ORGALIME

Cybersecurity of Industrial Systems

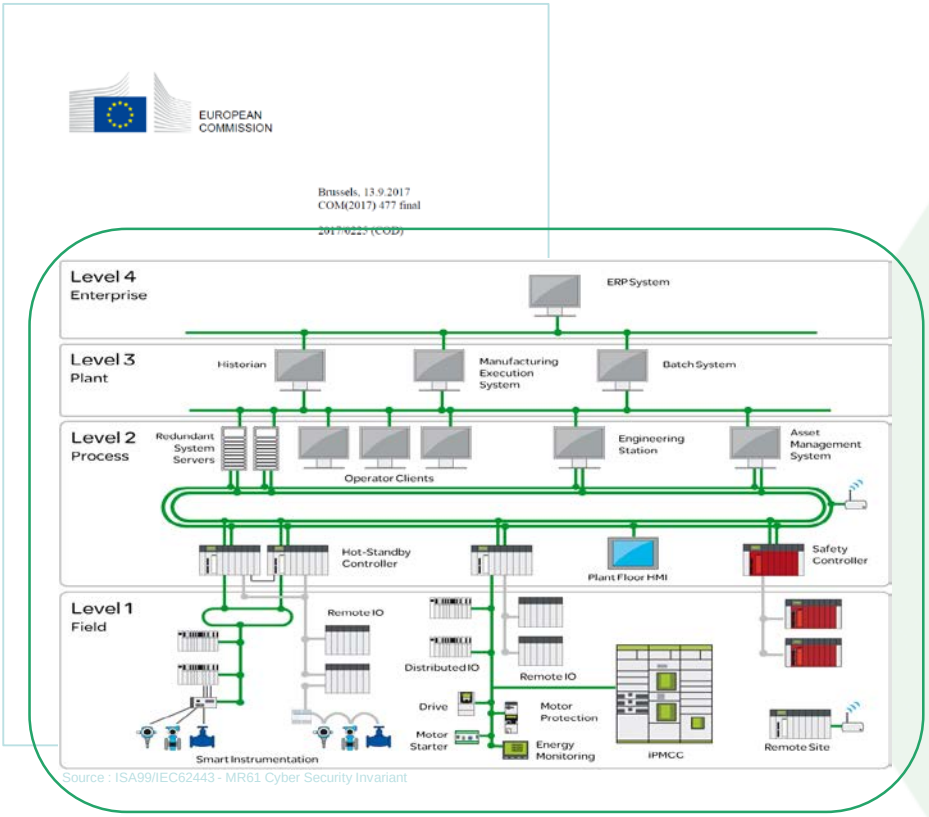
Effectively implementing the EU certification framework

Presented by : Pentcho Stantchev – Strategy & Development – Schneider Electric France

Life Is On Schneider Electric

The European Engineering Industries Association

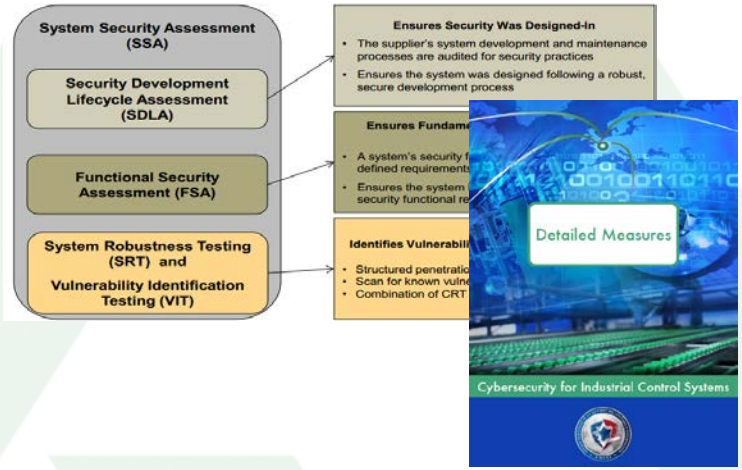
The European Cybersecurity Act provides good foundations that should be adapted to industrial cybersecurity



- We welcome its main objective of harmonizing the EU cybersecurity certification
- We support the voluntary approach taken by the EC as a key topic and as possibility for us to optimize costs and security by adapting to risk analysis and market demand
- We are aligned with the "security by design" methodology as underlined and valued in the proposal, while ensuring that future schemes also follow a risk-based approach, depending on the context and severity of the application
- More consistency and adaptation to industrial cybersecurity are needed
- Industrial cybersecurity differs in many key aspects from the cybersecurity of information and communication technologies.
- The highest priority here is to ensure the continuity of operations and to avoid possible malfunction, destruction and endangering of human lives

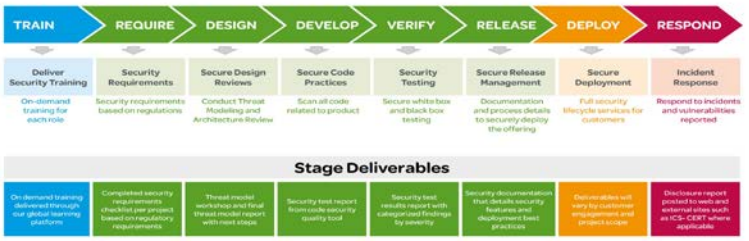
Key topics to be considered for achieving effective certification measures in the context of industrial cybersecurity

- A sector-specific approach with product and application-related risk analysis, is more suitable and efficient
- Industry-driven international standards provide well-tested foundations for certification and should be the baseline in order to reduce costs and maintain competitiveness of European companies
- Certification of the complete product lifecycle makes more sense than this oriented only to product properties
- Industrial cybersecurity is the result of a complete value chain of relevant stakeholders. Product security is not all. The certification approach has to also include requirements for system integrators and service providers
- ENISA should involve in the process relevant industry stakeholders in order to provide expertise and to ensure efficiency for industrial cybersecurity
- Orgalime's key messages on the Cybersecurity Act: http://www.orgalime.org/position/flexible-and-market-relevant-cybersecurity-compliance-and-certification-schemes-orgalime



Secure Development Lifecycle

IEC62443 / ISA99 - Standards



Our industry recommends schemes adapted to industrial products and processes, and self-declaration of conformity as baseline

- Industry Standards for voluntary certification
  - IEC 62443
  - focused on functional security
  - provides certification for products and product lifecycle processes
  - French First Level Security Certificate (CSPN)
  - similar to the vulnerability analysis performed within the Common Criteria
  - achieves relevant results in a less complex way
  - even for products providing protection for most critical systems
  - ISO/IEC 270xx series
  - relevant standards for cybersecurity management and processes
  - guidelines for organizational control and domain specific application
- Self-declaration of conformity to cybersecurity standards
  - inspired by the conformity assessment in the New Legislation Framework
  - should reflect relevant requirements at the time being
  - benefits for reducing certification costs, fostering innovation and market diversity