11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

A way towards a fully bridged European certification of IACS cybersecurity.

Paul THERON, PhD, FBCI

THALES

A word of introduction: an on-going struggle

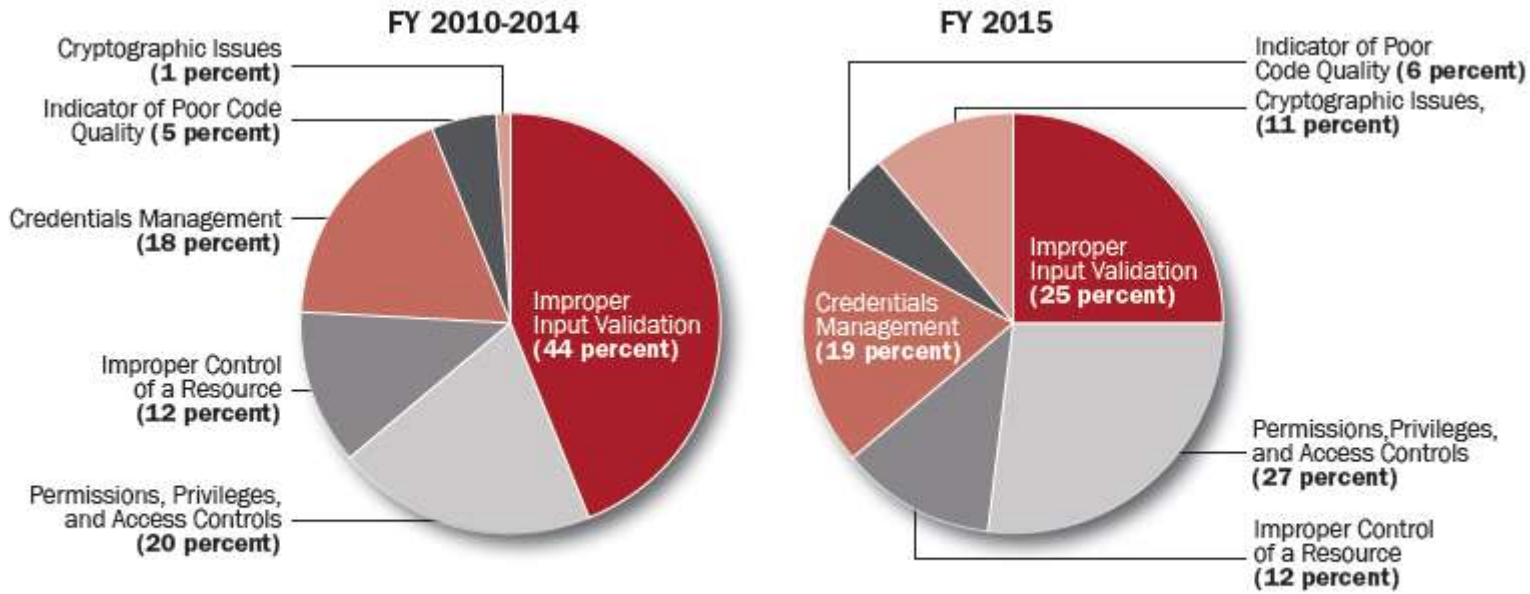


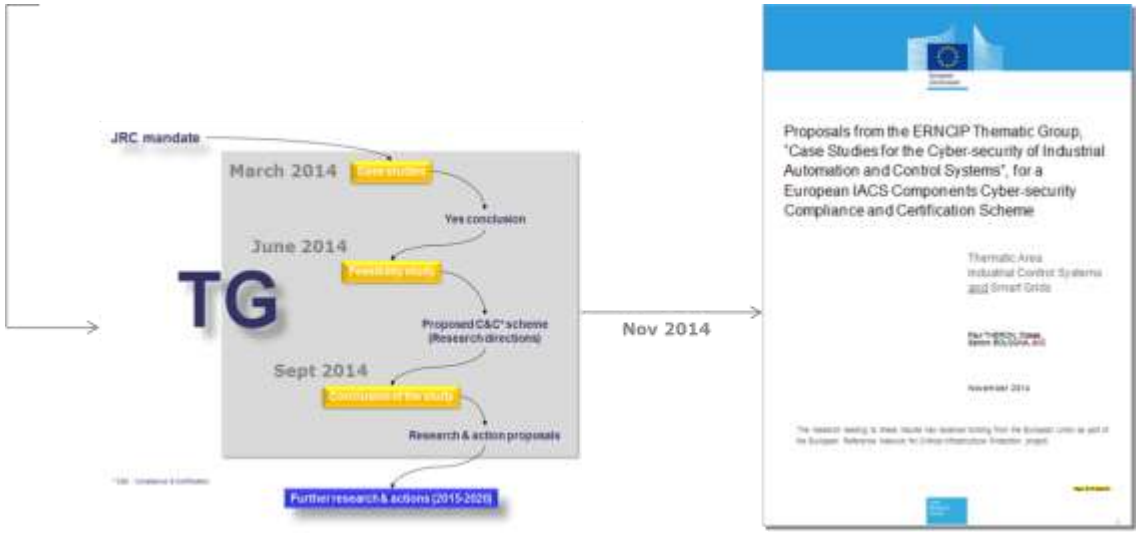
Figure 9. Categories of all vulnerabilities reported to ICS-CERT. (1311)

Source:DHS. (2015). NCCIC / ICS-CERT FY 2015 Annual Vulnerability Coordination Report. Retrieved Sept 11, 2016, from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf

Introducing the ICCF...

- The history of the IACS cybersecurity certification TG
- The philosophy of the ICCF
