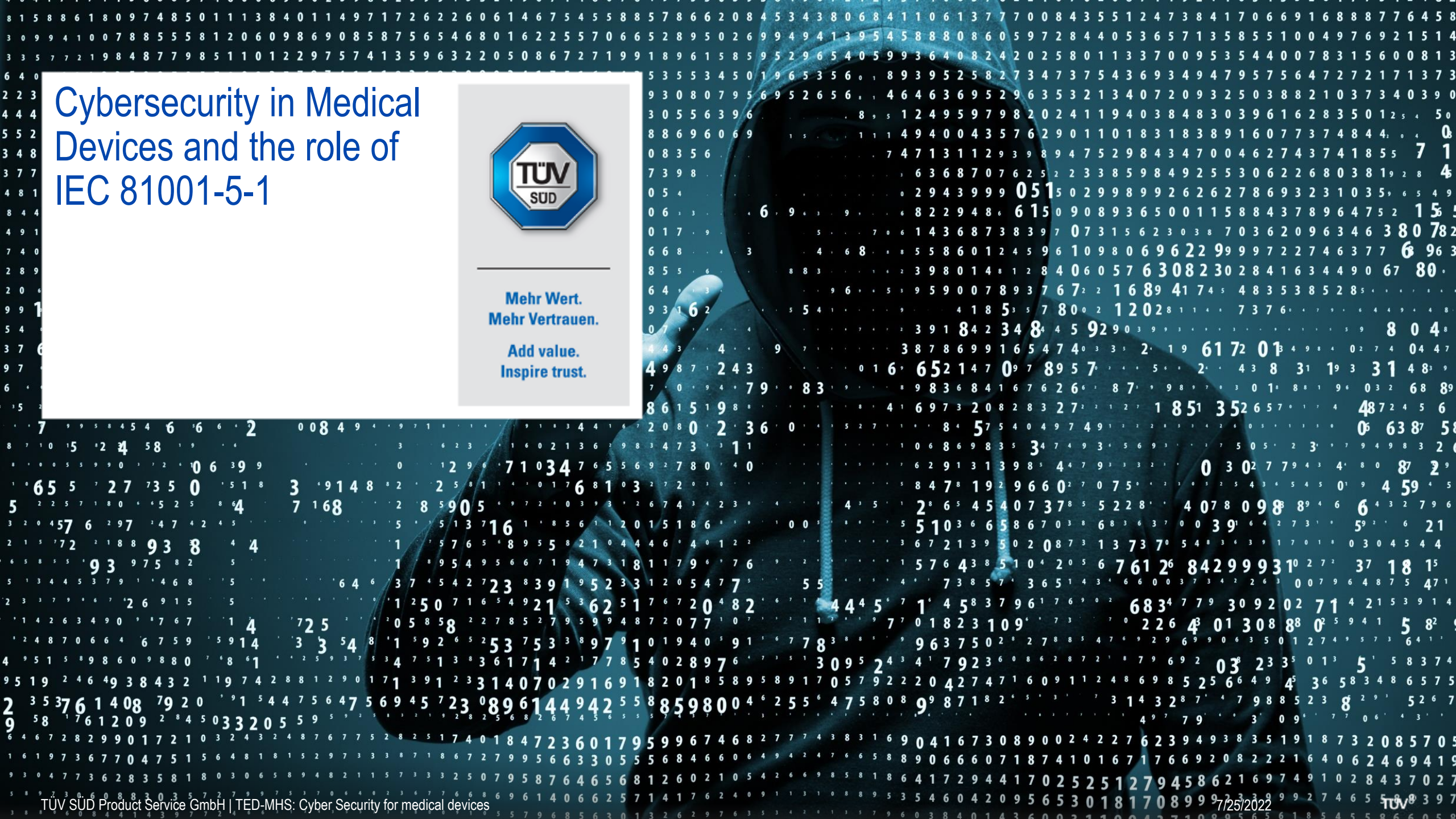
Cybersecurity in Medical Devices and the role of IEC 81001-5-1



Mehr Wert.
Mehr Vertrauen.

