Add value.
Inspire trust.

Digital Dialogues

You ask. Our experts answer.



Your partner for global MedTech market access

24 to 27 October 2022

Vol. 4



The role of IEC 81001-5-1 in Cybersecurity

Speaker:

Jan Küfner

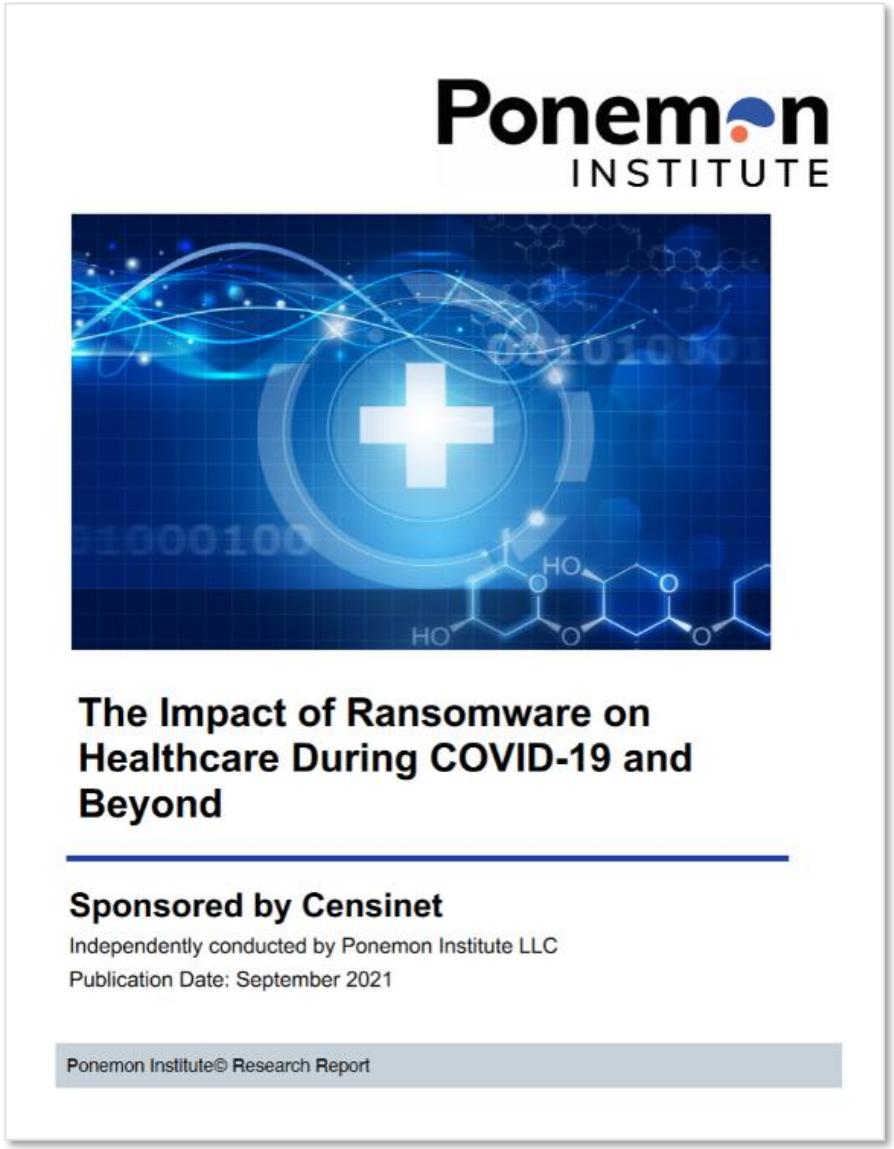
Senior Product Specialist
Cybersecurity
Medical Health Services

Focal areas:
Cybersecurity for Medical Devices

Email: jan.kuefner@tuvsud.com
Website: www.tuvsud.com/de-mdr
LinkedIn: www.linkedin.com/in/jan-kuefner

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





22% of 597 interviewed hospital IT and IT security staff think, that ransomware attacks have lead to a death of a patient

Ponemon Institute 2020

47 pages on cybersecurity requirements



1
sentence indirectly referring to (cyber)security

4
paragraphs on cybersecurity requirements

MDD

MDR
(into force, since May 2017)