- Gaining support from stakeholders
- The IACS Compliance & Certification Framework
- The General structure of the ICCF
- Principles of IACS components certification

The history of the IACS cybersecurity certification Thematic Group



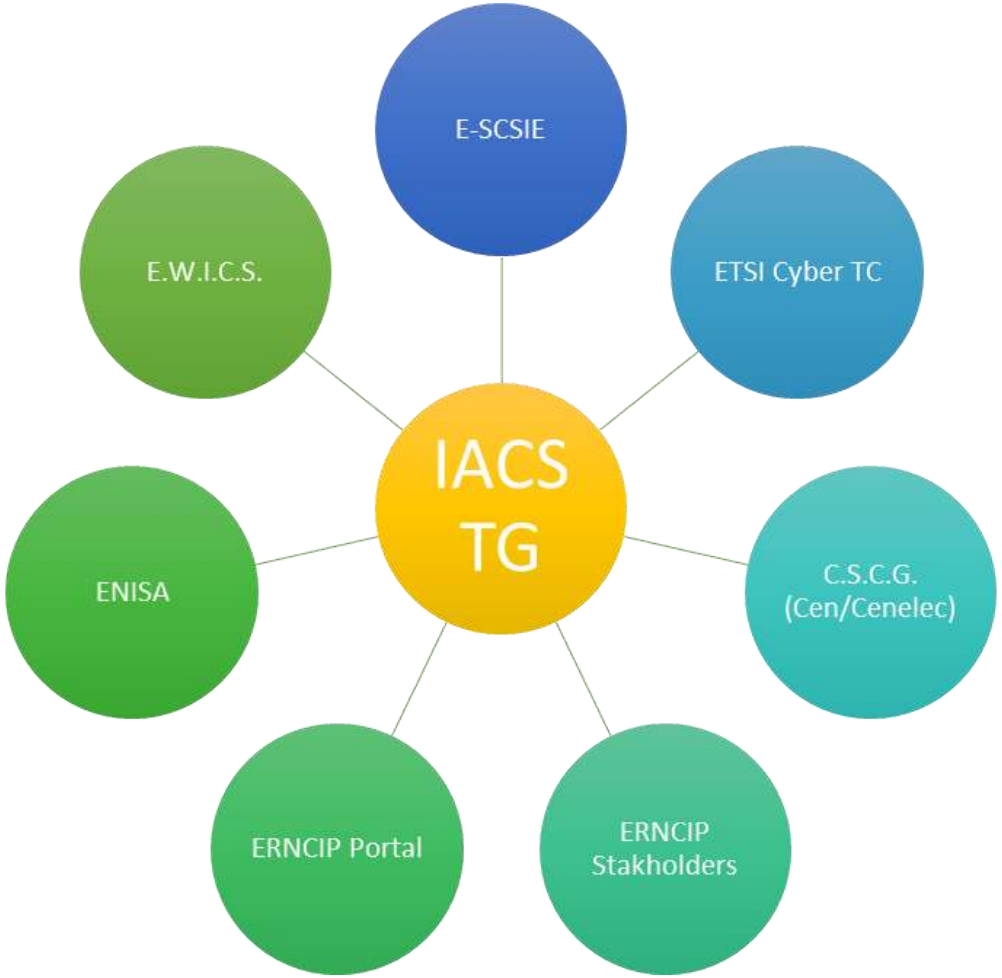
	2015		2016		2017		2018		2019		2020
1- Stakeholders consultation & project planning											
2- Product Register development											
3- CS Common Requirements project											
4- Standard Security Profiles project											
5- Compliance & Certification Process project											
6- Transition & Implementation Plan											
7- Launch of the C&C Scheme											

