PANACEA Security-by-Design Framework

RINA-C
Martina Bossini Baroggi
Agenda

- Healthcare sector context
- PANACEA project response
- Security by Design Approach
- PANACEA Security-by-design Framework
- Innovation points
Healthcare Sector context

➢ Lack of cyber awareness within healthcare sector

➢ Immediate and industrywide action

➢ Development of a programmatic approach to identification, mitigation, and remediation of risk

➢ Introduction of security aspects (cyber risk)
Security By Design Framework (SbDF), takes into account a typical assessment and system monitoring audit workflow with the support of specific solutions addressing conformity assessment (through by compliance schemes, CST) and risk assessment (addressing cybersecurity and engineering aspects, SDSP)

- SDSP – Secure Design Support Platform
- CST – Compliance Support Tool
Security by Design Framework (SbDF) has been proposed in order to overcome design limitations of medical devices and medical systems which currently don’t specifically or poorly include security engineering aspects regarding cyber risks.

**Security-by-design:** Approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attacks as possible through different measures such as continuous testing, authentication safeguards and adherence to best programming practices.

**Key point:** It is important for a device/system to be designed from the foundations to be secure. Therefore, good cyber security measures should be integrated into the design process.
Security by Design Approach

1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis and extraction
4. Conformity assessment
5. Risk assessment

Liaison with ENISA analysis on potential candidates of cybersecurity certification schemes [1]

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
1. **Context definition** Healthcare Domain, Medical device Lifecycle

2. Relevant standards/certification schemes identification

3. Standards mapping, gap analysis and extraction

4. Conformity assessment

5. Risk assessment

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
# Security by Design Approach

<table>
<thead>
<tr>
<th>Regulations and Standards</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>MDR (REGULATION (EU) 2017/745)</td>
<td>REGULATION (EU) 2017/745 on medical devices,</td>
</tr>
<tr>
<td>IVDR (REGULATION (EU) 2017/746)</td>
<td>REGULATION (EU) 2017/746 on in vitro diagnostic medical devices</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>Information Security Management</td>
</tr>
<tr>
<td>IEC 80001-1:2010</td>
<td>Application of risk management for IT-networks incorporating medical devices Roles, responsibilities and activities</td>
</tr>
<tr>
<td>ISO 13485:2016</td>
<td>Medical devices-Quality management systems-Requirements for regulatory purposes</td>
</tr>
<tr>
<td>ISO 14971</td>
<td>Medical Devices – Application of Risk Management to Medical Devices</td>
</tr>
<tr>
<td>IEC 62304:2006</td>
<td>Medical device software - Software life-cycle processes</td>
</tr>
</tbody>
</table>

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
Security by Design Approach

<table>
<thead>
<tr>
<th>Regulations and Standards</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>MDR (REGULATION (EU) 2017/745)</td>
<td>REGULATION (EU) 2017/745 on medical devices,</td>
</tr>
<tr>
<td>IVDR (REGULATION (EU) 2017/746)</td>
<td>REGULATION (EU) 2017/746 on in-vitro diagnostic medical devices</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>IEC 80001-1:2010</td>
<td>Application security for medical devices incorporating an information security management system</td>
</tr>
<tr>
<td>ISO 13485:2016</td>
<td>Medical devices - Application of conformity assessment for regulatory purposes for medical devices</td>
</tr>
<tr>
<td>ISO 14971</td>
<td>Medical Devices - Application of Risk Management to Medical Devices</td>
</tr>
<tr>
<td>IEC 62304:2006</td>
<td>Medical device software - Software life-cycle processes</td>
</tr>
</tbody>
</table>

ENISA: Mapping of OES Security Requirements to Specific Sectors

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis
4. Conformity assessment
5. Risk assessment

- **Standards Harmonization**
- **Checklist** extraction:
  the most relevant articles in terms of cybersecurity were extracted in order to define checklists useful to guide the user to assess conformities
- **Taxonomies** extraction:
  assets/vulnerabilities/threats/security controls/scenarios extraction

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis and extraction
4. Conformity assessment
5. Risk assessment

Security by Design Approach

CST: Compliance Support Tool

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis and extraction
4. Conformity assessment
5. Risk assessment

SDSP: Secure Design Support Platform

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes
From a technological point of view, the **PANACEA Security-by-design Framework** is composed of two solutions:

---

Secure Design Support Platform (SDSP)

It will support the security of a medical device/information system in development, by providing a software platform for risk assessment analysis over the system/software in development. Each risk assessment analysis may produce security controls that will lead to new requirements to be embedded in the system in order to improve its resulting security.

---

Compliance Support Tool (CST)

It will support the quality assurance process during the whole lifecycle of a medical device/system, in order to put in place an assessment audit of the process supporting health devices/systems providers/quality responsible, ensuring compliance to current standards in the health sector.

---

www.panacearesearch.eu
**Introduction of security aspects (cyber risk) since the beginning of the initial design process: from requirements phase to deployment phase and till the operational phase.**

**Design PROCESS:** The CST covers the compliance through the whole process.

**Design contextualized OUTPUT:** The SDSP supports the user to perform the risk assessment in each phase of medical device life-cycle.
Innovation points

- Development of a tool (CST) that will support the user to verify the compliance to standards relevant for cyber security during the whole life-cycle of a medical device or eHealth application;

- Development of a tool (SDSP) that will provide a risk-based approach to refine the security controls of a medical device/system during its development;

- Extraction of taxonomies (vulnerabilities/threats/security controls) from health care most relevant standards in order to take into consideration during risk assessments scenarios specific for this sector;

- Security-by-design principles support through the analysis of the security level/scenarios will support manufacturers in decision-making of possible security controls to implement during software/system engineering early phases;

- Security-by-design Framework takes into consideration the ENISA approach and guidelines for the analysis of potential candidates of certification schemes.