

Cybersecurity in Medical Devices and the role of IEC 81001-5-1



Mehr Wert.
Mehr Vertrauen.

Add value.
Inspire trust.

Jan Küfner



- SPS Cyber Security for medical devices
 - defining minimum requirements (according to MDR, MDCG & standards)
 - defining focal areas
 - creating templates
 - establishing UAA penetration testing
 - creating and conducting training
for market authorization assessments & MDR audits for medical devices.
- Cyber Security Assessor
- Lead Auditor
- Penetration Tester
- Member of standardization committee

- Patient harm
- GDPR, HIPAA fines
- Damage of reputation, Loss of sales
- Regulatory compliance
- ...



47 pages on Cybersecurity requirements

1
sentence indirectly referring to
(Cyber)security

MDD

4
paragraphs on Cyber-
security requirements

MDR
(into force, since May 2017)

MDCG 2019-16

Today

End of transition
(May 2021)

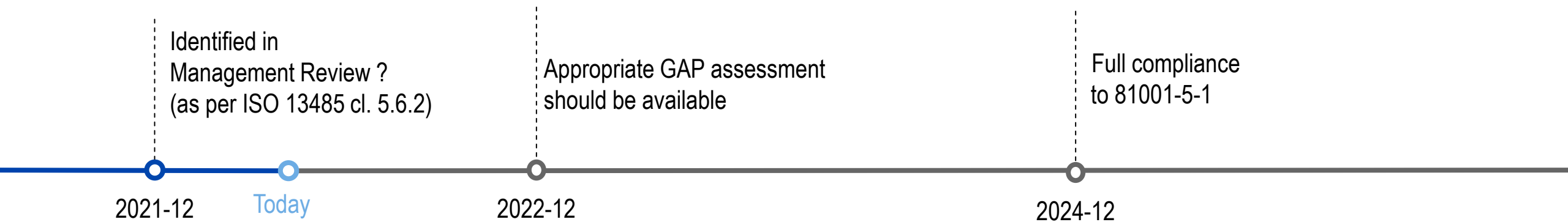


IEC 81001-5-1:2021

Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

ICS › 35 › 35.080

Published 2021-12



EU Cyber Security standards

Medical device requirements

- IEC TR 60601-4-5 (published, trial)