The philosophy of the ICCF

- A generic model for IACS products / components certification: not a standard
  - Helping vendors and buyers to approach the issue of certification
- An agnostic framework
  - Freedom of choice: standards, national schemes, etc.
- A way to engage stakeholders
  - Schemes from the least to the most demanding
- Guidelines for the European Commission and Professionals
  - How to start? And what to do?

Gaining support from stakeholders

- Stakeholders' consultation 2015-2016 and network of contacts
  - ERNCIP Conference 2015;
  - ENISA – EICS Group and E-SCSIE;
  - ENISA ICT Workshop 16th of March 2016;
  - GIMELEC
  - BSI
  - ANSSI
  - ISA
  - NIST
  - ETSI Cyber TC;
  - EWICS (European Workshop on Industrial Computer Systems Reliability Safety and Security – www.ewics.org);
  - CEN/Cenelec's Cyber Security Coordination Group (CSCG) on 27th April 2016;
  - ERNCIP-Improver Workshop 28th April 2016...



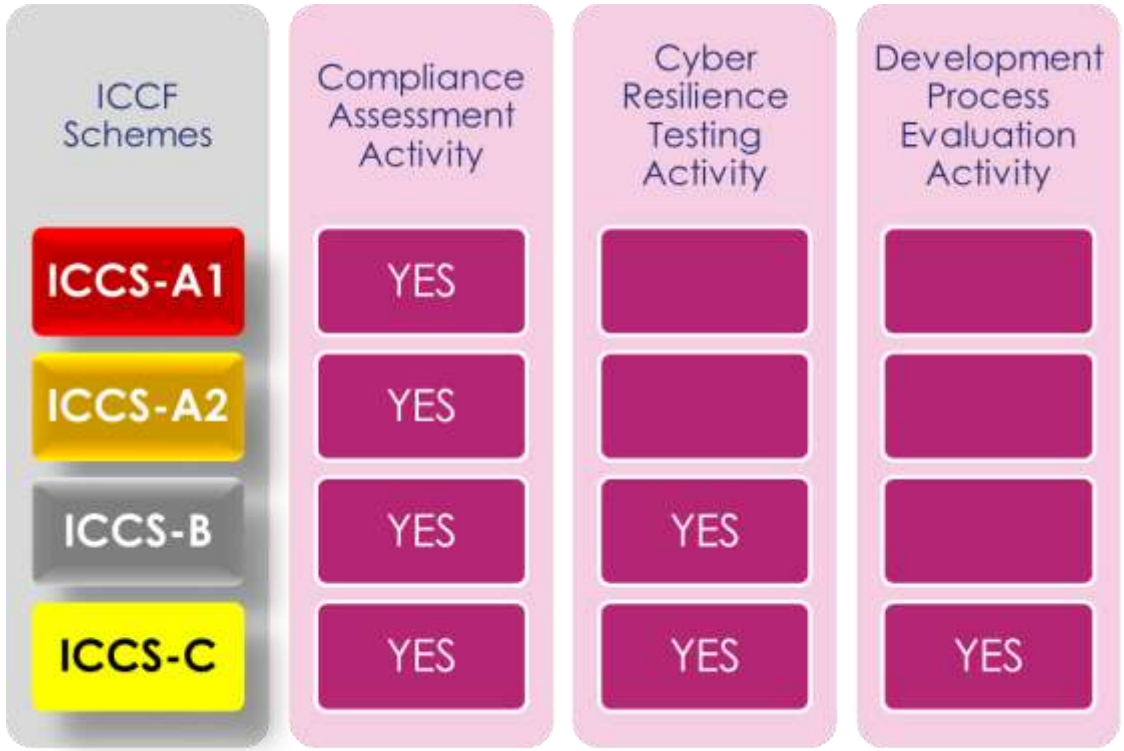
The IACS Compliance & Certification Framework

