Safety & Cybersecurity of embedded softwares in product and process

PROCESS SAFETY congress
May 30, 2018

Franck SADMI- Project Manager Safety & Cybersecurity
Technical Centre Europe

BUREAU VERITAS


No Safety without
CYBERSECURITY
BUREAU VERITAS 1828
BUREAU
VERITAS

Cyber events

Ukraine

In Y2017 Neutralization of a power plant.
2 attacks - 250,000 people without electricity for several days.

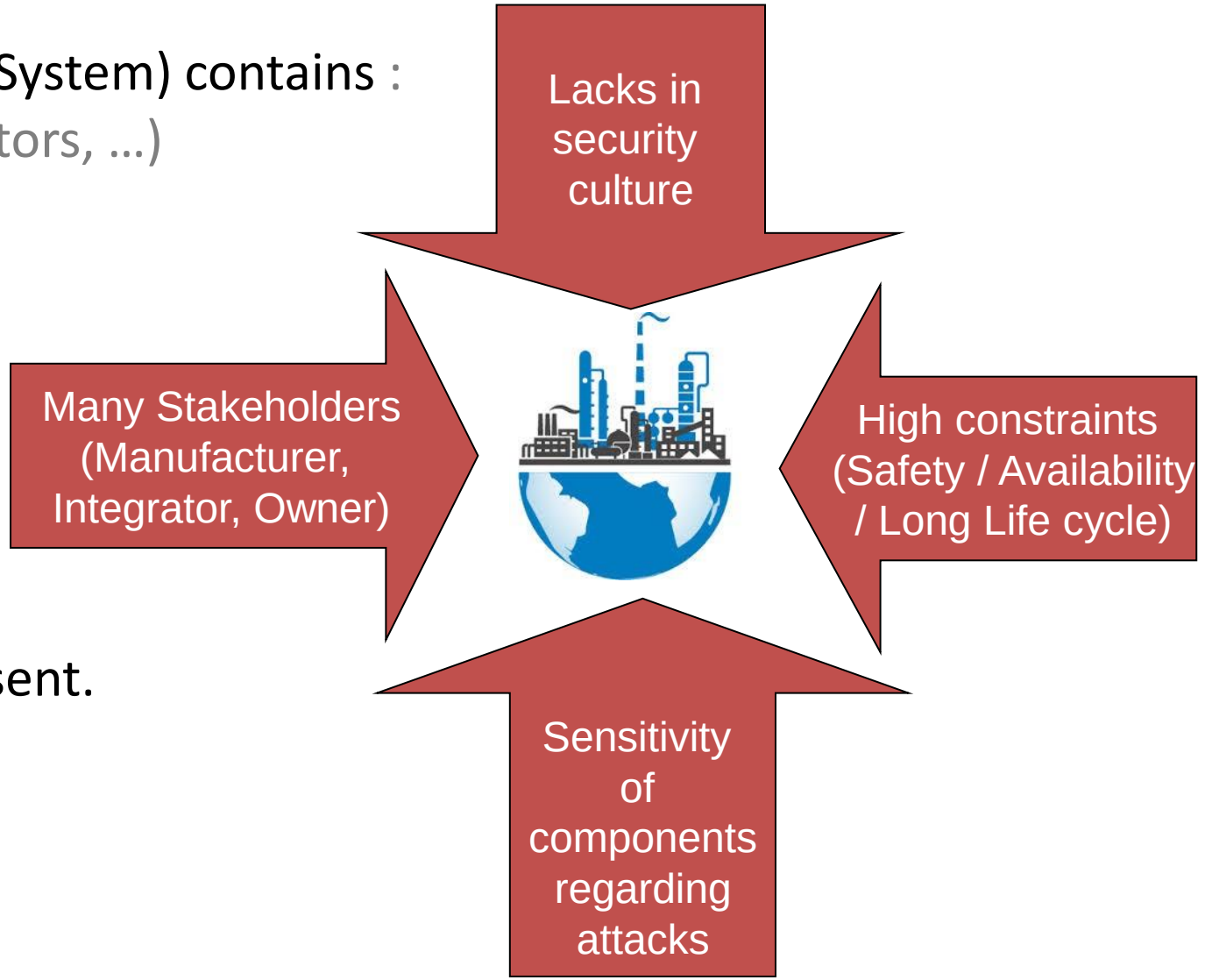
Middle East

In Y2017 dec , Malware TRITON targeted Triconex Safety Integrated System (SIS) causing an unavailability of the system.