MDCG 2019-16

Today

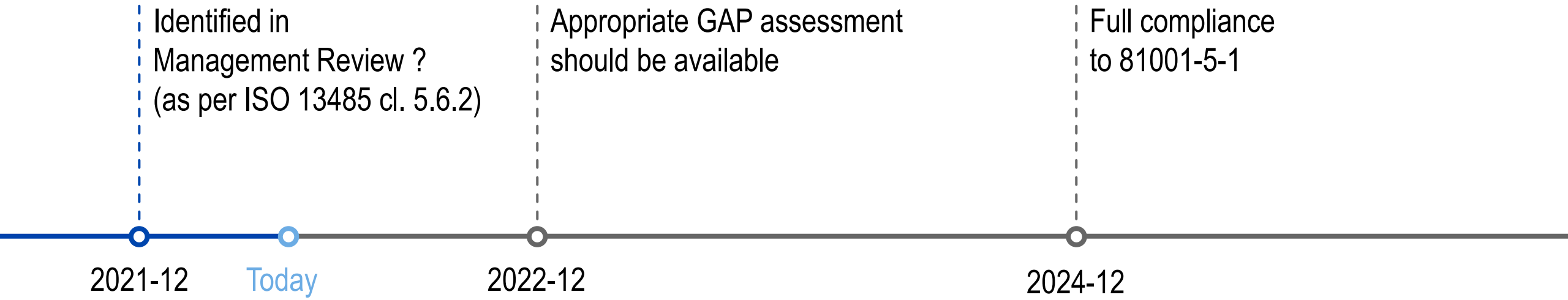
Harmonized standards

IEC 81001-5-1:2021

Published 2021-12

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

ICS › 35 › 35.080



EU cybersecurity standards

Medical device requirements

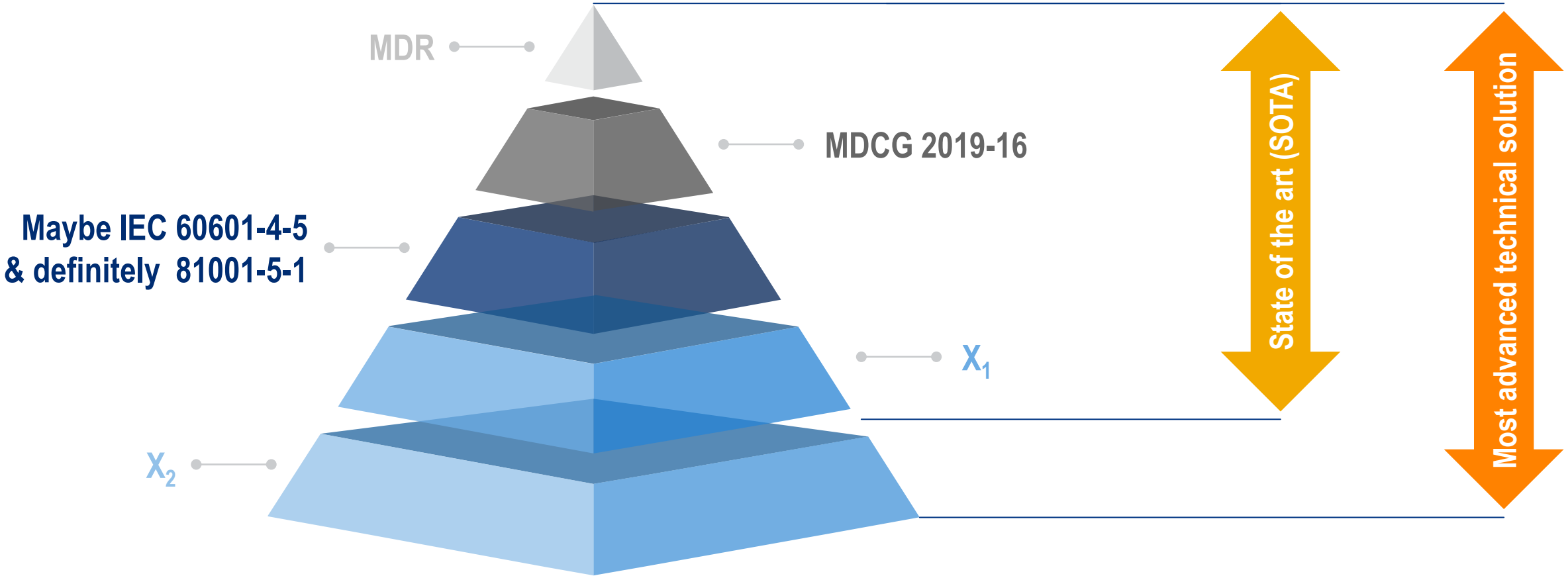
- IEC TR 60601-4-5 (published, trial)

