Cybersecurity für Medizinprodukte – Wie geht man vor ?

CE plus GMBH
MEDICAL DEVICES • IVD
Regulatory Affairs & More

Ittipan Kanluan
Regulatory Affairs Expert

About us

- CE plus
  - Service Provider for Regulatory Affairs
    - Medical Devices
    - In Vitro Diagnostics
    - Active Implantable Devices
  - Focus: CE-marking
    - Regulatory Strategies (e.g. Definition of Intended Use)
    - Technical File
    - Software Documentation
    - Risk Management
    - Requirements Engineering
    - Usability
    - Clinical Evaluation

Contents

Cybersecurity vs Medical Device

- „Medical device vulnerable to hackers“
- „Insulin pump can be hacked“
- „Big issue: Cybersecurity!“
- Data breaches must be reported to the authority under the new General Data Protection Regulation (GDPR)

Safety & Security

Definition:

Freedom from unacceptable risk

(ISO/IEC Guide 51:1999, definition 3.1)

Safety

Combination of the probability of occurrence of harm and the severity of that harm

(ISO/IEC Guide 51:1999, definition 3.2)

Risk

Physical injury or damage to the health of people, or damage to property or the environment

(ISO/IEC Guide 51:1999, definition 3.2)

Harm

Definition: Security

Condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

(IEC Guide 120)

Data and systems security

Operational state of a medical device in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

(AAMI TIR 57)

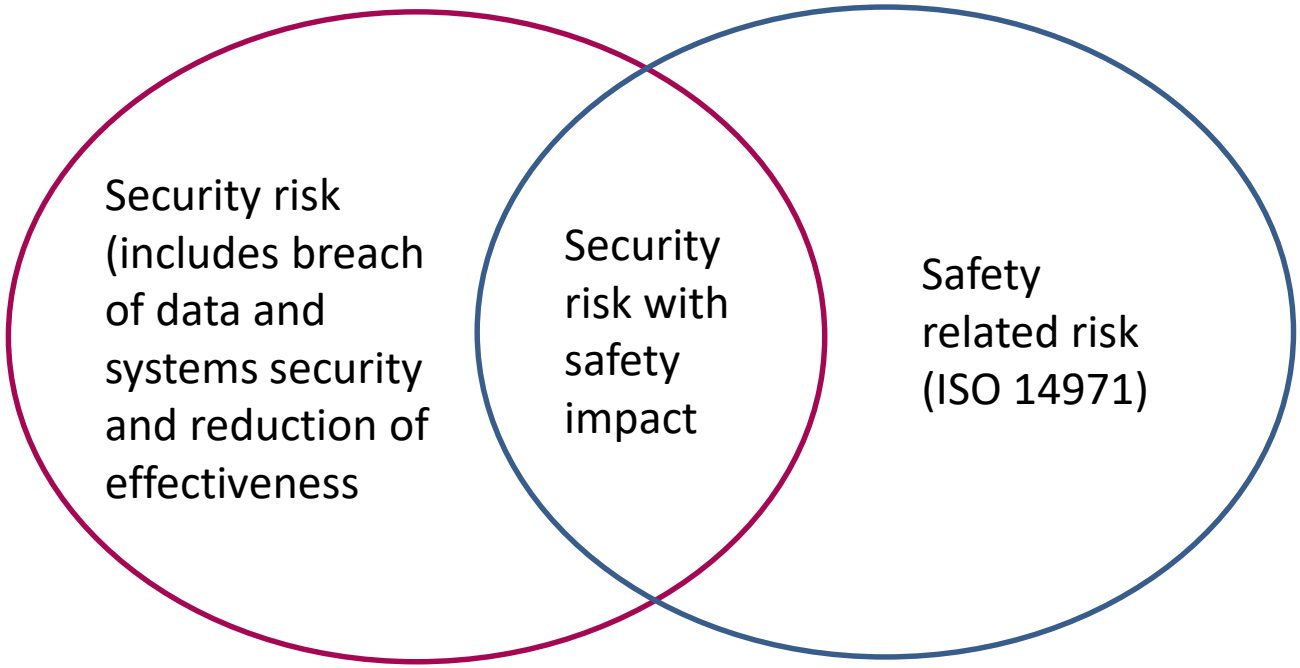
Definition (revisited): Harm

Physical injury or damage to the health of people, or damage to property or the environment, or reduction in effectiveness, or breach of data and systems security

