
SECURITY BY NORM

Hilft die IEC 62443 einer sicheren Produktentwicklung?



IEC 62443

Main Concepts

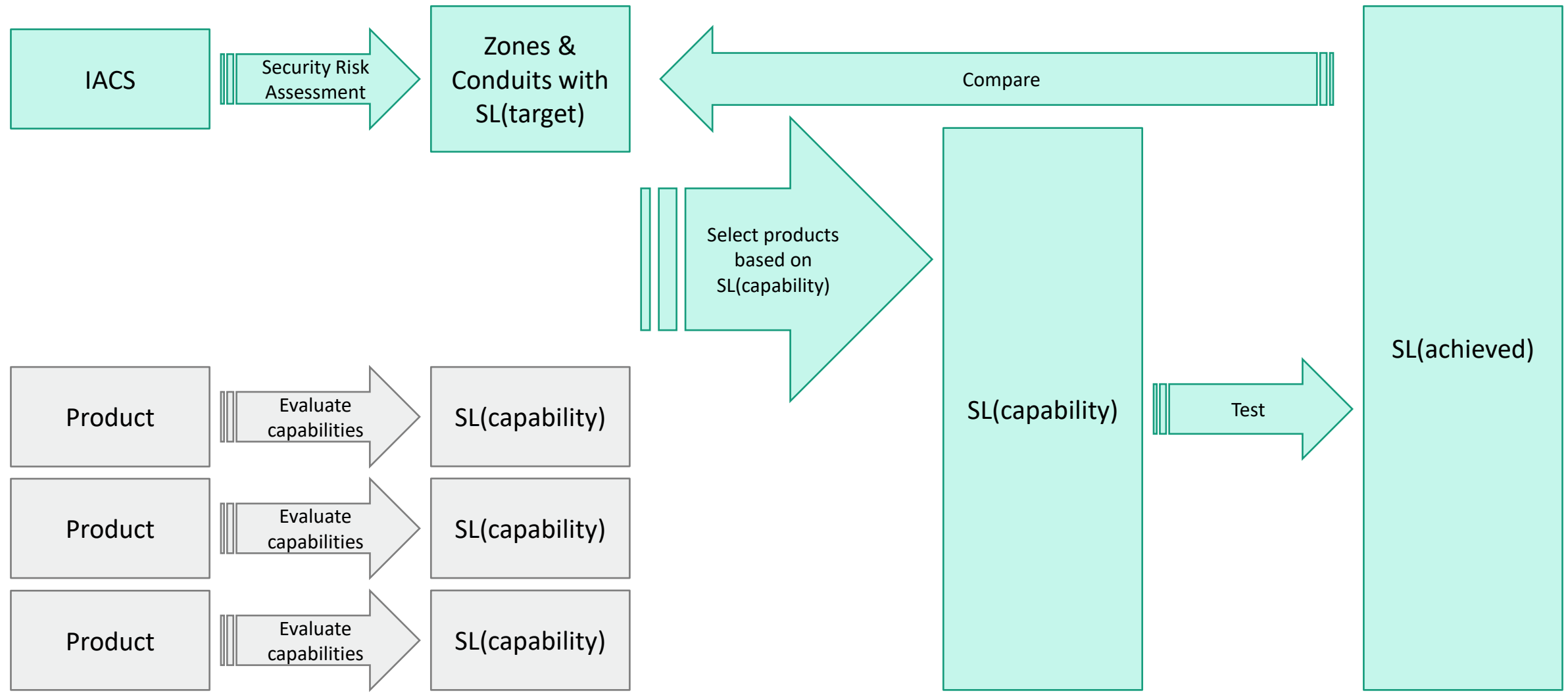
- Risk-driven security engineering
 - Define security zones and conduits
 - Identify and manage security risks
 - Determine Target Security Levels SL(target) for zones / conduits
- Security Lifecycle aspects
 - Capability Security Levels SL(capability) for zones / conduits / products
 - Achieved Security Levels SL(achieved) for zones / conduits
 - Security program maturity
- Defines common basics, terminology, and **what** to do, not **how** to do it



Source: IEC 62443-3-3

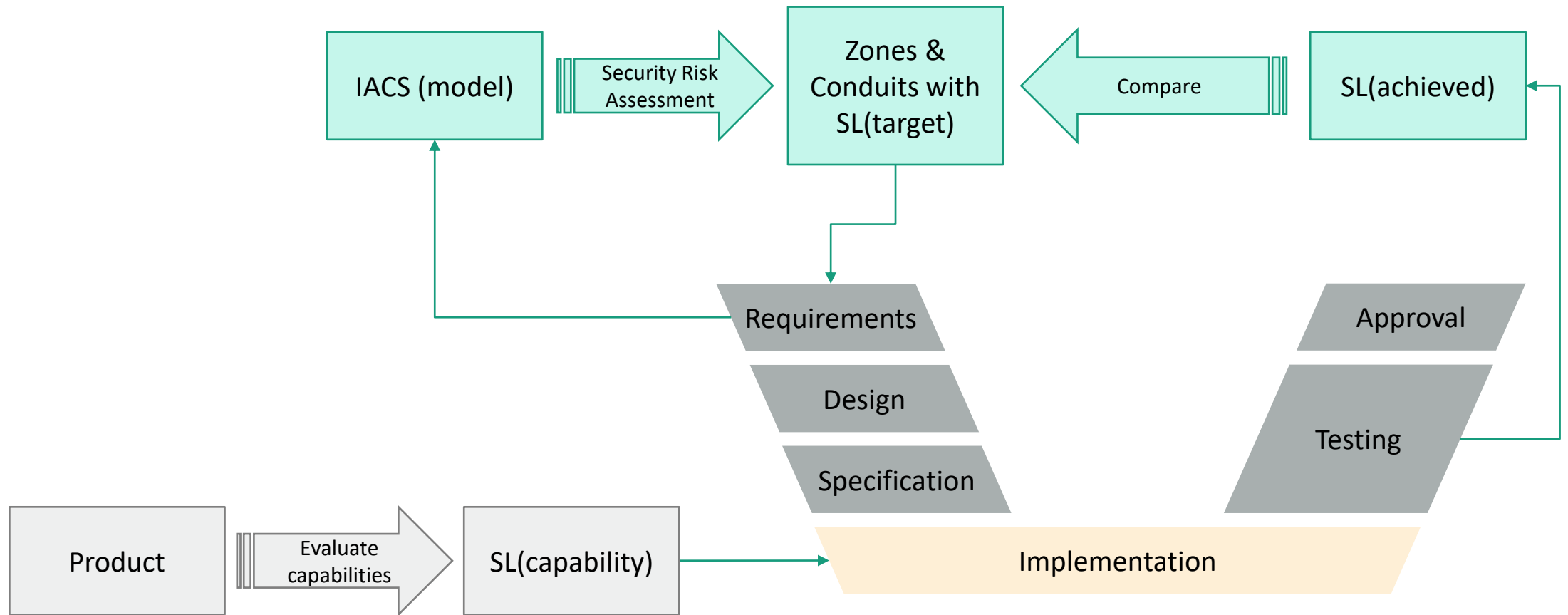
Security Levels

Target, Capability, Achieved



Security Levels

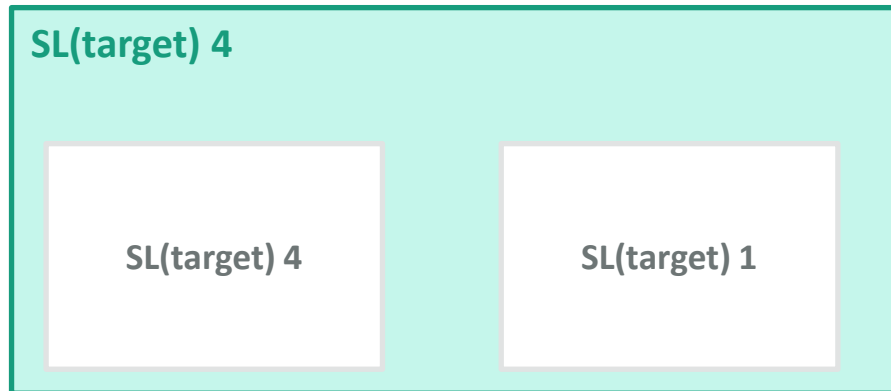
Target, Capability, Achieved



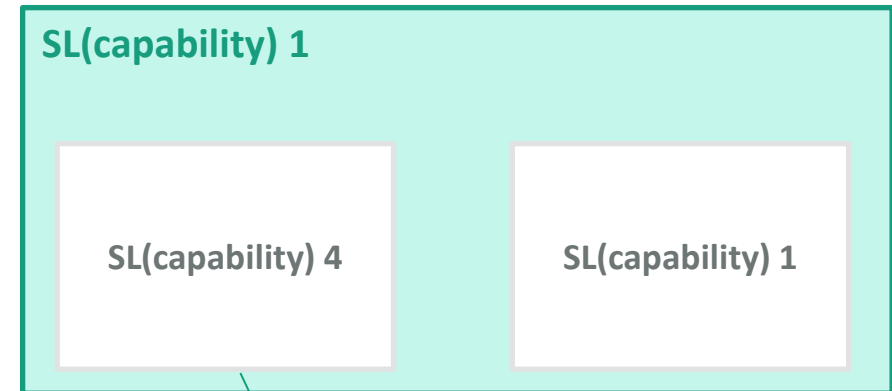
Security Levels

Target vs. Capability (or Achieved)

Security Level - Target



Security Level - Capability



Product label
→ cf. IEC 62443-4-2:2019

IEC 62443

Scope

- IT security for
 - Production sites
 - IACS Products
- Threats
 - “IT-based” attacks
 - Catastrophes (floods, earthquakes, ...)
 - Physical attacks (countered by “gates, guards, and guns”)

IEC 62443

Is it useful?

- Security is important...
 - ... against attackers¹
 - ... for your customers, who might request a specific SL(capability) / SL(achieved)
- Simplified communication along the supply chain
 - Common terminology
 - Communicate well-defined requirements → SL(target)
 - Make your security capabilities a product label → SL(capability)
- Get appropriate security countermeasures
 - Avoid high risks ...
 - ... but do not overspend on security / do not make your product too expensive
- Regulation might demand it (cf. UN-R.155 for the automotive sector)

Contact



Fraunhofer Institute for
Applied and Integrated Security (AISEC)

Lichtenbergstr. 11, 85748 Garching

Daniel Angermeier

Tel.: +49 89 32299 86-181

daniel.angermeier@aisec.fraunhofer.de

<http://www.aisec.fraunhofer.de/>