QMS (RnD) requirements

- 81001-5-1 (published)

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




MDR
MDCG 2019-16
Maybe IEC 60601-4-5
& definitely 81001-5-1
X1
X2
State of the art (SOTA)
Most advanced technical solution

EUROPEAN
COMMISSION

Brussels, 14.4.2021
C(2021) 2406 final

COMMISSION IMPLEMENTING DECISION

of 14.4.2021

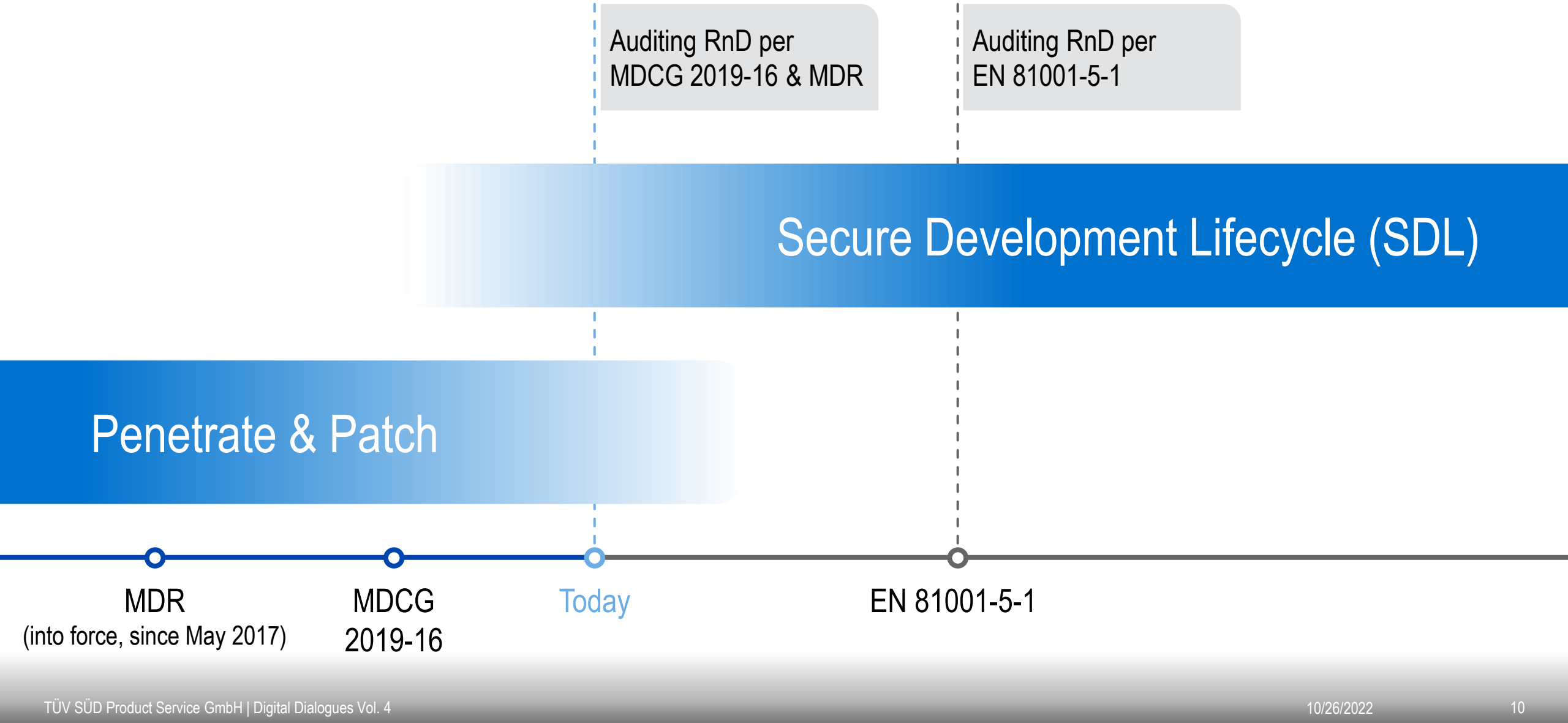
on a standardisation request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards medical devices in support of Regulation (EU) 2017/745 of the European Parliament and of the Council and *in vitro* diagnostic medical devices in support of Regulation (EU) 2017/746 of the European Parliament and of the Council