IEC 80001-1, AAMI TIR 57

Safety & Security

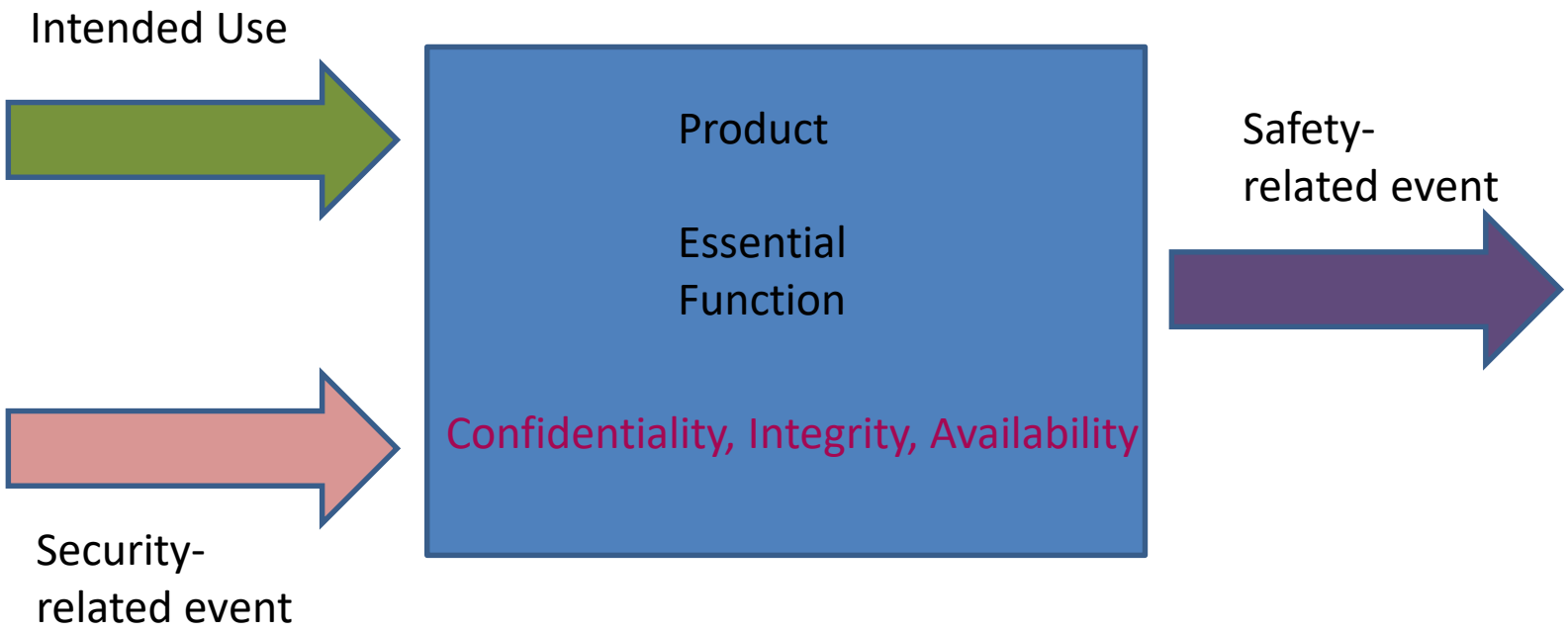
- Relationship between safety and security risk



