THALES

IACS cybersecurity certification: Results from the ERNCIP project

PAUL THÉRON, THALES COMMUNICATIONS & SÉCURITÉ

2ND ERNCIP CONFERENCE - 16 APRIL 2015 - BRUSSELS

Introduction

The ERNCIP Thematic Group (TG) "*Case studies for the cybersecurity of Industrial Automation & Control Systems*" :

- A research project defining directions
- Not a proposal of an applicable standard

It was to deliver :

- Case studies
- IACS Cybersecurity Certification Principles
- Research and action roadmap

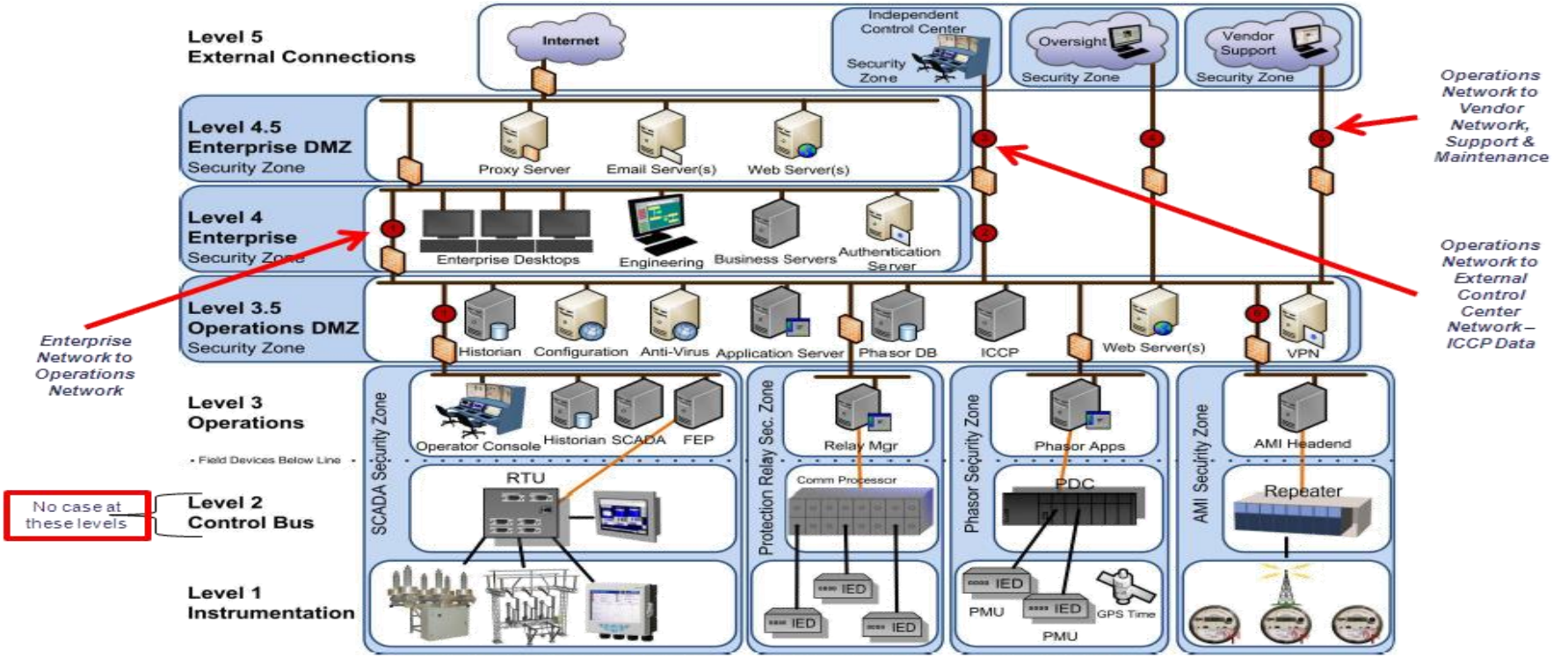
Started in January 2014

Ended in November 2014

Published in February 2015

THALES

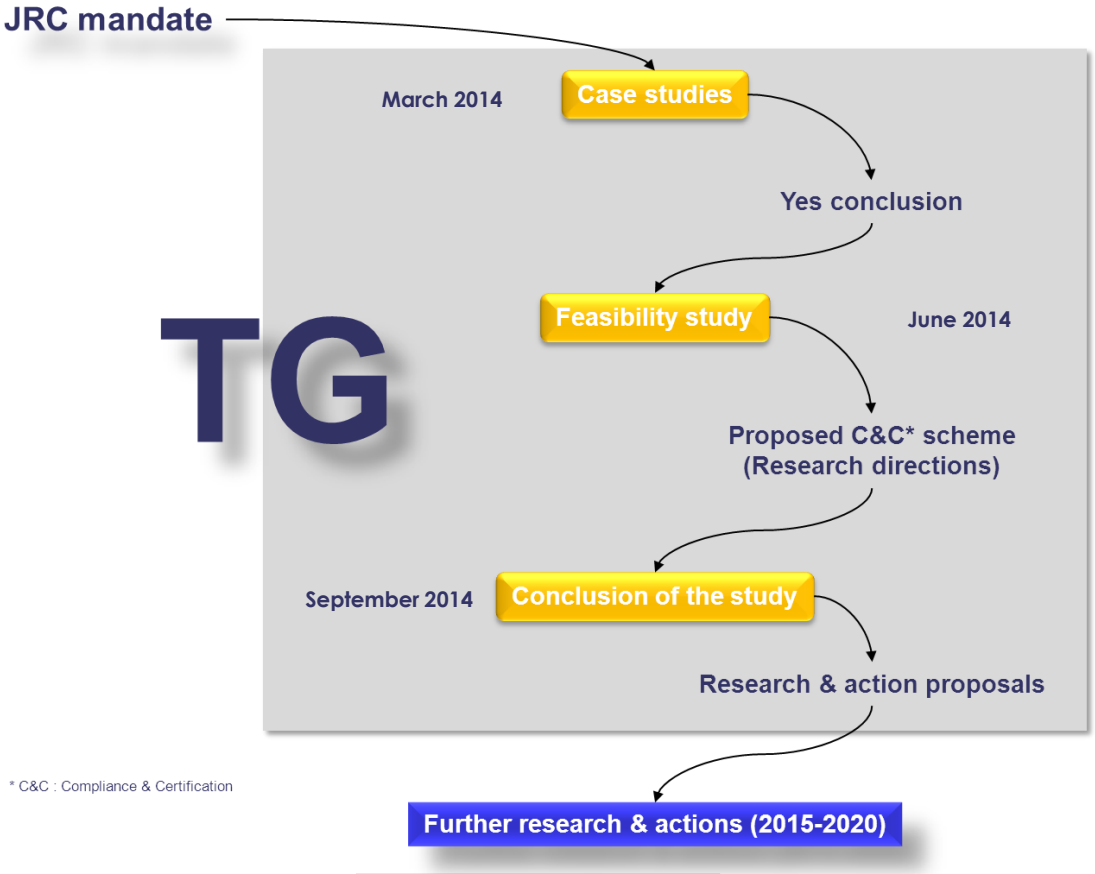
What an IACS is, and previous perspectives on cyber-vulnerabilities



US Department of Energy (2011). *Secure data transfer guidance for industrial control and SCADA systems*. PNNL-20776.