(Only the English, French and German texts are authentic)

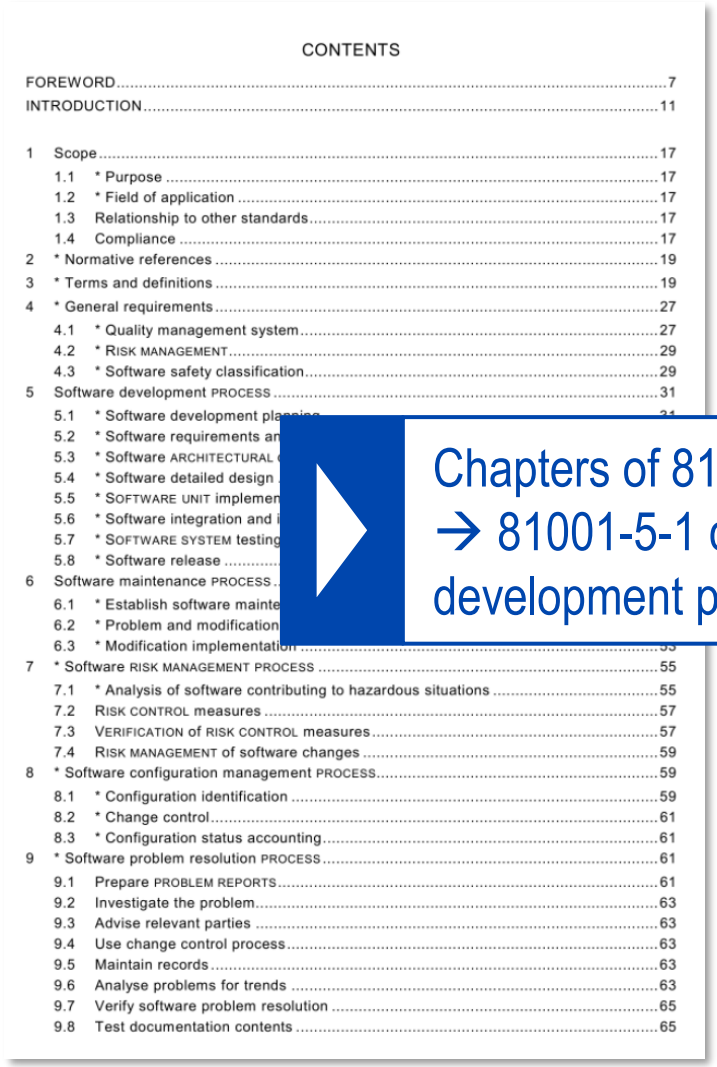
27.	Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle (IEC 81001-5-1)	27 May 2024

Deadline for the adoption

https://health.ec.europa.eu/system/files/2021-04/c_2021_2406_annex_en_0.pdf


Auditing RnD per
MDCG 2019-16 & MDR
Auditing RnD per
EN 81001-5-1
Secure Development Lifecycle (SDL)
Penetrate & Patch
MDR
(into force, since May 2017)
MDCG
2019-16
Today
EN 81001-5-1