Source: AAMI TIR 57

Safety & Security

Fundamental difference



Safety & Security

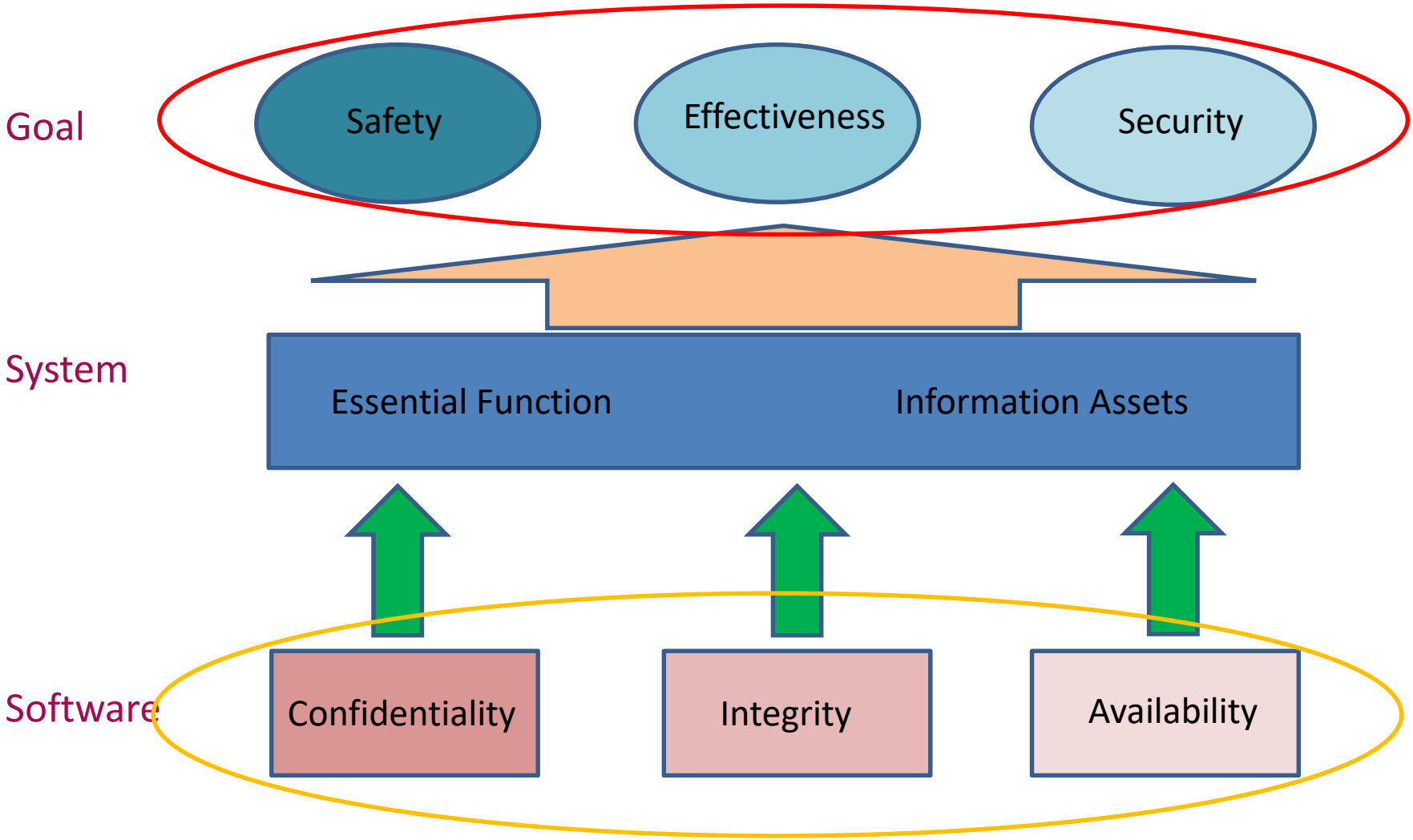
- Security is not mentioned in MDD

- How about MDR ?