Process Specificities

IACS (Industrial Automation Control System) contains :

- Electronic devices (sensors, actuators, …)
- Networks
- Computers (servers, PLC, …)
- Software
- SCADA



Software part is more and more present.

No Safety without Cybersecurity

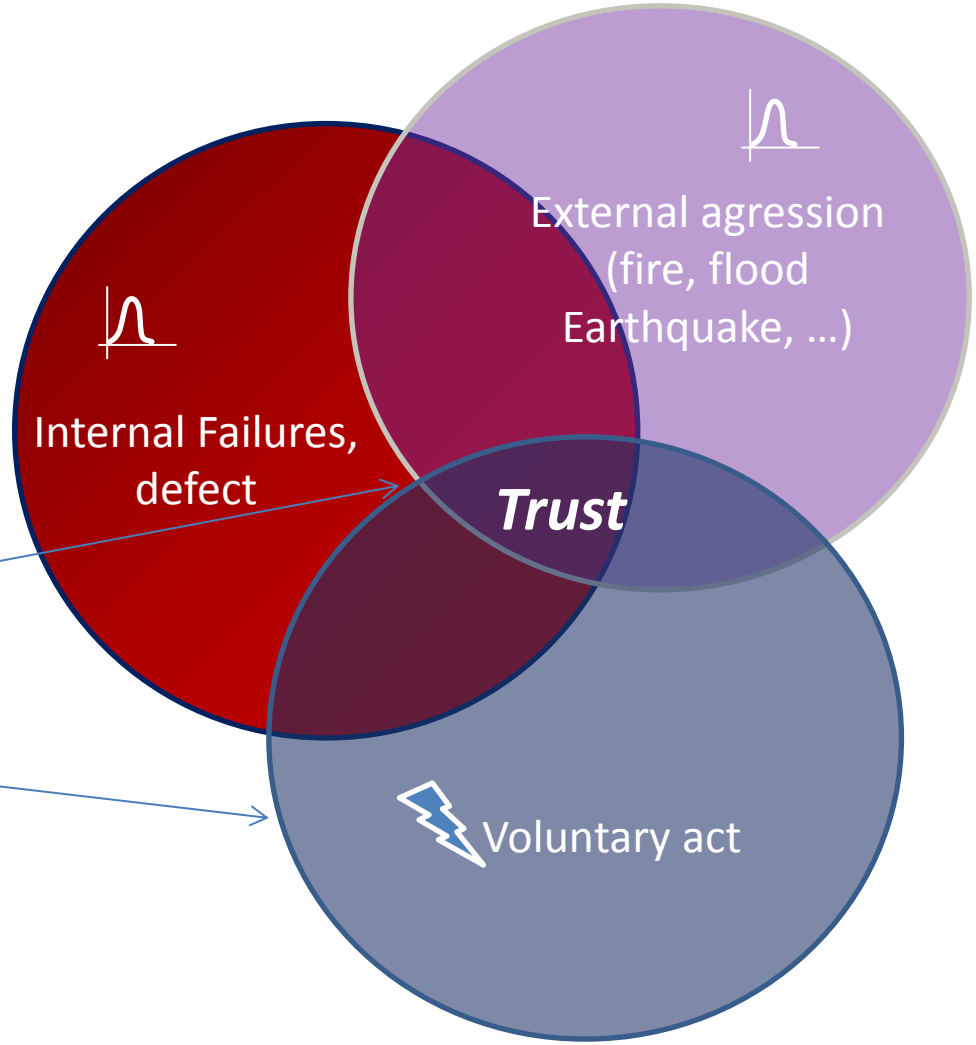
For SAFETY and CYBERSECURITY:

