„SERENE-IoT" - Safe and Secure Connected Medical Devices

Author: Gudrun Neumann, 22.11.2018

SGS TÜV SAAR

WHEN YOU NEED TO BE SURE

SGS

Agenda

1. SGS – TÜV Saar GmbH
2. Introduction SERENE-IoT
3. Relation Safety - Security
4. Example Risk Assessment

SGS-TÜV Saar GmbH

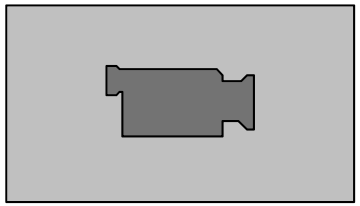
DAkkS Deutsche Akkreditierungsstelle D-IS-12088-02-01

DAkkS Deutsche Akkreditierungsstelle D-IS-12088-02-03

- SGS-TÜV Saar GmbH is a joint-venture between SGS-Group and TÜV Saarland e.V.
- Accredited inspection body for **Functional Safety and Cyber Security** according to ISO/IEC 17020:2012
- Accredited inspection body, type A, for **Medical Devices** according to ISO/IEC 17020:2012
- **Competence Center for Functional Safety and Cyber Security**
  - Headquarters in Munich, Germany
  - Branch Offices in Dortmund and Stuttgart, Germany
  - Local experts in Japan, Korea, China, Taiwan
- Member of relevant standardization committees, including ISO 26262 (Germany & international), IEC 61508 and Security

SERENE-IoT Project

- Secured & EneRgyEfficieNthEalth-care solutions for IoT market
- Use Cases (Demonstrators):
  - Remote Healthcare (moving care services from hospital to home)
  - Early detection of Methicillin-resistant bacteria
  - Fall Prevention/Detection



Best Practices for IoMT Security

- SGS-TÜV compares already existing Security Requirements with the new Threats
- A collection of existing international state-of-the art security requirements, not only in the area of medical devices, and our project experiences leads to
- A Synthesis of best practices for IoMT Security in terms of
  - Risk Analysis and Evaluation
  - Requirements
  - Mapping of Threats / Vulnerabilities / incident scenarios to the appropriate countermeasures
  - Test environment and procedures to show the efficiency of the countermeasures

Requirement Comparison
Legal versus Normative (1)

Topic	Requirements	
	Legal / Regulative	Normative
Location	**Country specific** regulations, laws and on European level harmonized regulations	**International** applied standards are available
Examples	SEAL	ISO/IEC 27001
Data Protection	Legal requirements included in specific Laws and directives	Requirements included in the standards
Examples	GPDR	IEC 62351-10, section 6

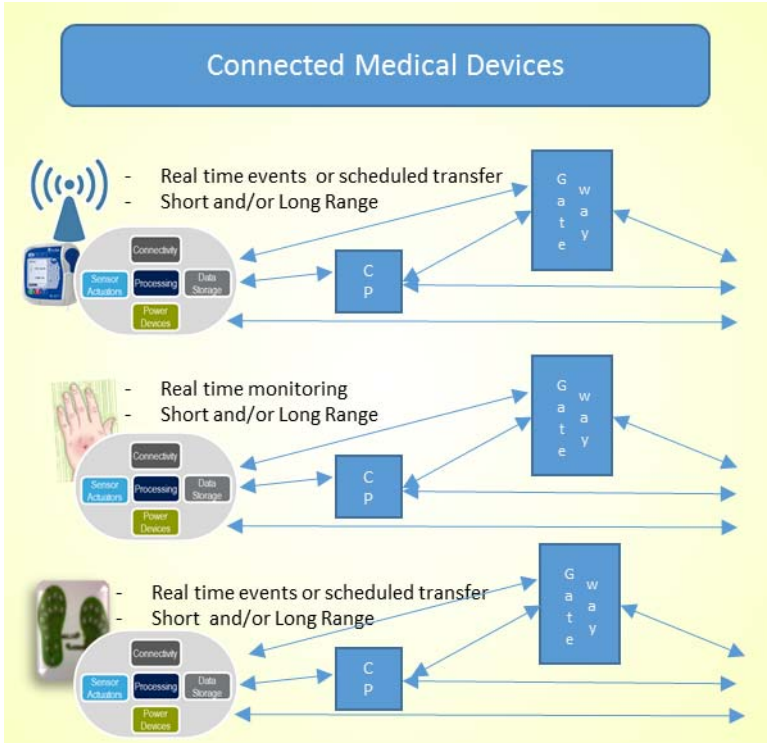
- This list is not complete. The intention is to show some differences.
- Seal of Cybersecurity: European Cyber Security Organization (ESCO); https://ecs-org.eu
- GPDR: General Data Protection Regulation, Regulation (EU) 2016/679