MDR, Annex I: General safety and performance requirements

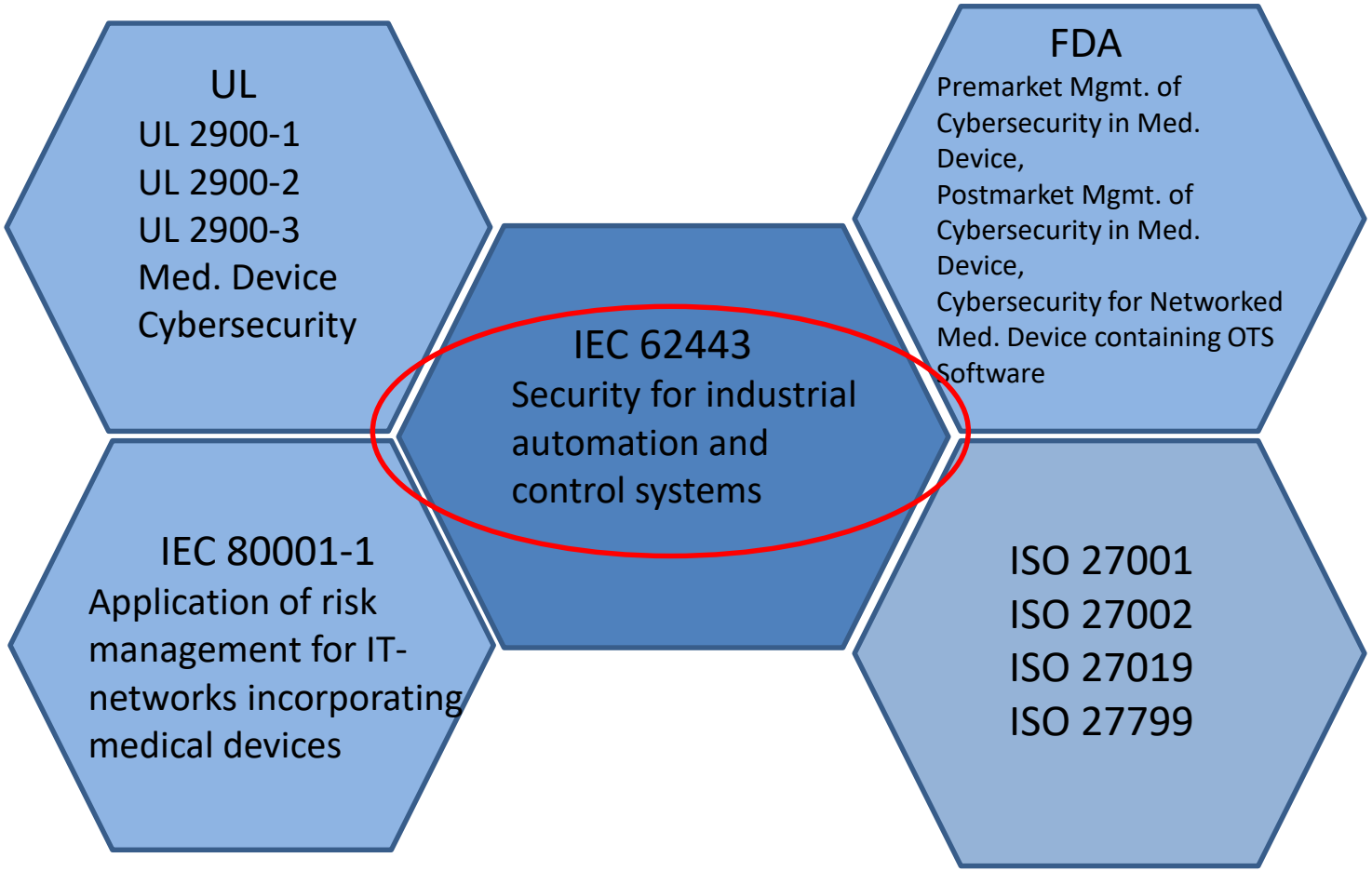
17.2) For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principle of development life cycle, risk management, including information security, verification and validation

Why Cybersecurity ?