Trust is the goal

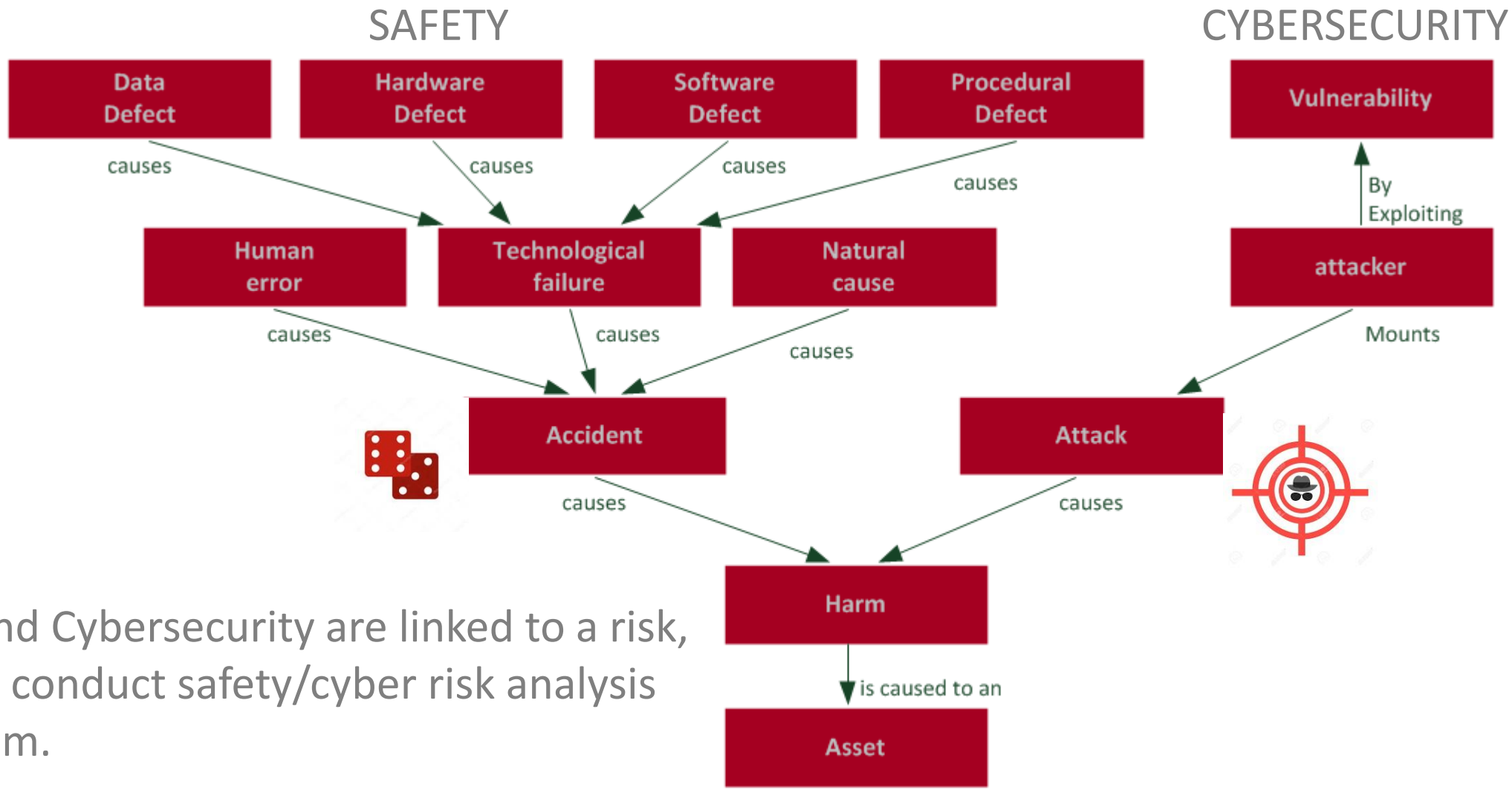
But methods for Risk quantification are not the same:

Quantitative approach for Safety

Qualitative approach for Cybersecurity



No Safety without Cybersecurity



Because Safety and Cybersecurity are linked to a risk, it makes sense to conduct safety/cyber risk analysis by a common team.

Firesmith, D. (2003). Common concepts underlying safety, security, and survivability engineering."

No Safety without Cybersecurity

For the Software development,

Safety & Cybersecurity needs will conduct to a common answer:

Quality, traceability, development process, whitebox test campaign, etc.