CRITIS 2016

- Proposes 4 IACS Compliance & Certification Schemes (ICCS)
  - ICCS-A1 (Self-declaration of compliance)
  - ICCS-A2 (Third-party compliance assessment)
  - ICCS-B (Cyber resilience certification)
  - ICCS-C (Full cyber resilience certification)

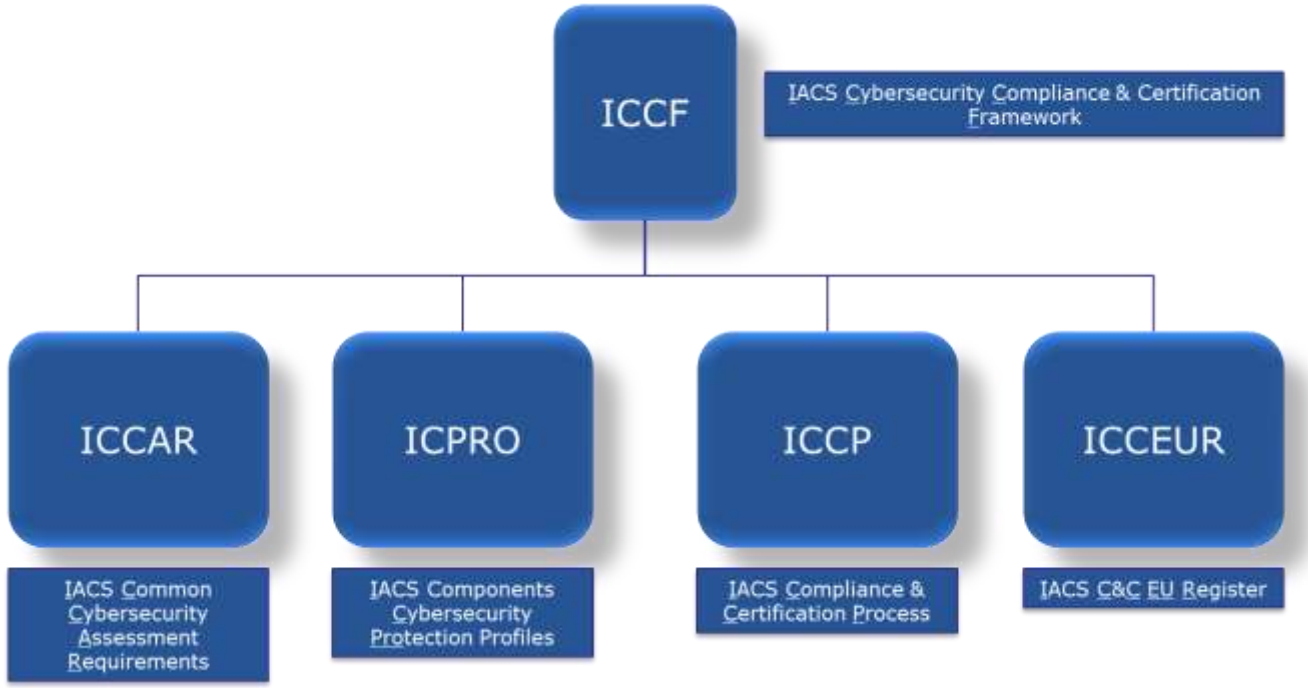
The IACS Compliance & Certification Framework