Norm / Standard

- Any norm/standard/Guidance to Cybersecurity ?
  - **Yes !**

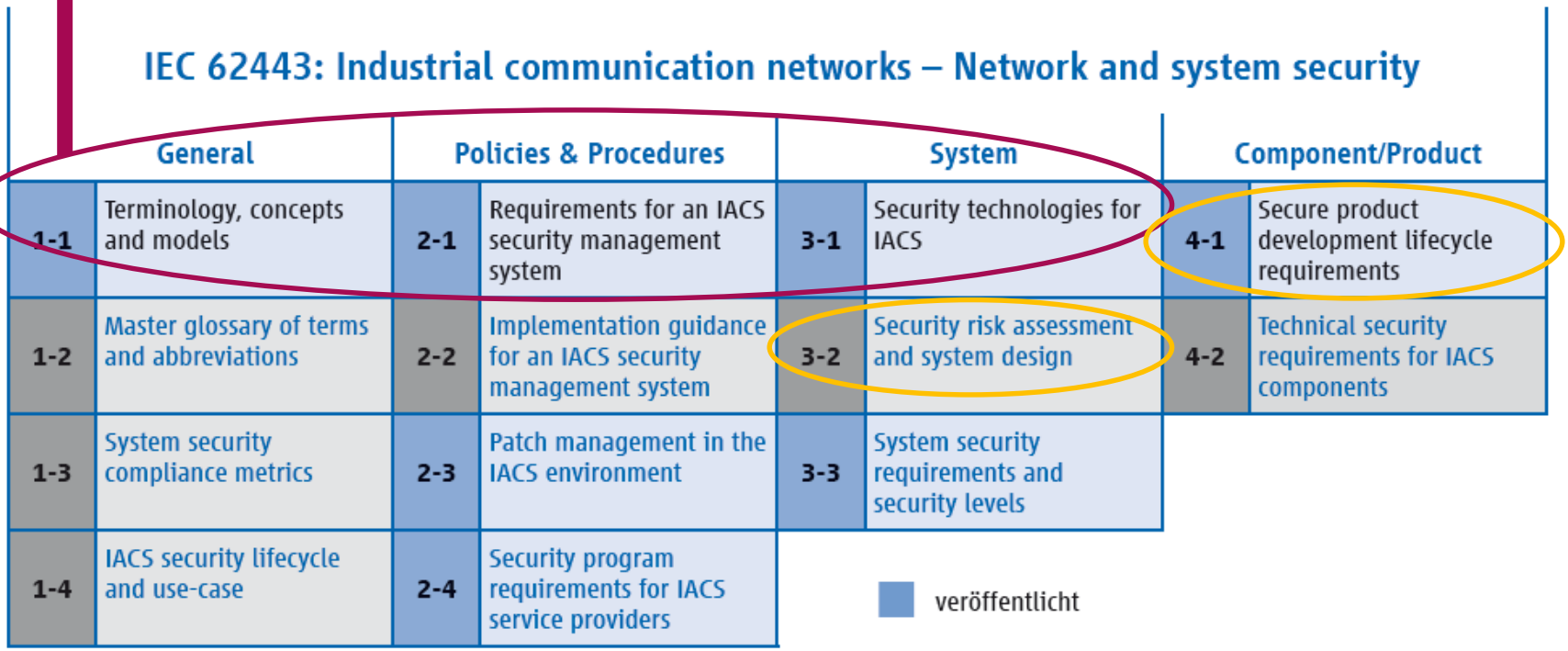


Introduction IEC 62443

- Why ?
  - Established norm for industrial automation, industry 4.0
  - FDA recognized (62443-1-1, 62443-2-1, 62443-3-1)
  - In 2016, first certification according to IEC 62443 in Germany by TÜV Süd
  - Offer connecting point to development process norm
  - Direct relationship to IEC 61508-1
    - *„7.5.2.2 If security threats have been identified, then a vulnerabilities analysis should be undertaken in order to specify security requirements. NOTE Guidance is given in IEC 62443 series.“* (Source: IEC 61508-1:2010)