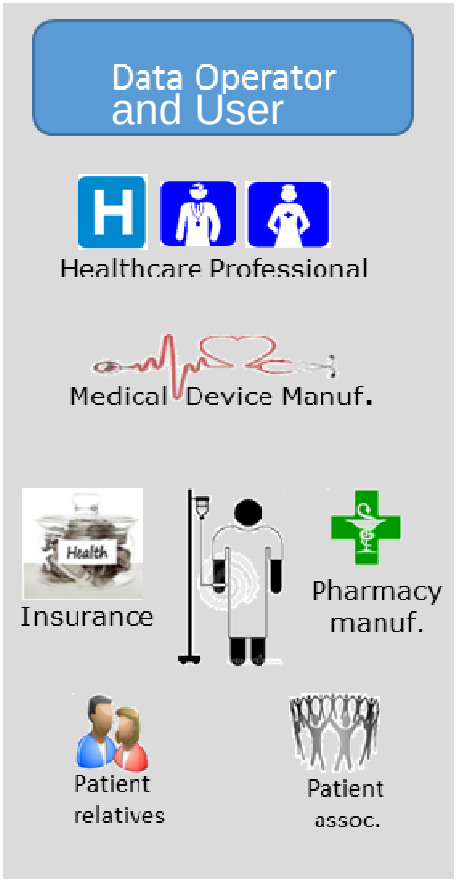
Requirement Comparison
Legal versus Normative (2)

Topic	Requirements	
	Legal / Regulative	Normative
Availability	Special Critical Infrastructure regulations	Business Continuity Management (BCM) for companies
Examples	IT-Sicherheitsgesetz	ISO 22301
Integrity	Special Critical Infrastructure regulations	Functional safety and Security standards requirements
Examples	NIST-Cybersecurity Framework	IEC 62443, IEC 61508

- This list is not complete. The intention is to show some differences.
- Critical Infrastructure: Power, Water and Communication Infrastructure in a country
- NIST: National Institute of Standards and Technology (USA)

SERENE-IoT Landscape





Security Objectives (CIA Triangle)

Confidentiality (and Privacy)

Availability

Integrity

Examples of Typical Problems

- Eavesdropper
- Data/Program are re-scheduled or inserted
- Fake Device
- Data Corruption

Methods to reach the Objectives

Humans

e.g. Awareness training

Processes

e.g. Information Security Management System (ISMS)

Technique

e.g. Firewall-HW, Face-Recognition-SW, RFID-Chip

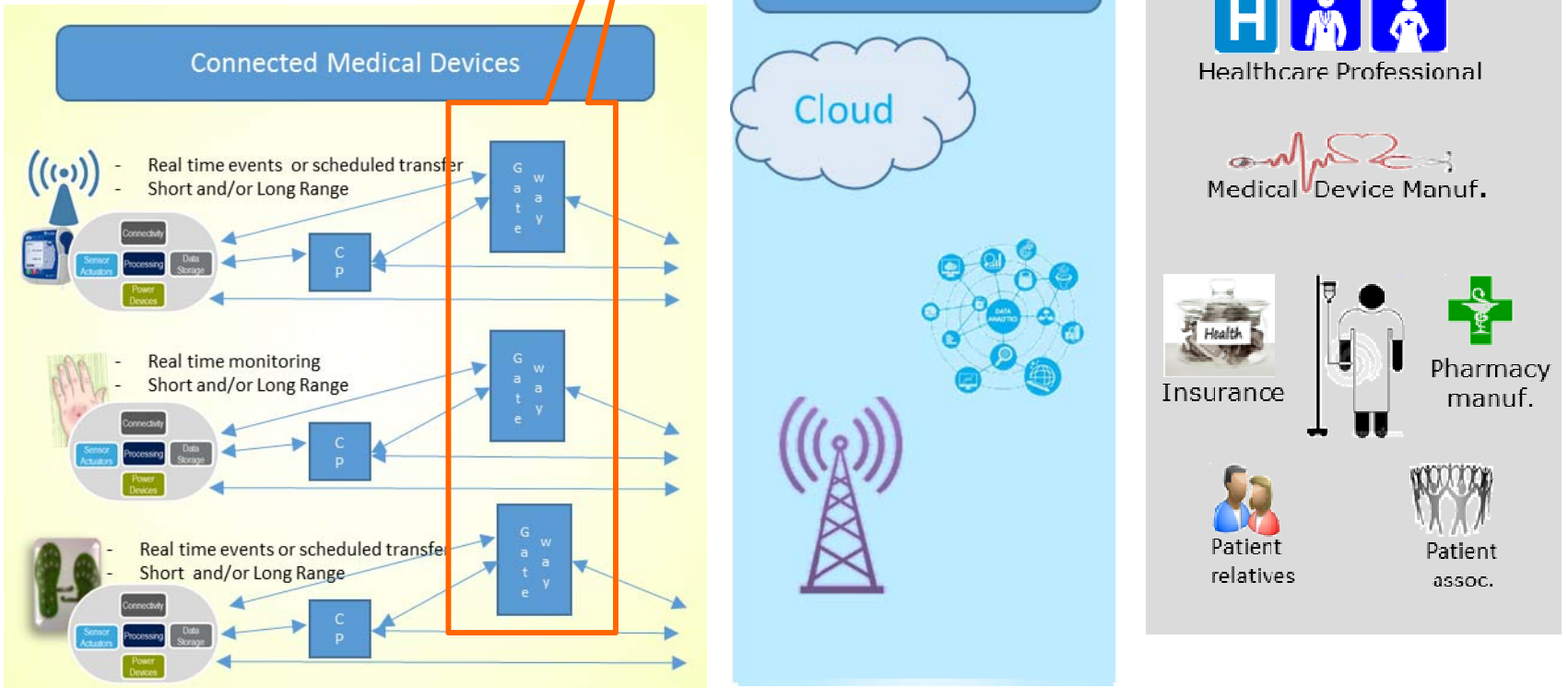
Cyber Security and Functional Safety Relationship & Analogies

