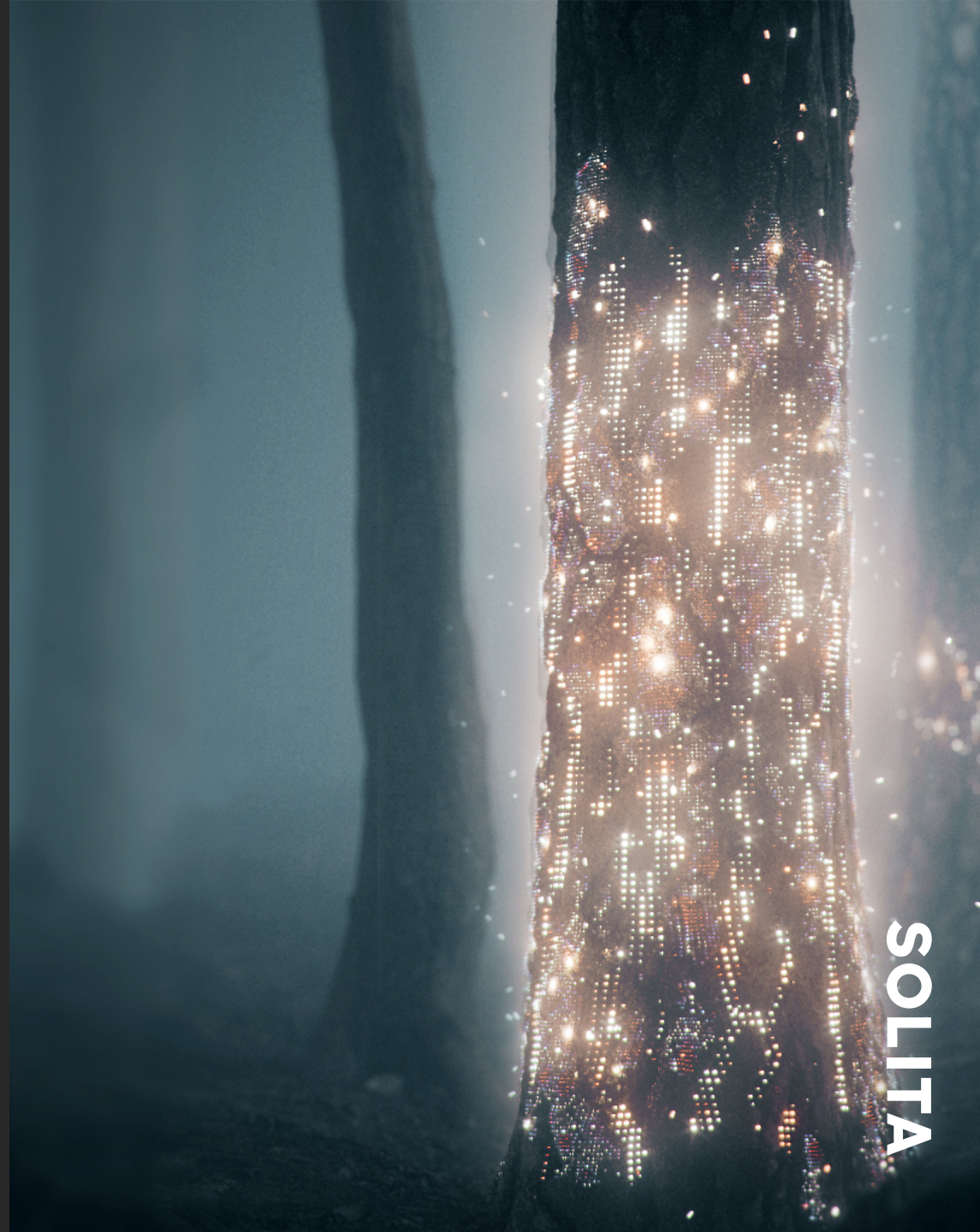
On Medical Device Cybersecurity Compliance in EU

Tuomas Granlund @solita.fi
SEH 2021



Outline

1. Background & Challenges
2. Towards cybersecurity compliance
3. Conclusions

Background

Regulatory landscape - cybersecurity

- Medical device development is a highly regulated domain in European markets
  - Regulations aim to ensure safety and effectiveness of the devices
  - Software development is no exception, because software with an intended medical use is considered a medical device as such.
- Before placing medical devices on the European Union market, a device must have the CE mark
  - The CE marking is manufacturer's claim that the product meets all relevant EU regulatory requirements
- The EU regulatory framework is currently undergoing change, and the new regulations take a more explicit position on devices' cybersecurity aspects
  - Cybersecurity is addressed from a broad perspective in the new legislation
    - Medical Device Regulation (MDR) 2017/745 and in the In Vitro Diagnostic Medical Device Regulation (IVDR) 2017/746
    - Guidance document: MDCG 2019-16, Guidance on Cybersecurity for medical devices