Overview of IEC 62443

FDA recognized



IEC 62443: Industrial communication networks – Network and system security

General		Policies & Procedures		System		Component/Product	
1-1	Terminology, concepts and models	2-1	Requirements for an IACS security management system	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	Implementation guidance for an IACS security management system	3-2	Security risk assessment and system design	4-2	Technical security requirements for IACS components
1-3	System security compliance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-case	2-4	Security program requirements for IACS service providers				

veröffentlicht

Source: ZVEI

Security concept

62443-1-1

Security objective
(CIA)
- Confidentiality
- Integrity
- Availability

Threat-risk assessment
(Asset, Vulnerabilities, Threat, Consequence, Risk

62443-4-1

Process requirements for the secure development of product

Secure development life-cycle (SDL):
Security requirements, Secure design, Secure implementation, verification and validation

62443-3-2

Security risk assessment based on the concept of zone and conduit, threat, vulnerabilities, impact,…

Intended for: asset owner, sytem integrator, service provider,..

Concept, Design, Development

- Manufacturer‘s approach for device cybersecurity
  - Intended Use
    - To find the ground for optimal measures for safety and security
  - Intended Environment
    - Constrain the relevant attack scenarios
  - Threat / Risk Analysis (TRA)
  - Instruction for (secure) Use
    - Vulnerabilities that cannot be mitigated technically shall be documented as user measures
  - Use Secure Development Life-cycle

- Cybersecurity measures must not interfere with the essential function of the device
- Intended environment limits the impact (consequence) of the security threats

- Threat / Risk Analysis according to AAMI TIR 57

Risk = F(threats, vulnerabilities, impacts)

- Threat / Risk Analysis according to AAMI TIR 57
  - **Comparison of terminologies:**

ISO 14971	AAMI TIR 57
Harm	Harm* *(with extended definition)
Hazard	Vulnerability
Hazardous situation	Threat event
Probability of occurrence of harm	Likelihood of occurrence
Risk	Risk

Concept, Design, Development

- Medical device software – Software life cycle processes (IEC 62304)
  - Goal:
    - **Safety**
    - **Effectiveness**
  - What about security ?

Definition:

Security: protection of information and data so that unauthorized people or systems cannot read or modify them and so that authorized persons or systems are not denied access to them

What about security ? (IEC 62304)

Security requirements

Example includes:

- those related to the compromise of sensitive information
- authentication
- Authorization
- Audit trail, and
- Communication integrity

Regarding security aspects, it is still not sufficient !