- Involves up to 3 Evaluation Activities
  - Compliance Assessment (in all four ICCS)
  - Cyber Resilience Testing (ICCS-B & C)
  - Development Process Evaluation (ICCS-C)

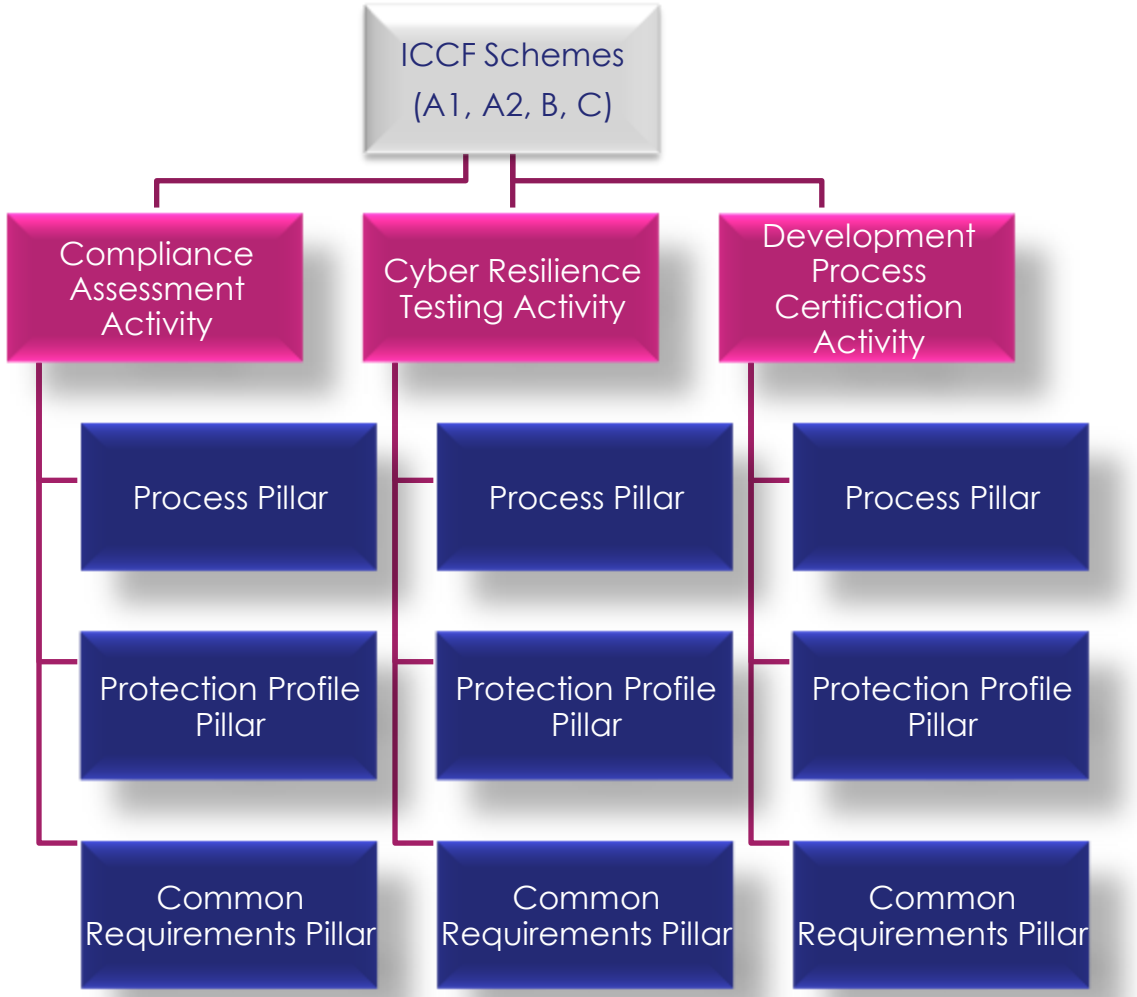


The IACS Compliance & Certification Framework

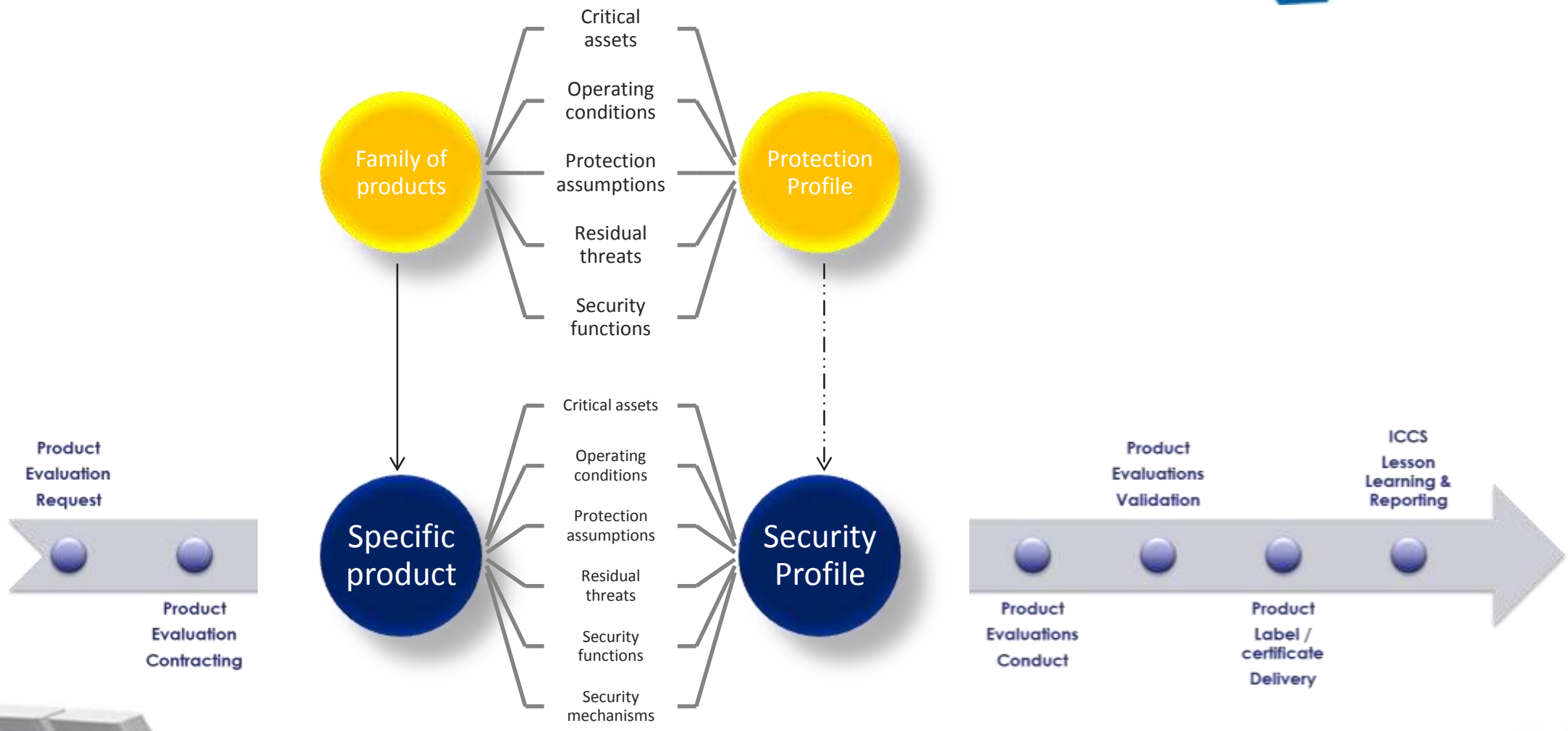
- Requires the guidelines and resources of 3 Pillars
  - IACS Common Cybersecurity Assessment Requirements (ICCAR)
  - IACS Components Cybersecurity Protection Profiles (ICCPRO)
  - IACS Compliance & Certification Process (ICCP)
- ... And involves a 4th pillar for fostering and disseminating the ICCF
  - IACS C&C EU Register (ICCEUR)



The General structure of the ICCF



Principles of IACS components certification



In conclusion: Join the trials in 2017

Thank you for your attention

Email: paul.theron@thalesgroup.com

THALES