IEC 62304:2006/Amd 1:2015



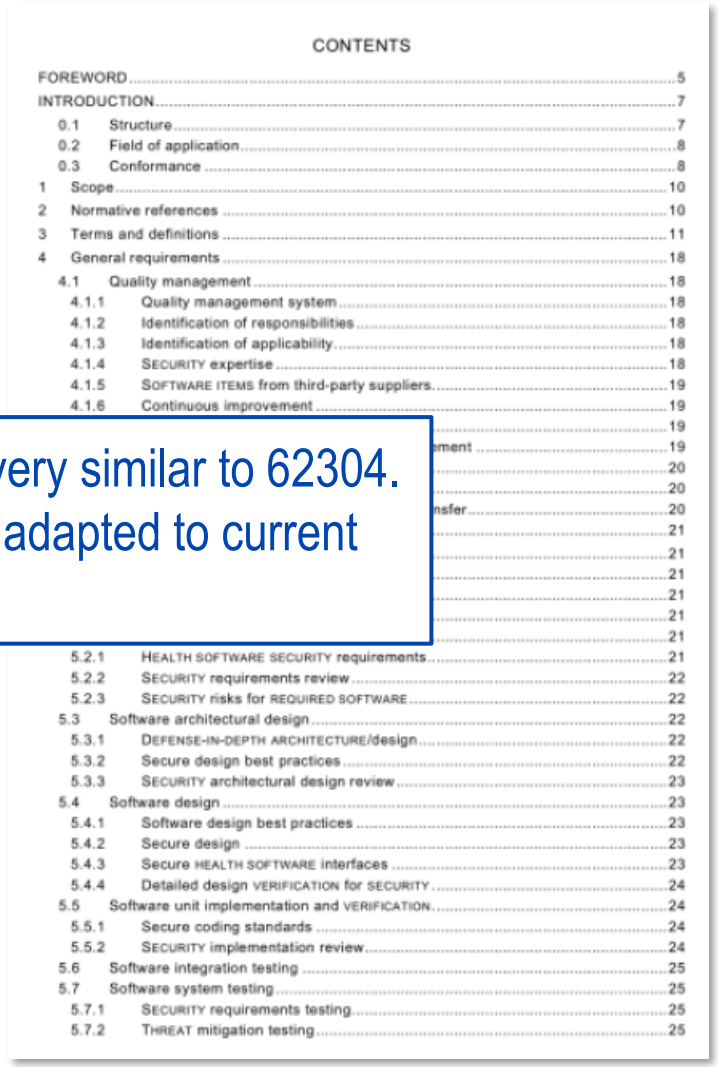
CONTENTS

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 29
4.3 * Software safety classification 29
5 Software development PROCESS 31
5.1 * Software development pla
5.2 * Software requirements an
5.3 * Software ARCHITECTURAL
5.4 * Software detailed design
5.5 * SOFTWARE UNIT implemen
5.6 * Software integration and
5.7 * SOFTWARE SYSTEM testing
5.8 * Software release
6 Software maintenance PROCESS
6.1 * Establish software mainte
6.2 * Problem and modification
6.3 * Modification implementation
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

IEC 81001-5-1:2021



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 Identification of responsibilities 18
4.1.3 Identification of applicability 18
4.1.4 SECURITY expertise 18
4.1.5 SOFTWARE ITEMS from third-party suppliers 19
4.1.6 Continuous improvement 19
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