But some topics are clearly in opposition:

Requires arbitration / technical choices

Safety	CyberSecurity
Stability quest	Update is a priority
Performance Quest	Algorithm for Cyber could be resource consumer (degrading global performances)
Simplicity is the ally of reliability	By adding complex algorithm, volume of source code could drastically increase
Easy accessibility to device	Limit the logical /physical access

No Safety without Cybersecurity

During the project life cycle, Safety & Cyber have to be addressed in parallel:

Std for Safety : IEC 61511 (for example)

Std for Security : IEC 62443 (for example)

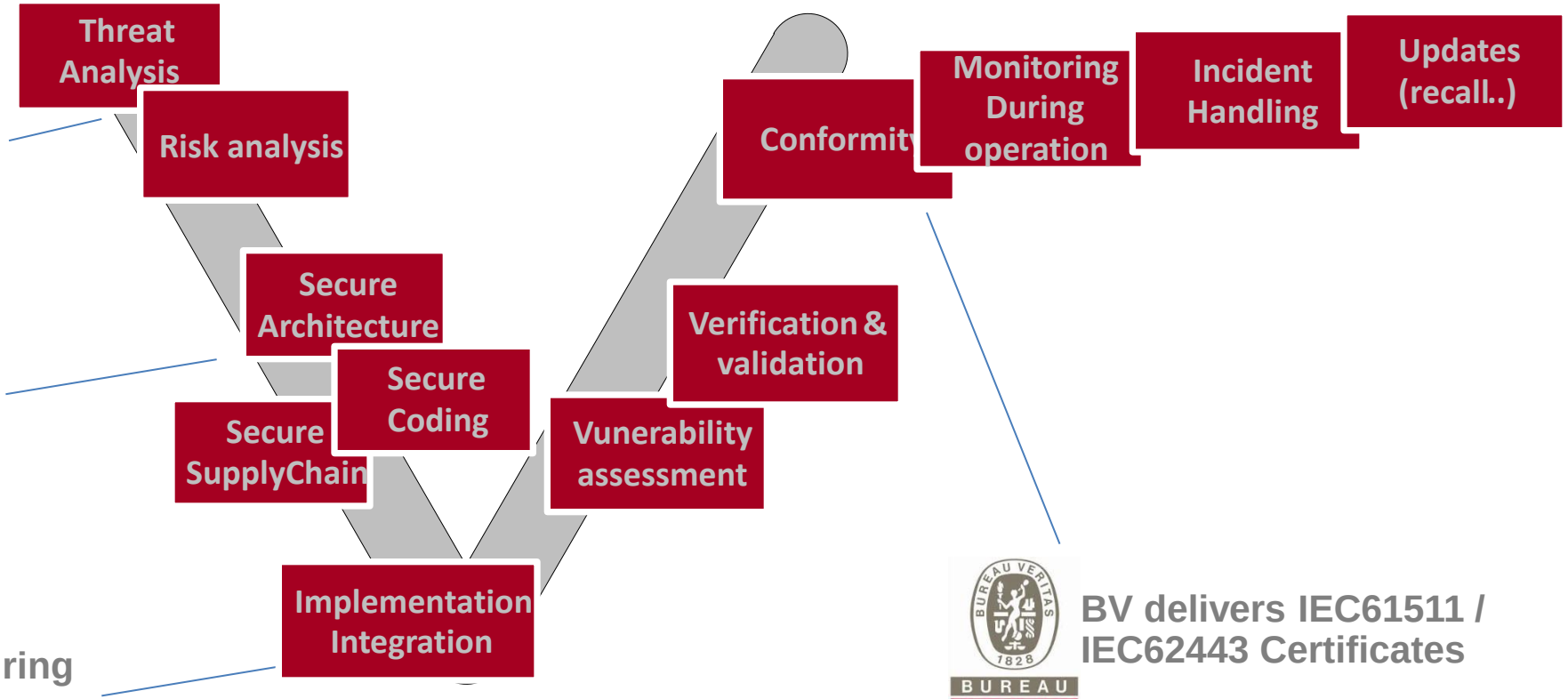
BV supports its customers during Risk analysis

BV publishes guidelines :