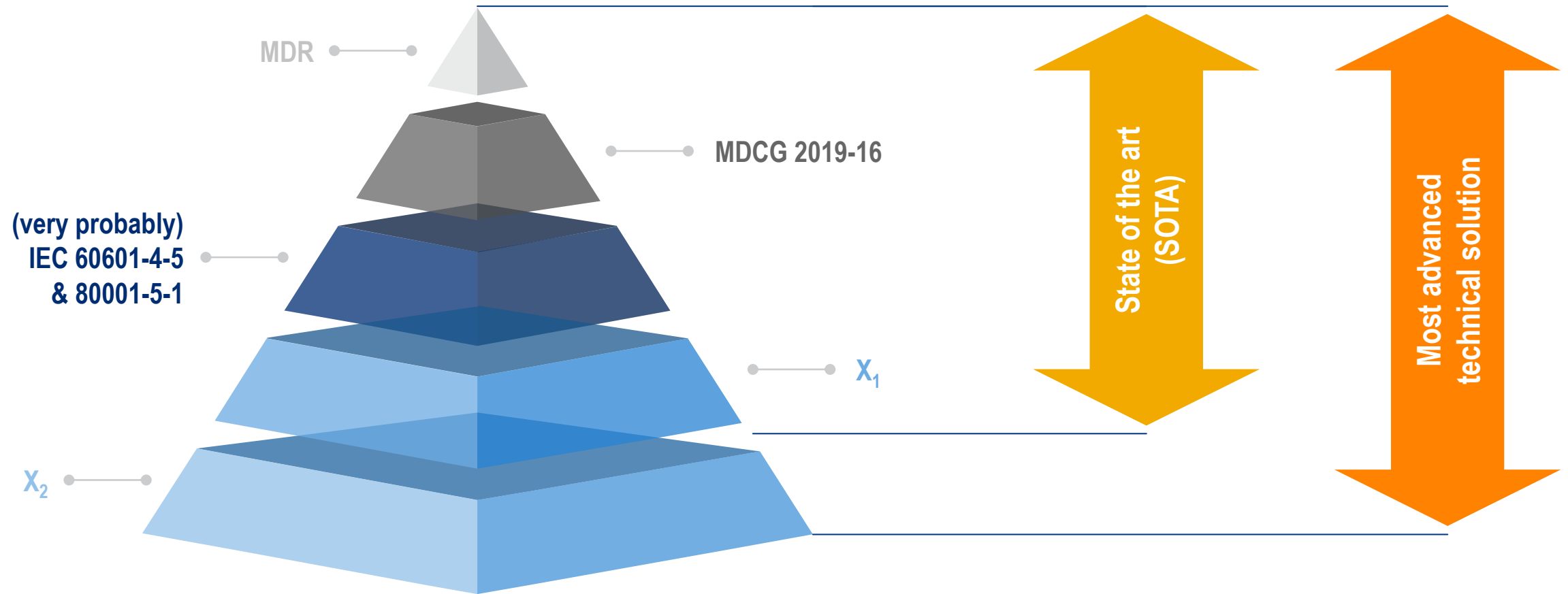
QMS (RnD) requirements

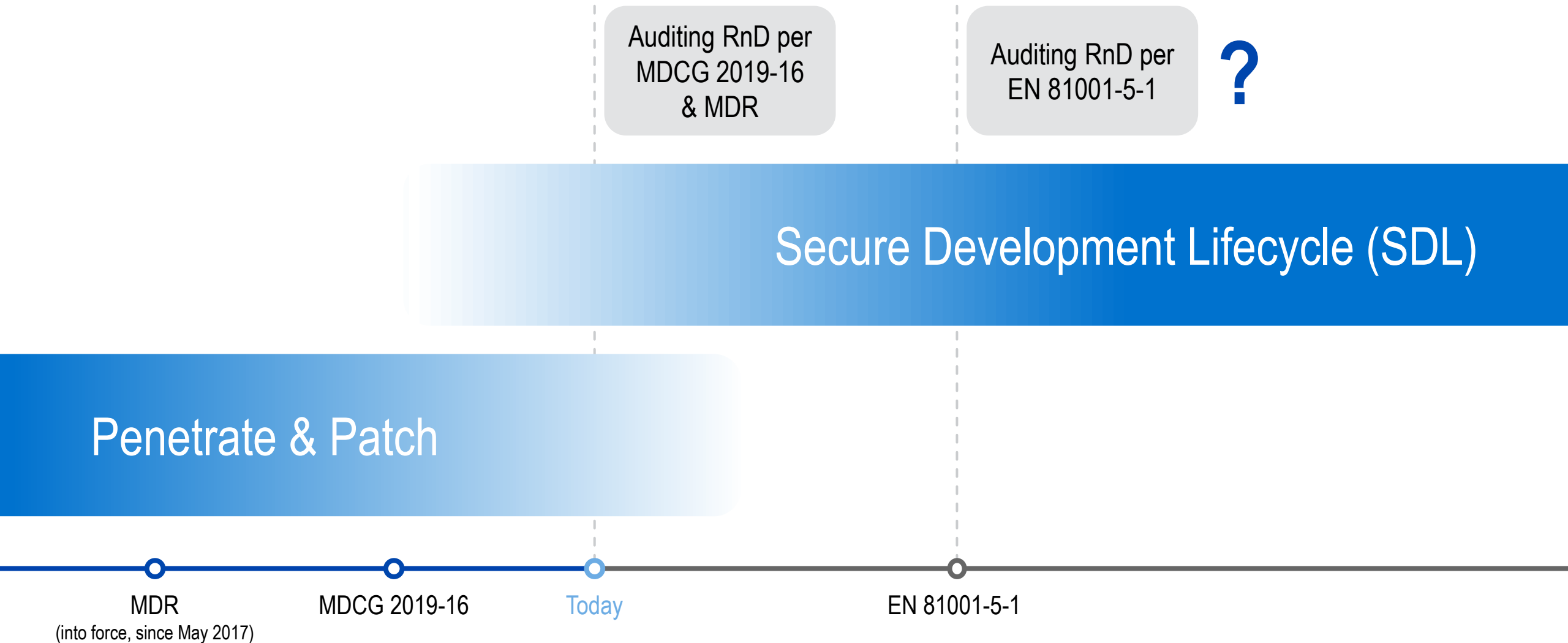
- 81001-5-1 (published)