THALES

The TG's work process



THALES

The need is there…

An IACS CS T&C scheme would be useful

- Users would buy CS certified products rather than non CS certified ones

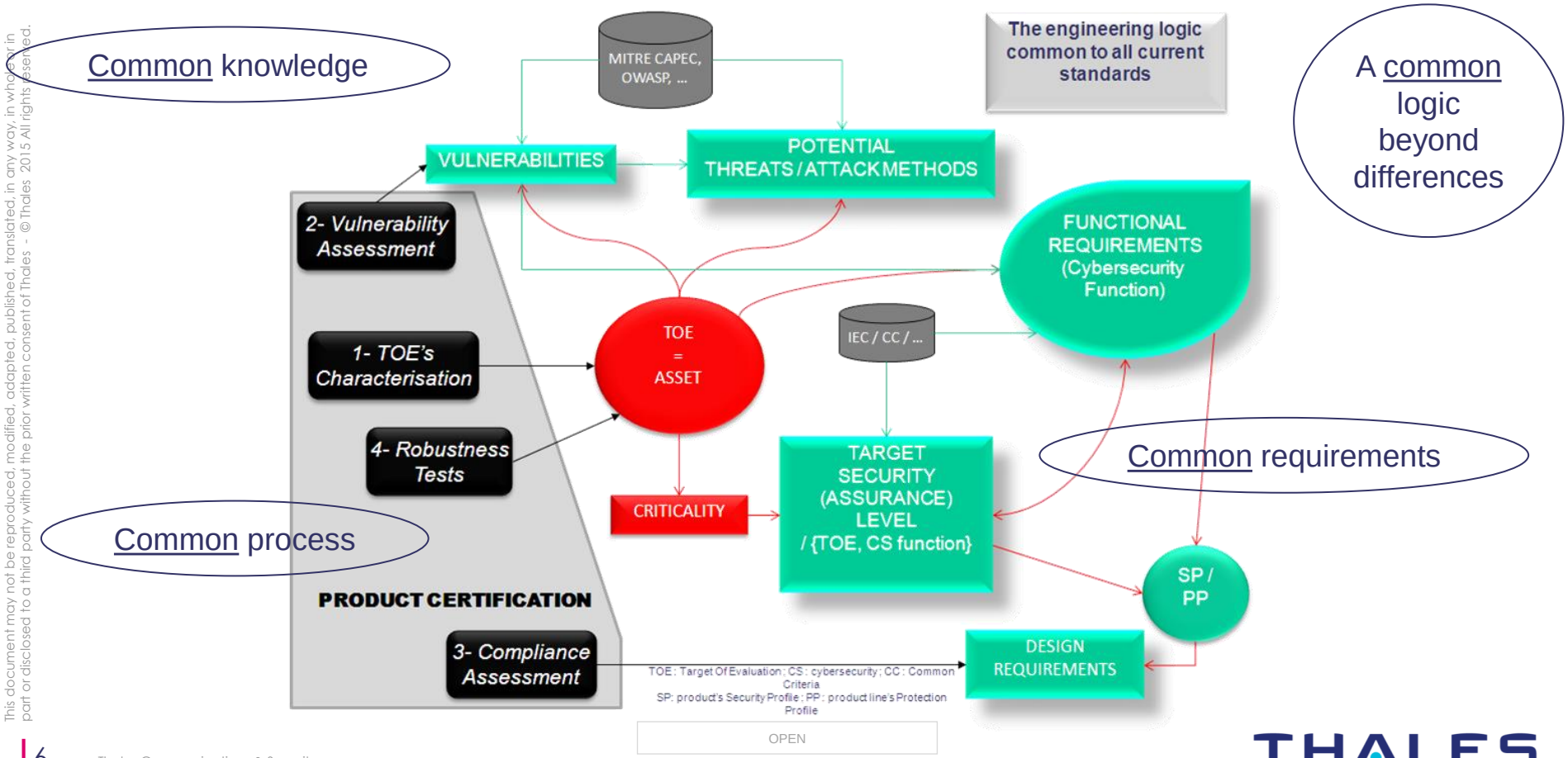
It should focus on IACS products / components only

- Valid for a component, in a given version, under specified operating conditions
- Cyber secure products little more expensive (// plants' set-up & running costs)
- Selling CS certified products would not entail unbearable extra costs for vendors

It should overcome basic obstacles

- What is the value of a certificate if cyber-attacks are unavoidable? (MITRE, 2011)
- Should be European, not only national
- Stakeholders do not want T&C to be mandatory (ENISA, 2013)
- Currently no European obligation for IACS CS certification, hence voluntary
- Vulnerabilities detection primarily in the hands of process owners, also of vendors
- Integrators & users need further efforts to cyber secure systems and plants

Product certification: common needs, common state-of-the-art



THALES

A possible 4-level IACS Compliance & Certification EU scheme

LEVEL 4: THIRD-PARTY FULL CERTIFICATION
(Same as L3 + Process certification)

LEVEL 3: THIRD-PARTY PRODUCT CERTIFICATION
(Same as L2 + Robustness tests)