BV-SW100

BV-SW200

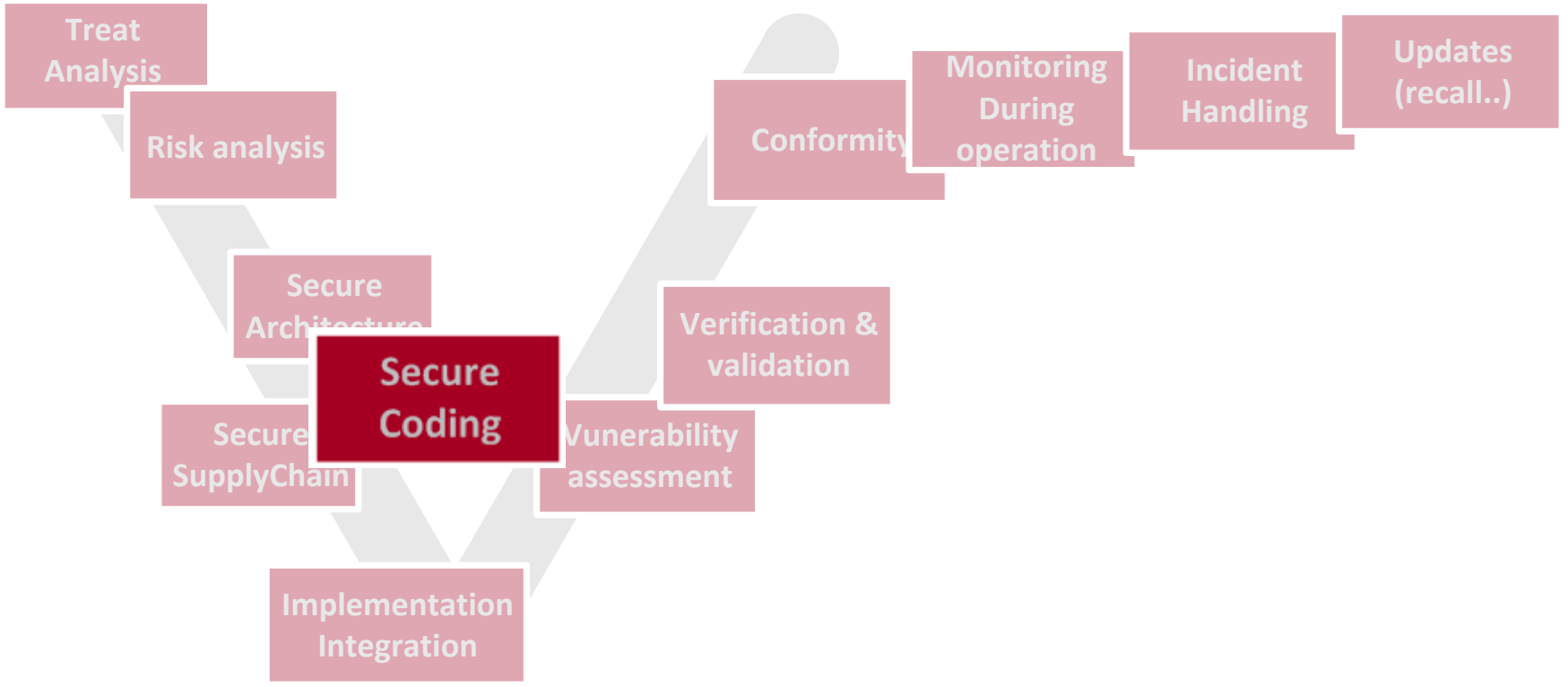
BV supports its customers during Software development