Very likely to replace the numerous guidelines, which we have now







IEC 62304:2006/Amd 1:2015

IEC 81001-5-1:2021

CONTENTS	
FOREWORD	7
INTRODUCTION	11
1 Scope	17
1.1 * Purpose	17
1.2 * Field of application	17
1.3 Relationship to other standards	17
1.4 Compliance	17
2 * Normative references	19
3 * Terms and definitions	19
4 * General requirements	27
4.1 * Quality management system	27
4.2 * RISK MANAGEMENT	27
4.3 * Software safety classification	27
5 Software development PROCESS	27
5.1 * Software development planning	27
5.2 * Software requirements analysis	27
5.3 * Software ARCHITECTURAL design	27
5.4 * Software detailed design	27
5.5 * SOFTWARE UNIT implementation and verification	27
5.6 * Software integration and integration testing	27
5.7 * SOFTWARE SYSTEM testing	27
5.8 * Software release	27
6 Software maintenance PROCESS	27
6.1 * Establish software maintenance plan	27
6.2 * Problem and modification analysis	27
6.3 * Modification implementation	53
7 * Software RISK MANAGEMENT PROCESS	55
7.1 * Analysis of software contributing to hazardous situations	55
7.2 RISK CONTROL measures	57
7.3 VERIFICATION of RISK CONTROL measures	57
7.4 RISK MANAGEMENT of software changes	59
8 * Software configuration management PROCESS	59
8.1 * Configuration identification	59
8.2 * Change control	61
8.3 * Configuration status accounting	61
9 * Software problem resolution PROCESS	61
9.1 Prepare PROBLEM REPORTS	61
9.2 Investigate the problem	63
9.3 Advise relevant parties	63
9.4 Use change control process	63
9.5 Maintain records	63
9.6 Analyse problems for trends	63
9.7 Verify software problem resolution	65
9.8 Test documentation contents	65

<https://www.iso.org/standard/64686.html>

CONTENTS	
FOREWORD	5
INTRODUCTION	7
0.1 Structure	7
0.2 Field of application	8
0.3 Conformance	8
1 Scope	10
2 Normative references	10
3 Terms and definitions	11
4 General requirements	18
4.1 Quality management	18
4.1.1 Quality management system	18
4.1.2 Allocation of responsibilities	18
4.1.3 Applicability	18
4.1.4 Use of third-party suppliers	19
4.1.5 Improvement	19
4.1.6 Security-related issues	19
4.1.7 SECURITY defect management	19
4.1.8 DOCUMENTATION review	20
4.1.9 IMPLEMENTATION	20
4.1.10 Mitigation relating to risk transfer	20
4.1.11 PROCESS	21
4.1.12 Planning	21
4.1.13 LIFE CYCLE PROCESS	21
4.1.14 Environment SECURITY	21
4.1.15 Standards	21
4.1.16 Requirements analysis	21
5.2.1 HEALTH SOFTWARE SECURITY requirements	21
5.2.2 SECURITY requirements review	22
5.2.3 SECURITY risks for REQUIRED SOFTWARE	22
5.3 Software architectural design	22
5.3.1 DEFENSE-IN-DEPTH ARCHITECTURE/design	22
5.3.2 Secure design best practices	22
5.3.3 SECURITY architectural design review	23
5.4 Software design	23
5.4.1 Software design best practices	23
5.4.2 Secure design	23
5.4.3 Secure HEALTH SOFTWARE interfaces	23
5.4.4 Detailed design VERIFICATION for SECURITY	24
5.5 Software unit implementation and VERIFICATION	24
5.5.1 Secure coding standards	24
5.5.2 SECURITY implementation review	24
5.6 Software integration testing	25
5.7 Software system testing	25
5.7.1 SECURITY requirements testing	25
5.7.2 THREAT mitigation testing	25

<https://www.iso.org/standard/76097.html>

Chapters of 81001-5-1 are very similar to 62304.
→ 81001-5-1 can easily be adapted to current development processes.

IEC 81001-5-1:2021 & ISO 14971:2019 & MDCG 2019-16

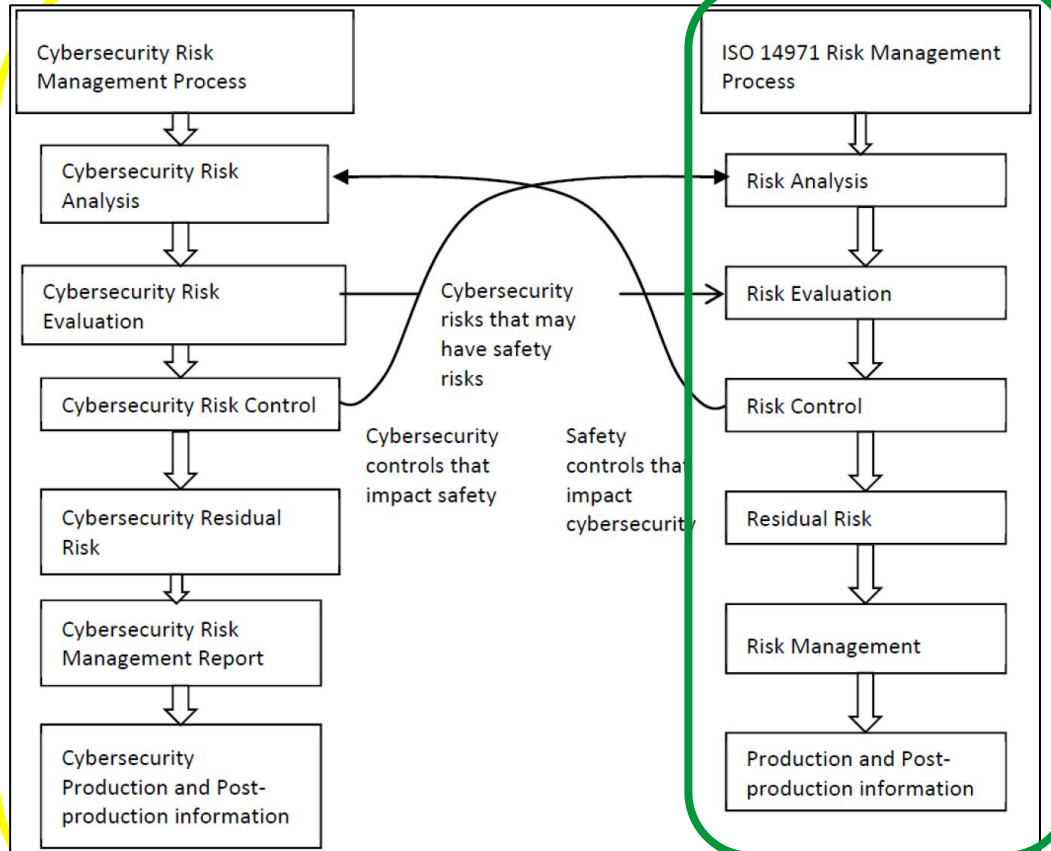
81001-1-5-1

cl 7.2

cl 7.3

cl 7.4

cl 7.5



MDCG 2019-16

No separate security risk process

MDCG 2019-16

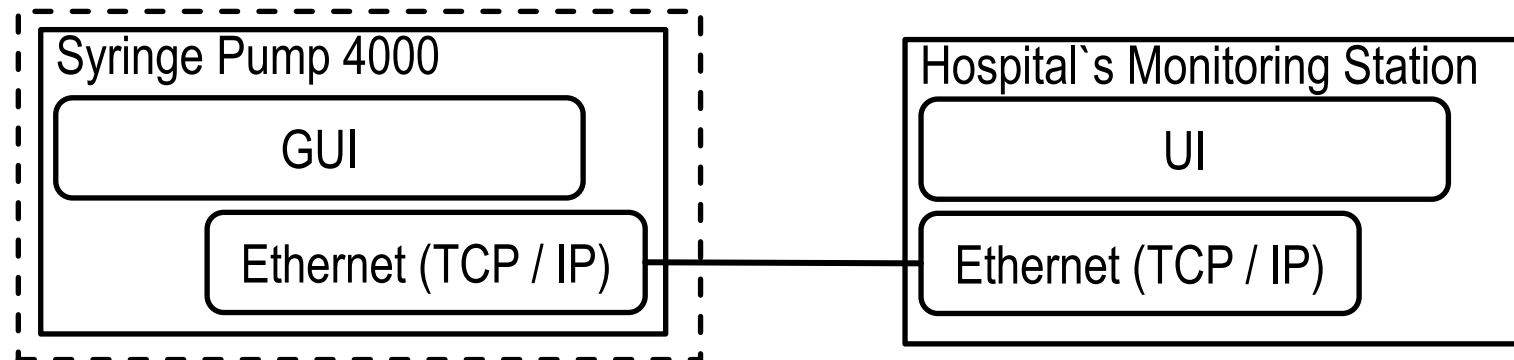
Cybersecurity should be covered by the existing risk management process with added requirements and documentation for cybersecurity

MDCG 2019-16

These ACTIVITY(s) shall be employed to ensure that all PRODUCTS shall have a THREAT MODEL specific to the current development scope of the PRODUCT with the following characteristics (where applicable):

- a) correct flow of categorized information throughout the system;
- b) TRUST BOUNDARIES;
- c) PROCESSES;
- d) data stores;
- e) interacting external entities;
- (...)

81001-5-1 cl.7.2



Common pitfalls for recent MDR Technical Documentation submissions

- Bad or missing system diagram (e.g. Data Flow Diagram DFD)
- Non-systematic cyber security risk management
(Tipp: use STRIDE)
- Bad or missing pen-testing
 - Tester not skilled enough
 - Tester not independent
 - Non appropriate tools used
 - Testing depth insufficient
 - Testing scope too narrow
 - Test house lacks medical expertise
- Bad security concept

The **primary means** of security verification and validation is testing. Methods can include security feature testing, fuzz testing, **vulnerability scanning** and **penetration testing**

MDCG 2019-16 section 3.7

TÜV SÜD
opinion

Penetration testing & vulnerability scanning
needs to be conducted under MDR

Medical Device Penetration Testing



USA

- Trainings (Presential & Online), Security Concept Evaluation
- Available (Partners)

Germany & Europe

- Trainings, Security Concept Evaluation and Cybersecurity testing capabilities

Japan

- Trainings (Online), Security Concept Evaluation
-



Abtin Rad

abtin.jamshidirad@tuvsud.com

Available

Singapore

- Trainings (Online), Security Concept Evaluation
- Available (Shared Service Center)

- Products Available per region
- Cyber Security Laboratory

UPDATED
incl. 81001-5-1 & 60601-4-5



Add value.
Inspire trust.

MDR Cyber Security Risk Management 2 Days ONLINE TRAINING

This course will provide you with key knowledge, to conduct efficient Cybersecurity Risk Management under the new requirements of the Medical Device Regulation (MDR) and MDCG 2019-16, 81001-5-1 & 60601-4-5. Through examples and group work you will gain in depth knowledge on relevant threat modelling techniques, risk assessment strategies, secure design principles and documentation needs.



<https://www.tuvsud.com/en-us/services/training/e-learning-courses/mdr-cybersecurity-risk-management>