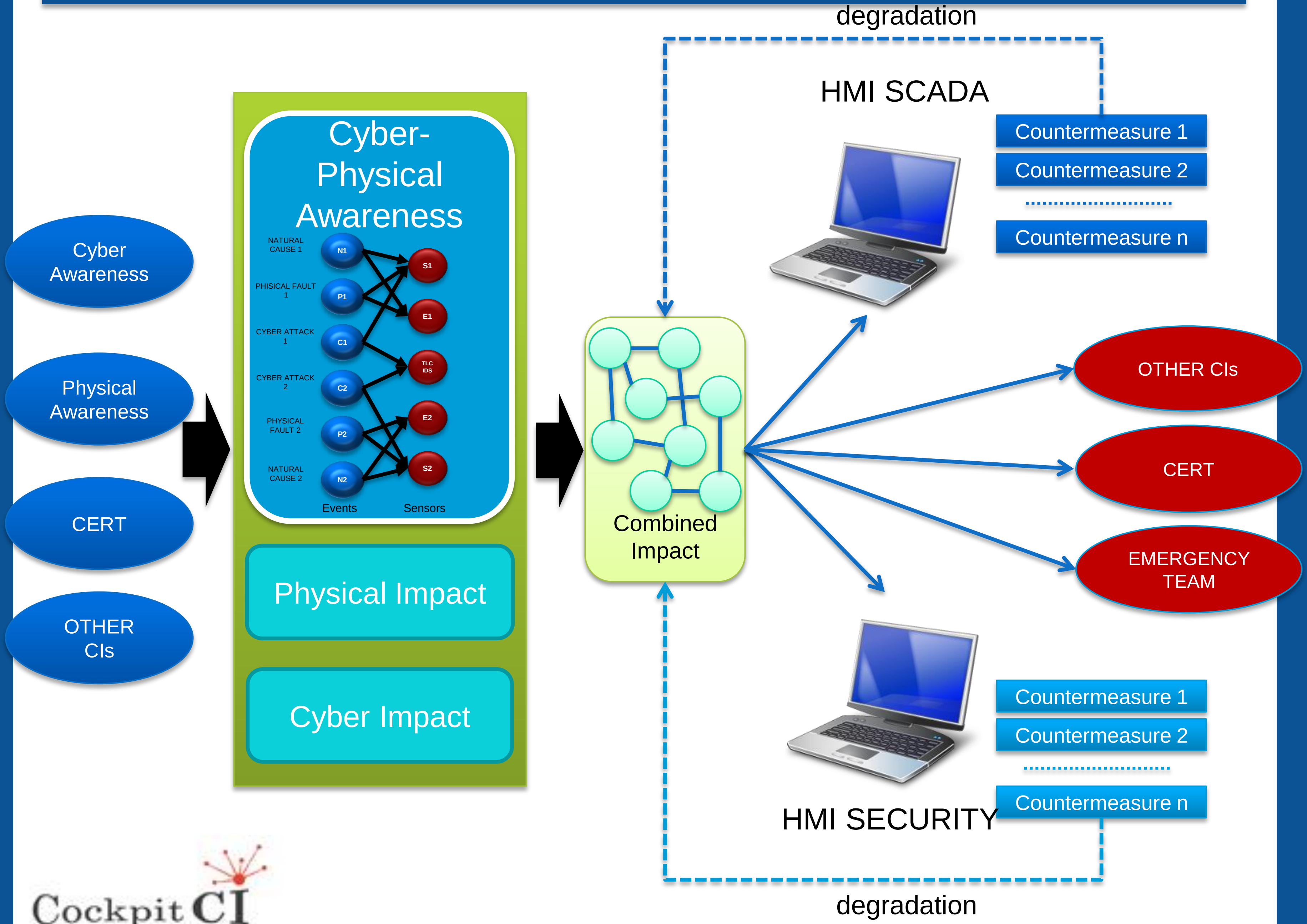
Countermeasures


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
Countermeasures
ICT Counter-measures

- Operators countermeasures:
  - Firewall reconfiguration for network isolation
  - Augmented security for electric network
  - ELE network reconfiguration (unusual)
- Automatic countermeasures:
  - RTU alerting
- Suggested countermeasures:
  - possible network reconfiguration for risk reduction (TLC & ELE)

Cockpit CI

COUNTERMEASURES



Cyber Awareness

Physical Awareness

CERT

OTHER CIs

Cyber-Physical Awareness

Physical Impact

Cyber Impact

Combined Impact

degradation

HMI SCADA

Countermeasure 1

Countermeasure 2

....

Countermeasure n

OTHER CIs

CERT

EMERGENCY TEAM

Countermeasure 1

Countermeasure 2

....

Countermeasure n

HMI SECURITY

degradation

Cockpit CI