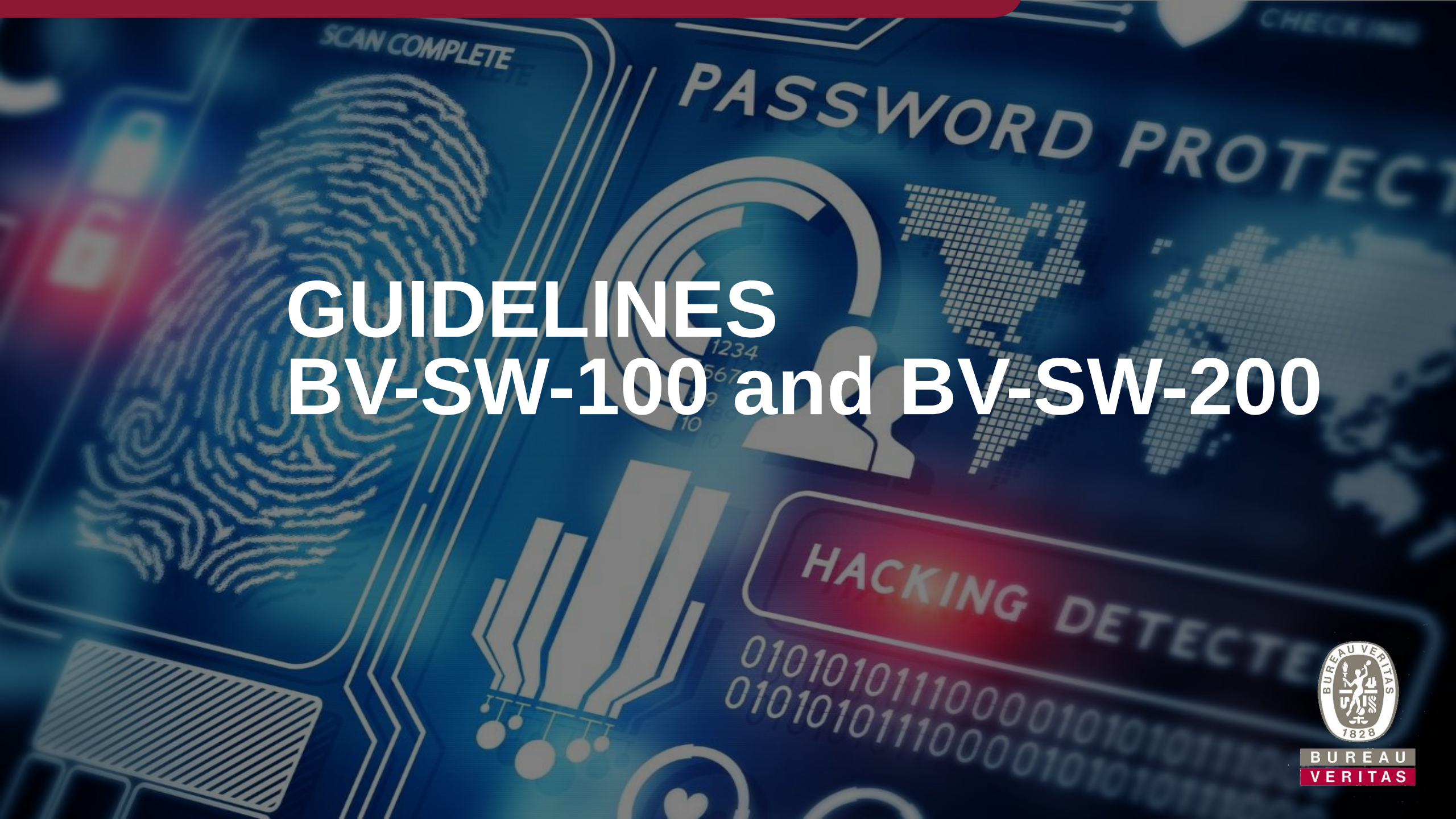


BV delivers IEC61511 / IEC62443 Certificates

No Safety without Cybersecurity

Focus on the « coding » step





GUIDELINES
BV-SW-100 and BV-SW-200

BUREAU VERITAS

Secure By Design

- We can distinguish at least three types of errors :
  - ordinary coding or implementation errors,
  - administrative and configuration errors,
  - fundamental design problems.