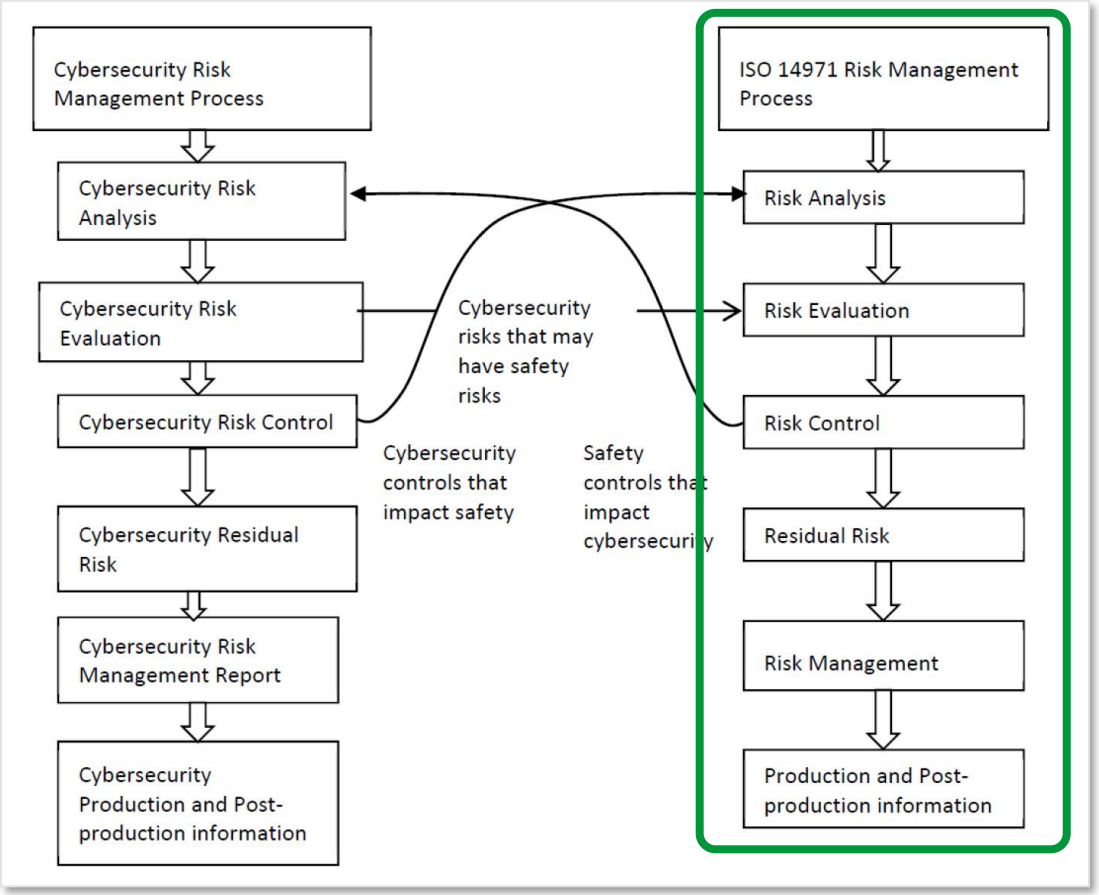
81001-1-5-1

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;

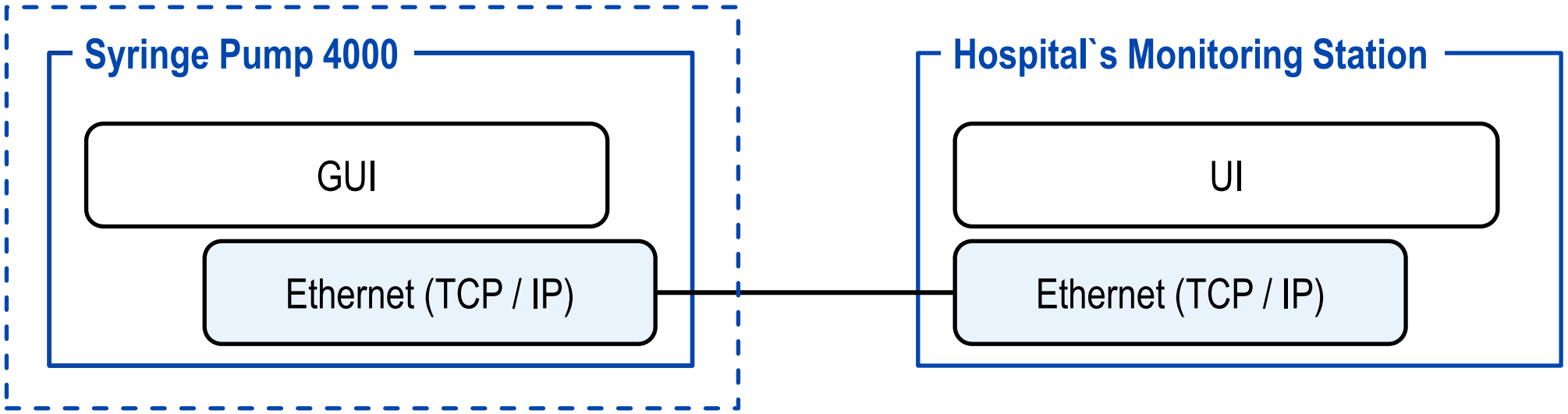
(…)

