Cybersecurity for Medical Devices – Crash Course

TRAINING FACTSHEET

Date: January 22 – 26th 2024, Online
Duration: 16:30 hours | 5 x 2:00 – 5:30 PM CET
5 x 09:00 AM– 12:30 PM EST

Veranex trainer:
Somashekara Koushik Ayalasomayajula
Quality & Regulatory Affairs Director

About the speaker:

Somashekara Koushik Ayalasomayajula is a polymer engineer with 5+ years of experience within the medical device industry in product development and quality & regulatory affairs. Koushik leads digital health team focusing on emerging topics like AI/ML, cybersecurity and also supports our courses related to quality and regulatory affairs, deploying QMS according to ISO 13485, integrating MDSAP, ISO/IEC 27001 (ISMS), GMP requirements and in the preparation of technical documentation of medical devices for global regulatory submissions. Koushik is ASQ certified Medical Device Auditor (ASQ-CMDA) and holder of RAC Devices from RAPS.

CertX Trainer:
Loan Bétend
Cyber Security Specialist
CertX AG

About the speaker:

Loan, a cybersecurity specialist at CertX AG, pursued his studies in Information and Communication Technology, specializing in embedded and mobile systems, at the University of Applied Science Fribourg. He then accumulated industrial experience through projects in the automotive, avionics, and industrial environments, serving as a consultant. Currently, Loan is part of the first Swiss certification body for functional safety and cybersecurity, where he contributes as an auditor and trainer for product and operational technology (OT) cybersecurity.

TRAINING OBJECTIVES:

This training is organized into 5 modules with the goal of providing participants with an extended understanding of the requirements related to medical device software. The individual modules link key regulatory and technical considerations related to developing medical device software, with a specific focus on cybersecurity requirements. The training is aimed at any software engineer, product manager, regulatory affairs specialist, or regulatory manager seeking to enhance their competence in this rapidly developing domain.

TRAINING CONTENT:

Module 1: Key requirements for marketing medical device software
(3:30 hours)

- When would my software qualify as a medical device?
- How do I classify my software under the Medical Device Regulation?
- How is cybersecurity linked with regulatory requirements?
- What is the scope of my responsibility toward cybersecurity?
- Which guidance and standards can help me meet these requirements?

Module 2: IEC 62304: Medical device software life cycle processes
(3:30 hours)

- How do I develop medical device software within a quality management system?
- How do I manage vulnerabilities within the risk management process?
- What is Software Safety Classification under IEC 62304?
- How do I develop a verification and validation plan for my software?
- How do I test cybersecurity requirements?

Module 3: IEC 62443-4-1: Tailoring of the SW life cycle process with cyber security
(3:30 hours)

- How to map the generic model of IEC 62443 to specific MD concerns
- What are the relevant parts of IEC 62443 and how to use them?
- How to extend IEC 62304 to cover advanced cyber security aspects?
- Introduction to cyber security principles and methods
- Use case – Threat Analysis and Risk Assessment (TARA) – Phase 1
- Proposition of Cyber secure MD Software lifecycle

Module 4: IEC 62443-4-2/3-3: Application of cyber security related technical requirements for MD
(3 hours)

- What are the relevant parts of IEC 62443 and how to use them?

- Introduction to cyber security primitives and algorithms
- State-of-the-Art of Cyber security for IoT applied to Medical industry
- Use case – Threat Analysis and Risk Assessment (TARA) – Phase 2

Module 5: Demonstrating Conformity
(3 hours)

- What are the key steps to ensure compliance with cybersecurity requirements for my CE Mark
- How do I generate and organize technical documentation?
- What is the IEC 62443 certification scheme and why should I pursue it?
- What shall I present to my notified body during a CE Mark conformity assessment process?
- How do I leverage my Post Market Surveillance process to further demonstrate compliance on my CE Marked software?

TRAINING FORMAT:

The training is a partnership between Veranex and CertX. The training will be delivered online through 5 sessions of approximately 3 to 4 h during a week crash course.

- Presentation with interactive discussions
- Exercises during the training
- End of training assessment (participants will receive training certificate)

WHO SHOULD ATTEND:

The training is aimed at any software engineer, product manager, regulatory affairs specialist, or regulatory manager seeking to enhance their competence in this rapidly developing domain.

PRICE:

EUR 950 incl. course material and certificate

Registration: education-veranex.talentlms.com
Contact: MDD-training@veranex.com