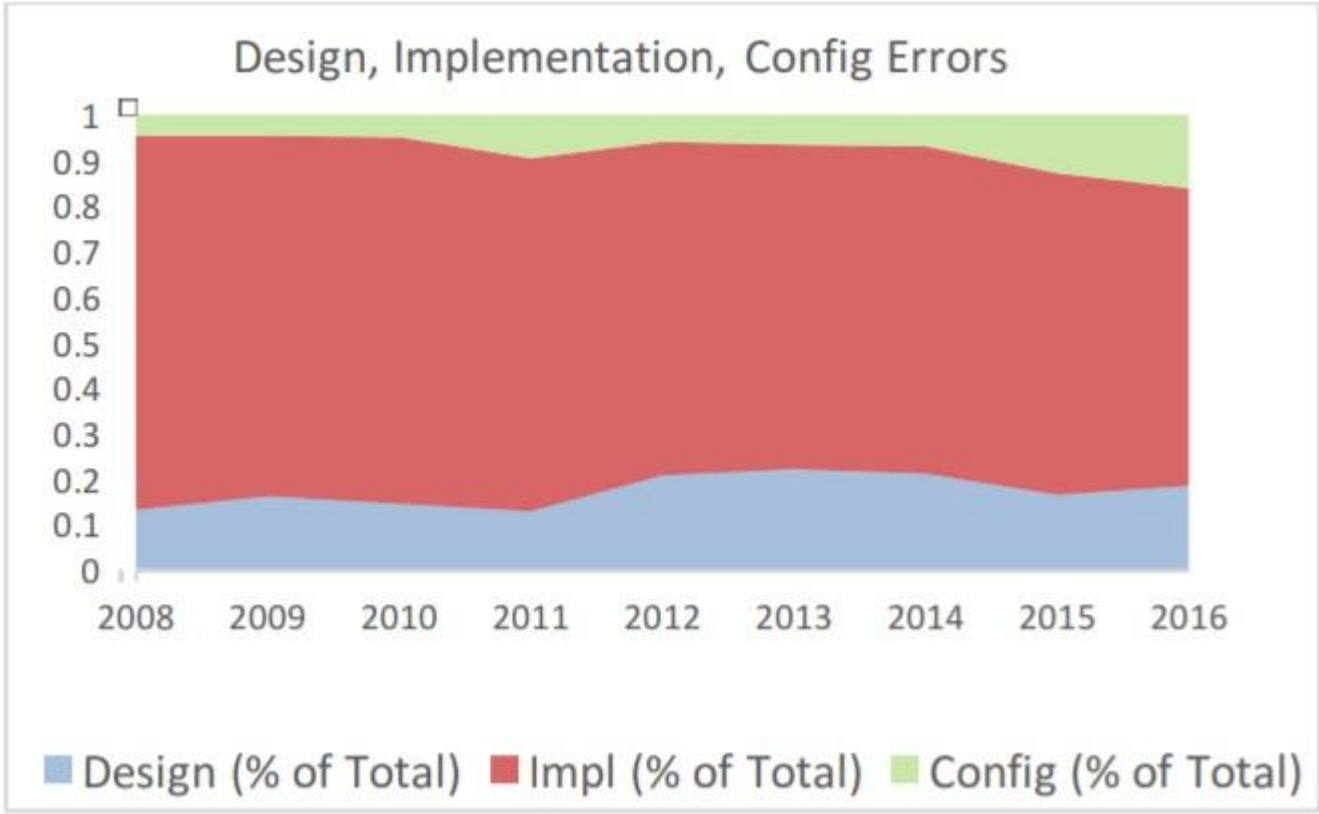
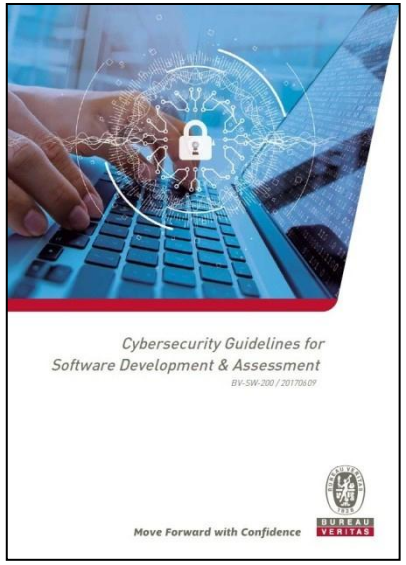


Fig. 3. Vulnerability Class Trends, 2008-2016

BV Guidelines

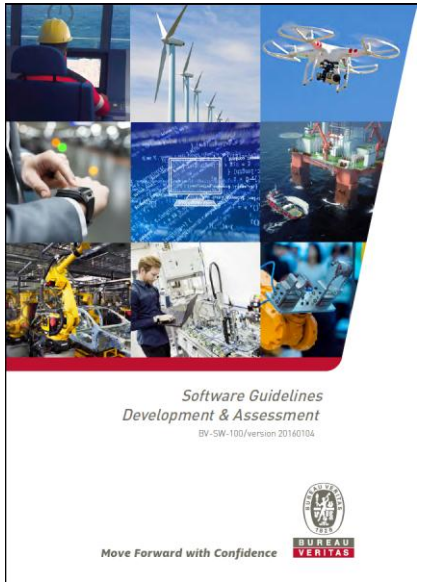
Customer feedback:

- Trouble to embrace the large number of cybersecurity & safety standards
- No specific standard dedicated to the Software development for cybersecurity