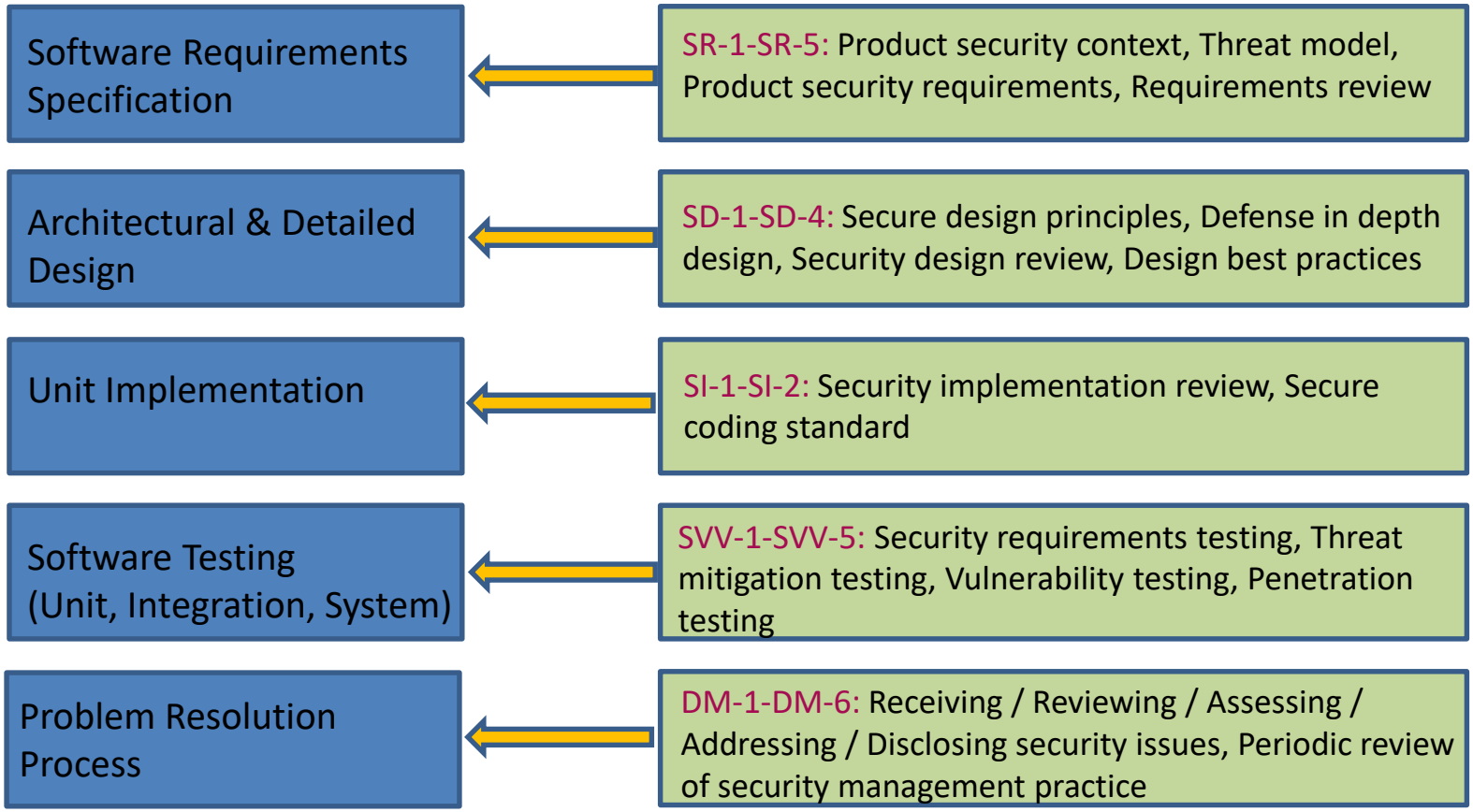
Concept, Design, Development

- Medical device software – Software life cycle processes (IEC 62304)
  - Use of only IEC 62304 is not sufficient for secure development life cycle (SDL) !