LEVEL 2: THIRD-PARTY COMPLIANCE ASSESSMENT
(based on a generic product profile)

LEVEL 1: SELF-DECLARATION OF COMPLIANCE
(based on a generic product profile)

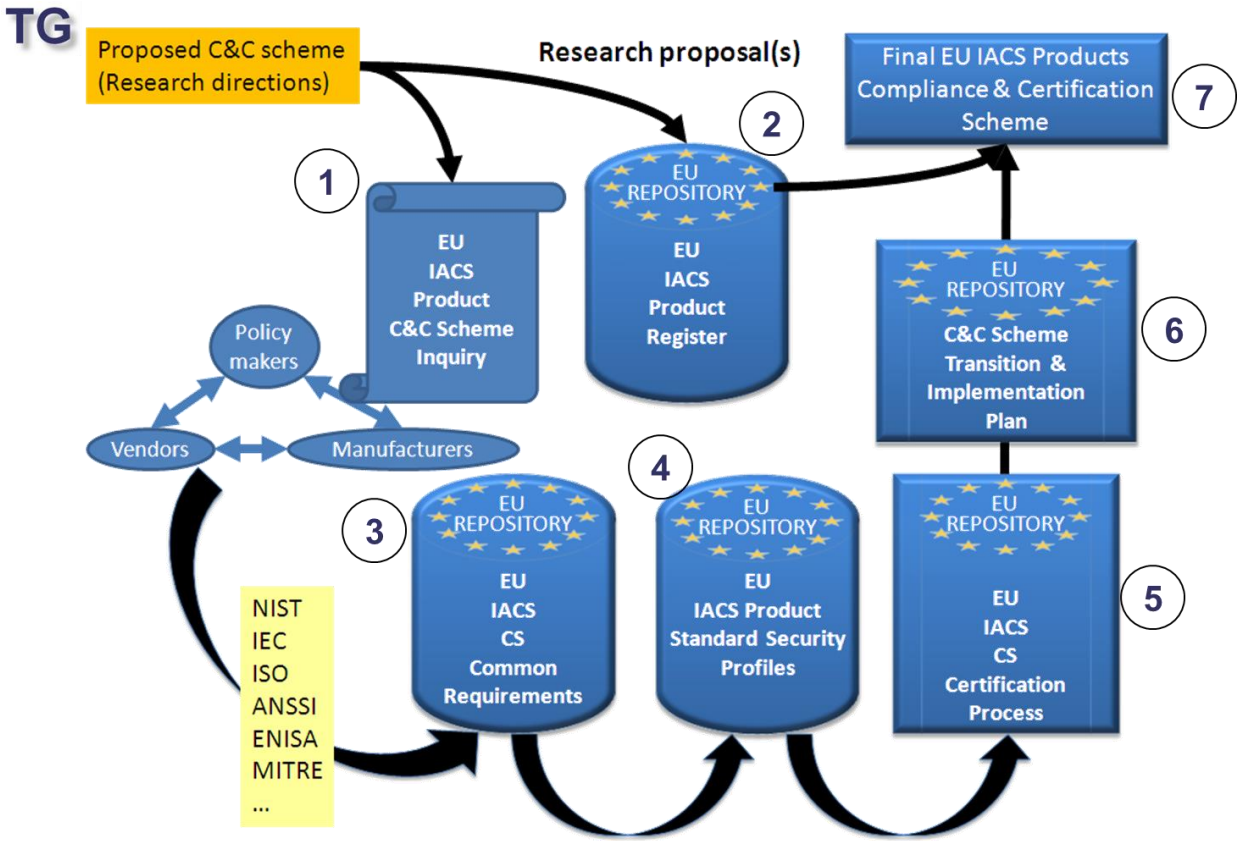
Obligation
Defence, Space, …

Possible obligation
Sector regulation

No obligation
Clients' request in RFPs

No obligation
Vendors' initiative

Research & action proposals for 2015-2020



THALES

In conclusion…

Going beyond cyber-naïveté :

- Cybersecurity is not just in IT guy's hands

Getting involved in defining the future EU IACS cybersecurity C&C scheme

- From mere support to active membership

THALES

Thanks for your attention…

PAUL THÉRON
+33 6 86 65 20 81