BV-SW-200
Cybersecurity guidelines
for Software
Development & Assessment

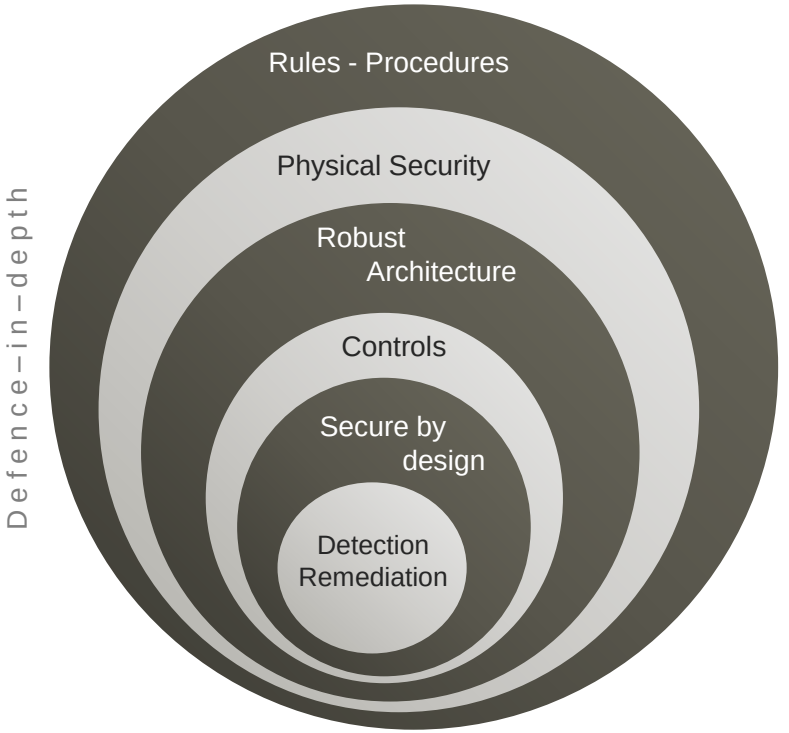
BV-SW-100
Software Guidelines
Development & Assessment



Secure by Design

Are we obliged to apply the SECURE by DESIGN concept?

- Yes, in order to respect the Defense In depth approach.



How far can we go in the cybersecurity implementation ?

- BV guidelines propose a gradual approach:
  - 4 **Safety classes** in the BV-SW-100 from SC1 to SC4
  - 2 **Security classes** in the BV-SW-200 SC0 à SC1

Code Analysis

- **Static code Analysis**
  - **Kill 2 Birds with 1 stone … :**

    Source code analysis is relevant for Software failure (**Safety**) and SW vulnerability (**Cyber**) detection.

  - **Frama- C:**

    Open Source software CEA-Tech Research center

- **Threat Analysis & Risk Assessment**
  - **STRIDE:**

    SPOOFING, TAMPERING, REPUDIATION, INFORMATION DISCLOSURE, DENIAL of SERVICE , ELEVATION of PRIVILEGES

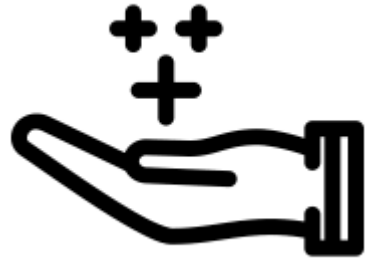
Requirements / Objectives - Acceptance Criterias

Objectives Description

- **Notation :** ex: OBJ_COTS_040
- **Objectifs typés :**
  - **TOOLS_ ,** (Tools)
  - **DES_ ,** (Design)
  - **DEV_,** (development)
  - **COTS_,** (Library, code re-used)
- **Acceptance Criteria:**
  - What needs to be done to fulfill the objective

CONCLUSION

- **No Safety without Cybersecurity**
  - Safety is necessary & is well adressed by standards for years (pillar)
  - Cybersecurity has to be integrated in existing safety lifecycles
  - Software is the heart of the systems
  - Like Safety, Cybersecurity has to be seen during design & operations



- **To help you**
  - Standards & guidelines in Cybersecurity are available (http://www.bureauveritas.com/white-papers/cybersecurity-guidelines-for-development-and-assessment-bv-sw-200)
  - Bureau Veritas can provide services on consultancy or assessment in order to give you confidence on your products in Cybersecurity and safety

Questions ?