Common challenges for the manufacturers

- The gap between the new requirements and the existing implementation
  - Safety risks emerging from the cybersecurity dimension should already be appropriately managed today
  - However, many manufacturers seem to have shortcomings in their security culture and processes
- Identification of cybersecurity requirements
  - The EU regulatory framework is characterized by a certain level of complexity
  - The requirements in concern many interconnected processes, and are divided into different sections of the document
- Implementing security actions in required processes
  - Development and manufacturing, Post-market surveillance
  - Manufacturers need resources with in-depth knowledge about cybersecurity

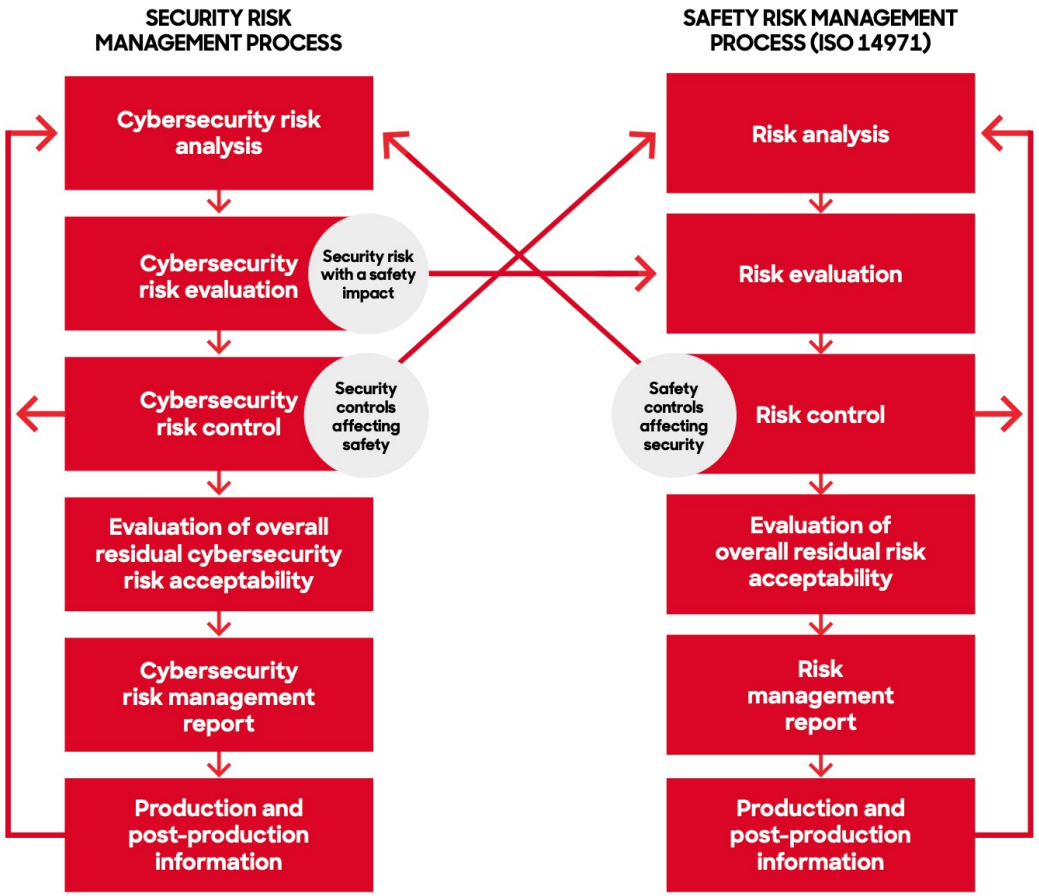

Towards Cybersecurity
Compliance

1. Risk relationship between safety and security

- Medical device risks are typically managed in accordance with ISO 14971 standard
  - As a result, the perspective tend to focus solely on safety-related risks, i.e., risks that affect the (physical) safety of the patients or the users.
- New regulations require a broader view of risk to address the new cybersecurity requirements
  - Three main types of risks:
    - Security risk without a safety impact
    - Security risk with a safety impact
    - Safety risk without relation to security