81001-5-1 cl.7.2

Alternative

Element	Symbol	Discussion
External entity		A sharp-cornered rectangle. Anything outside your control. Examples include people and systems run by other organizations or even divisions. For example, Joe's mobile phone, the Mint data aggregators (assuming you're modeling from a bank's perspective.). If you're modeling Mint, then the bank's systems would be external entities.
Process		A rounded rectangle. Any running code, including compiled, scripts, shell commands, SQL stored procedures, et cetera.
Data store		A drum. Anywhere data is stored, including files, databases, shared memory, S3, cookies, et cetera.
Data flows		An arrow. All the ways that processes can talk to data stores or each other.
Trust boundary	…	A closed shape drawn with a dashed or dotted line. Usually a box.

https://github.com/adamshostack/DFD3


Syringe Pump 4000
GUI
Ethernet (TCP / IP)
Hospital`s Monitoring Station
UI
Ethernet (TCP / IP)

The security risk management process has the same elements as safety risk management process, all documented in a security risk management plan. The process elements are security risk analysis, security risk evaluation, security risk control, evaluation of residual security risk and reporting.

MDCG 2019-16

STRIDE

- Systematic like a pFMEA (allows for spot checking, faster market approval)
- Most used threat model for medical device submissions
- Easy to follow for third persons
- Can easily be integrated to well known FMEA style risk assessment
- Great way to document why something is not done / necessary

Attack vector	STRIDE	Threat	Pre-mitigation			Risk control	Post-mitigation		
			Ability to exploit	Severity	Risk		Ability to exploit	Severity	Risk
Ethernet	Spoofing	…	Hard	Minor	OK	NA			
Ethernet	Tampering	…	Hard	Minor	OK	NA			
Ethernet	Repudiation	NA, since …							
Ethernet	Information Disclosure	NA, since …							
Ethernet	DoS	…	Easy	Critical	NOK	ID122…	Ha		
Ethernet	EoP	NA, since …							

TIPP: Keep all lines in your STRIDE, even those where there is no threat, do 3rd parties can follow your thought process. Add an explanation why there is not threat as necessary

Attack vector	STRIDE	Threat	Pre-mitigation			Risk control	Post-mitigation		
			Ability to exploit	Severity	Risk		Ability to exploit	Severity	Risk
PROFI BUS	Spoofing	…	Hard (since this BUS is within the sealed box)	Minor	OK	NA			
PROFI BUS	Tampering	…		Minor	OK	NA			
PROFI BUS	Repudiation	…		Minor	OK	NA			
PROFI BUS	Information Disclosure	…		Minor	OK	NA			
PROFI BUS	DoS	…		Minor	OK	NA			
PROFI BUS	EoP	…		Minor	OK	NA			

TIPP: In case it isn`t obvious why there is no mitigation, add some explanation!