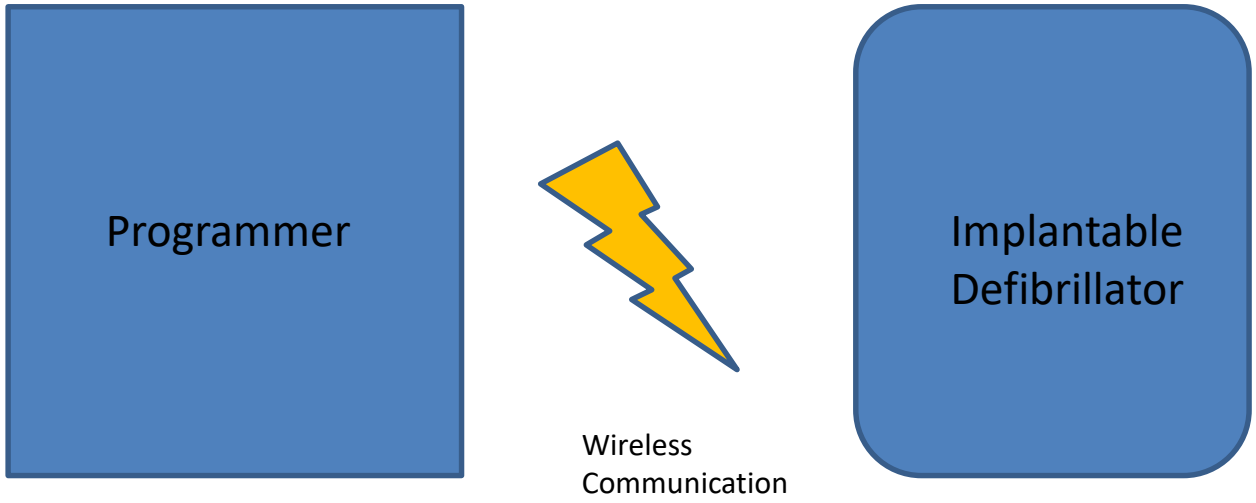
- Approach:
  - IEC 62304 + 62443-4-1
  - Based on process requirements in IEC 62304, activities and artifacts are extended to inclulde the security aspects

Concept, Design, Development

IEC 62304 + Security Concept according to IEC 62443-4-1



Case Study


Programmer
Wireless
Communication
Implantable
Defibrillator

Case Study

- Implantable Defibrillator
  - Intended Use (Essential function)
    - Transmit patient information wirelessly
    - Transmit device status wirelessly
    - Provide therapy
- Programmer
  - Intended Use (Essential function)
    - Set/Get patient information wirelessly
    - Set therapy parameter wirelessly
- Intended Environment
  - Clinic & hospital use

Case Study

Scenario

- The programmer and defibrillator use a static unique identifier with each transmission to provide authentication

Threat event

- „An attacker eavesdrops the wireless communication and captures the unique identifier and data packet. The attacker modifies the data, changes the therapy logic and send the data packet to the defibrillator.“

Impact

- Patient data disclosure -> Data breach
- Patient therapy modification -> Harm

Case Study

Security risk estimation

Risk ID	Asset	Threat	Vulnerability	Likelihood	Impact
1	Patient data	Attacker gets access to patient data	Lack of encryption on transmitted data	Medium	Medium: Disclosure of patient data
2	Patient therapy	Attacker manipulate the therapy by changing therapy parameter	Lack of authentication of transmitted data	Medium	High: Inappropriate therapy, death

Risk ID 1 ⇒ Confidentiality breach

Risk ID 2 ⇒ Integrity breach

Residual security risk estimation

Risk ID	Asset	Threat	Measure	Likelihood (Post-Mitigation)	Impact (Post-Mitigation)
1	Patient data	Attacker gets access to patient data	Cryptographic Encryption (e.g. symmetric key)	Low	Medium: Disclosure of patient data
2	Patient therapy	Attacker manipulate the therapy by changing therapy parameter	Cryptographic Authentication (e.g. Message Authentication Code (MAC))	Low	High: Inappropriate therapy, death

Secure Development Life-cycle

Summary

- IEC 62443 norm series could be used as a guideline for an addition to 62304

- Approach for device manufacturers
  - Formulate the Intended Use and the Intended Environment
  - Perform Threat/Risk Analysis (TRA)
  - Design/Develop the product by considering Secure Development Life-cycle
    - Use IEC 62443-4-1 with IEC 62304
  - Also consider other standard/guidance as appropriate, e.g UL standard, FDA guidance,..

Contact:
ittipan.kanluan@ceplus.eu

MEDICAL DEVICE & IN VITRO DIAGNOSTICS

REGULATORY AFFAIRS SOLUTIONS STRATEGIES

CE plus GMBH
MEDICAL DEVICES • IVD
Regulatory Affairs & More