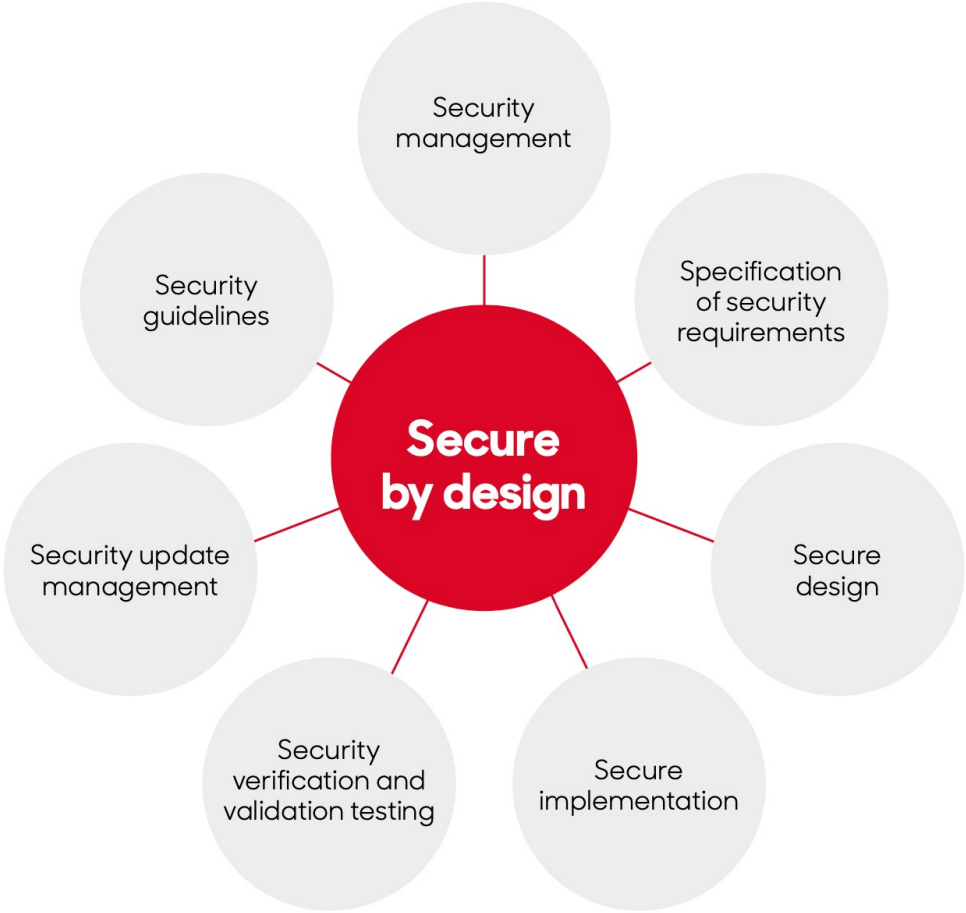
2. Aligned safety and security risk management processes

- Safety risk management process is one of the core processes of MD manufacturing
  - It is essential that the risk management process is working efficiently!
- Due to a broader perception of risk, a separate companion process is recommended for security risks
  - To ensure complete and consistent security management
- If a security risk has a safety impact, it will be propagated as an input item to safety risk evaluation
  - As new risk controls may introduce new risks, the impacts must be analyzed from both safety and security perspectives



3. Secure design and development lifecycle

- Security risk management is an integral part of the secure development lifecycle
  - Potential security threats need to be identified with a systematic approach, such as threat modelling
- Medical device software development process is typically implemented according to IEC 62304
  - It is recommended to extent the existing development process with cybersecurity activities
  - This approach is supported by the forthcoming standard IEC 80001-5-1



4. Post-market cybersecurity activities

- The new regulations require a more proactive approach to post-market surveillance
- In general, the number of safety-related hazards of a medical device will stay relatively stable over time
  - The same does not hold when considering cybersecurity threats, so post-market cybersecurity activities need special consideration
  - The key to efficient process is identifying new changes in security environment proactively and resolving issues timely yet without compromising safety or compliance

Conclusions

Conclusions

- In our paper,
  - we address the new cybersecurity requirements and
  - propose an approach that can be used to explain the most fundamental aspects of cybersecurity compliance:
    - Risk relationship between safety and security
    - Well-aligned safety and security risk management processes
    - Practical implementation within well-controlled secure design and development process
    - Cybersecurity aspects must be considered also in post-market activities
- Call for action:
  - Manufacturers need to improve their culture of cybersecurity and implement the new requirements in their processes
  - The expectations of the regulatory authorities need to be expressed more clearly

Thank you!

tuomas.granlund@solita.fi