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

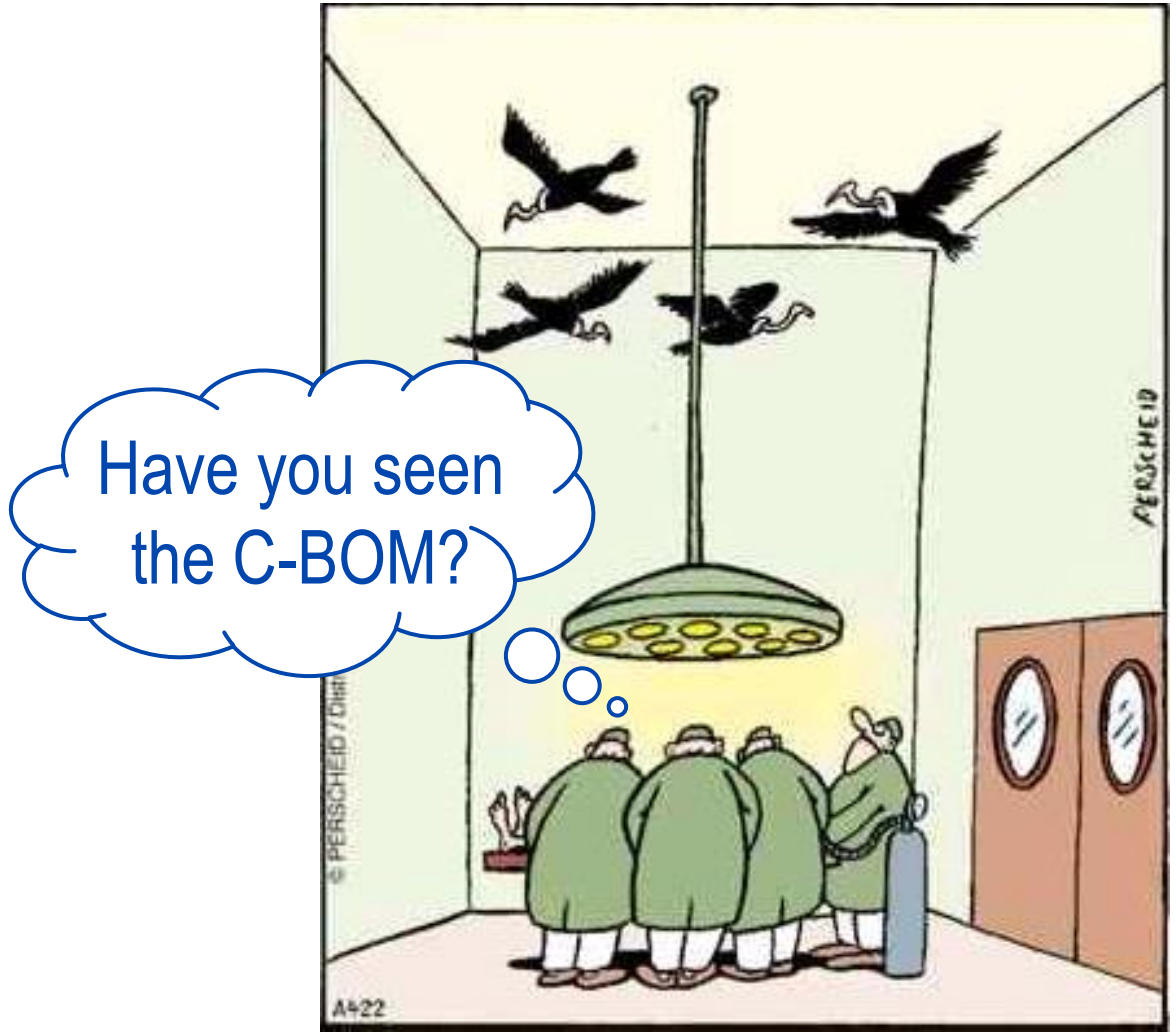
A client: "*Penetration Test cannot be shared with TÜV SÜD, since it is strictly confidential and raw data*"

Not correct,
TÜV SÜD should have a complete TD as per MDR.

Post Market System

Proactive and appropriate vulnerability scanning including timely and appropriate mitigation

Part of MDR audits



Services

Cybersecurity Services provided by TÜV SÜD MHS

- **Training**
- **Concept Evaluation**
- **Vulnerability Scans**
- **Penetration Test**
- **Fuzz Testing**

Client understands the requirements defined in the **regulation / Standards**

Client understands what **Gaps** they have in their technical documentations

Client knows what **known** vulnerabilities are found in their system

Client knows what **un-known** vulnerabilities are found in their system

Client knows understands if the system can handle unexpected input



Abtin Rad
abtin.jamshidirad@tuvsud.com

TÜV SÜD is currently the only test house **accredited** for the security standard IEC TR **60601-4-5**



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

Conclusion

Conclusion

81001-5-1

- Closes gaps in interpretation
- Provides clear requirements for certain elements
- Is a global standard very likely to get harmonized
- Is relevant for RnD, so you might implement it already now
- Is convenient due to its alignment to 62304
- Is well written and precise
- Should be at least considered in management review (ISO 13485 cl. 5.6.1)
- Helps to fulfill MDCG2019-16 requirements
- …



Questions?

Thank you for your attention!

Explore all our **Digital Dialogues** Live Events & Meetings:

Live Events







Register for your individual one2one meeting



Our social media channels: