Cybersecurity threats in flow measurments

MSc. Satish Soekhoe, NMi Certin B.V.

Compliance Requirements

- Mandatory application of the directive requires products to be secure by design, secure by default, and incorporate means for regular updates.
- Self-declaration of compliance for most products, but with stringent documentation and evidence requirements.

Technical Challenges

- Adapting existing products to meet new security requirements can be costly and complex.
- Implementing effective mechanisms for vulnerability reporting and handling.

Transitional Implications

- Transitioning from current practices to full compliance with CRA involves updating or redesigning products, which could be resource-intensive.
- Understanding and implementing European Harmonized Standards across products and systems.
- CE marking will indicate products comply with the CRA

NIS2 - Directive on Security of network and Information Systems

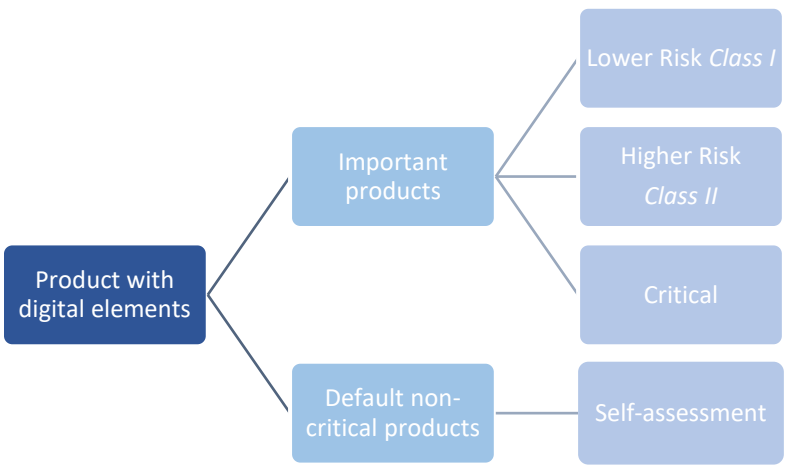
- Operational resilience in critical infrastructure
- Adopted 14 December 2022
- Effective 16 January 2023

RED- Radio Equipment Directive

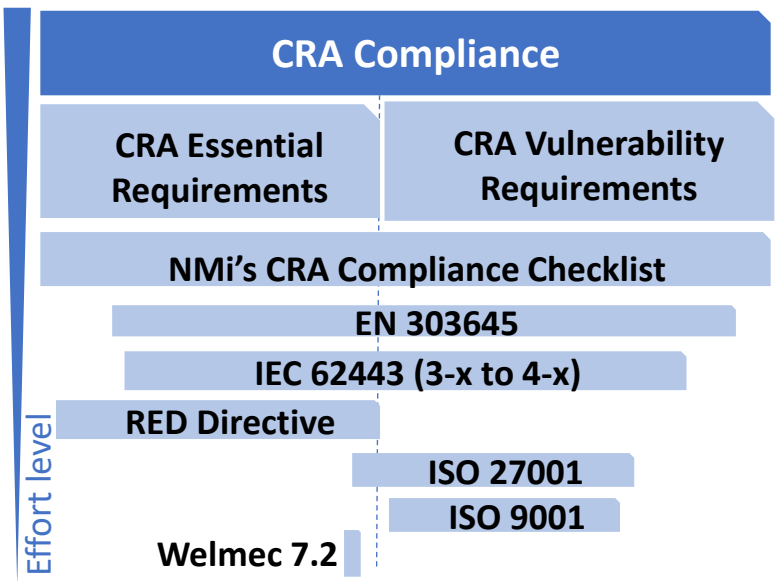
- Communication security (instrument with wireless communication)
- Adopted 16 April 2014
- Effective 1 August 2025

CRA- Cyber Resilience Act

- Embedded device and software cybersecurity
- Adopted 23 October 2024
- Effective 11 December 2027



Type of product	Class	Criticality	Risk Level
Meters (Gas, water, etc.)	Critical*	Critical Infrastructure Device	Moderate to Higher Risk
EV Chargers	Critical*	Critical Infrastructure Device	Higher Risk
Payment Terminals	Important Class I	Important Infrastructure Device	Moderate to Higher Risk
Flow Computers / PLCs / SCADA	Critical*	Critical Infrastructure Device	Moderate to Higher Risk



Key parts of the standard for CRA compliance:

- IEC 62443-3-3 System security requirement and security levels
- IEC 62443-4-1 Secure product development lifecycle requirements
- IEC 62443-4-2 Technical security requirement for IACS components

(SRs) or (CRs) associated with the foundational requirements (FR) Total 7FRs:

1) Identification and authentication control (IAC)
2) Use control (UC)
3) System integrity (SI)
4) Data confidentiality (DC)
5) Restricted data flow (RDF)
6) Timely response to events (TRE)
7) Resource availability (RA)