Cyber Security	Functional Safety
Exploitation of vulnerabilities by an attacker shall be avoided	Harm due to failures shall be avoided
Avoid losses in • financial • operational • privacy • safety	Avoid harm to • life • health • environment • property

Analogies Cyber Security and Functional Safety engineering

Cyber Security	Functional Safety
Build Cyber Security into design	Build safety into design
Perform Thread Analysis and Risk Assessment (TARA)	Perform Hazard Analysis and Risk Assessment (HARA)
Derive Cyber Security requirements from Cyber Security goals	Derive safety requirements from safety goals
Requires Cyber Security culture	Requires safety culture
perform field observation	perform field observation

Risk Assessment
Example Mobile Gateways



System Definition and Assets

- Intended Use:
  - Gateway for Medical Device Data
- Characteristics:
  - Physically Location: Somewhere, between user and data cloud
  - Access Possibilities: physical on-site and remote
- Assets:
  - Encrypted communication keys with the medical device
  - Authentication information that grants access to specific functionalities of the medical device
  - Personal and medical information
  - Algorithms of gateway control software

Risk Definition

Security	Safety
IEC TS 62443-1-1:2009, 3.2.87 Risk is the expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.	ISO 14971:2007, 2.16 Risk is the combination of the probability of occurrence of harm and the severity of that harm

Hazards

Security	Safety
Identification of Threats Identification of Vulnerabilities Incident scenario description	Identification of hazards
- passive : Side-channel attacks, reverse-engineering - active : Fault injection	- Mechanical energy - Vibration - EMC - Electrical

Risk Assessment and Analysis

Security	Safety
Threats (incl. assets and vulnerability) are ranked acc. to level of risk (including likelihood and consequences of these risks)	Risk evaluation
- passive: Side-channel attacks, reverse-engineering: risk for financial loss for gateway manufacturer is high	- Vibration: risk low because device not in motion

Defining Countermeasures

Security	Safety
Risk Treatment a) Risk Modification (by changing the likelihood and/or consequences) b) Risk Retention (based on the risk acceptance criteria or by informed decision) c) Risk avoidance (by deciding not to start or continue with activity that rises to the risk) d) Risk Sharing (with other parties by insurance, sub-contracting or risk financing	Risk control options - Design - Safety Functions - Information
- Against Side-Channel Analysis : Strong encodings, static masking	- Mechanical design appropriate - Device self tests

Risk Evaluation and Acceptance

Security	Safety
Decision based on - Likelihood of occurrence and - Grade of Consequences	Decision based on - Severity of Harm - Probability of occurrence of hazardous situation - Probability of exposure
Security	**Safety**
Risk can be accepted by manufacturer	- If risk is not tolerable, more countermeasures needed

SERENE-IoT Questions

- Which security requirements are mandatory for medical device IoT solutions?
- Is there a common approach of compliance and assessment criteria?
- Which test equipment is necessary?

Our Contacts:

Munich, Germany (Headquarters)
SGS-TÜV Saar GmbH
Functional Safety & Cyber Security
Hofmannstrasse 50,
81379 München
Phone +49 89 787475-271
fs@sgs.com

Dortmund, Germany (Branch Office)
SGS-TÜV Saar GmbH
Joseph-von-Fraunhofer-Str. 13,
44227 Dortmund
Phone +49 231 9742-7323
do.fs@sgs.com

Stuttgart, Germany (Branch Office)
SGS-TÜV Saar GmbH
Am Ostkai 15-17
70237 Stuttgart
Phone: +49 711 90702-674
s.fs@sgs.com

Thank You, For Your Attention