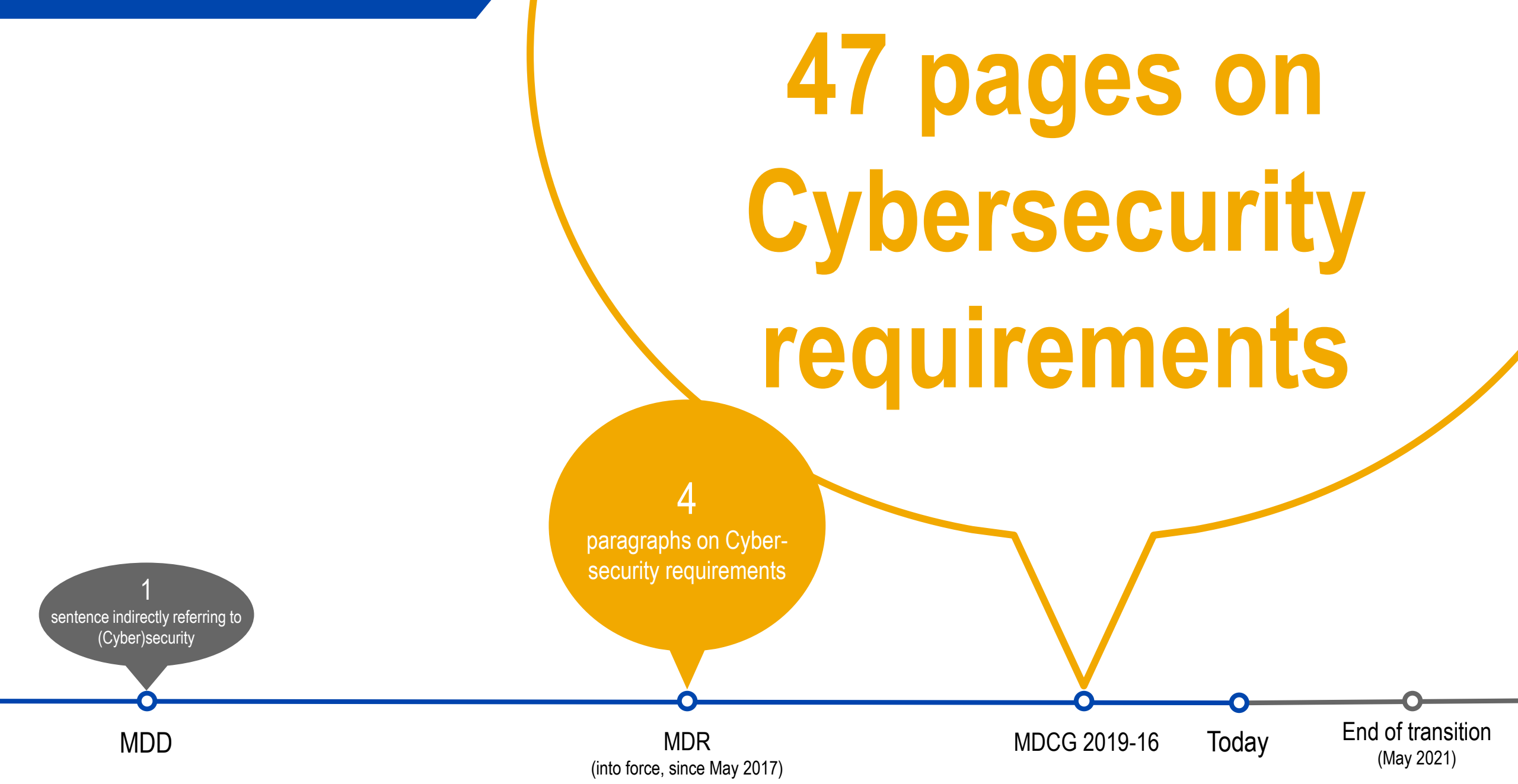
Add value.
Inspire trust.

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
- …

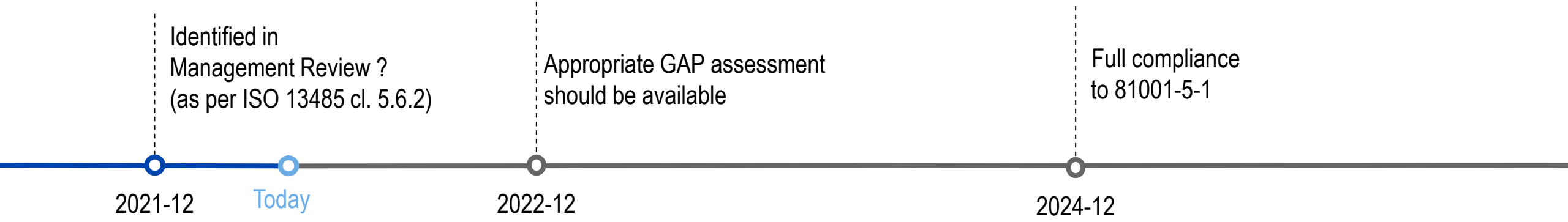
47 pages on Cybersecurity requirements



Published 2021-12

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



EU Cyber Security standards

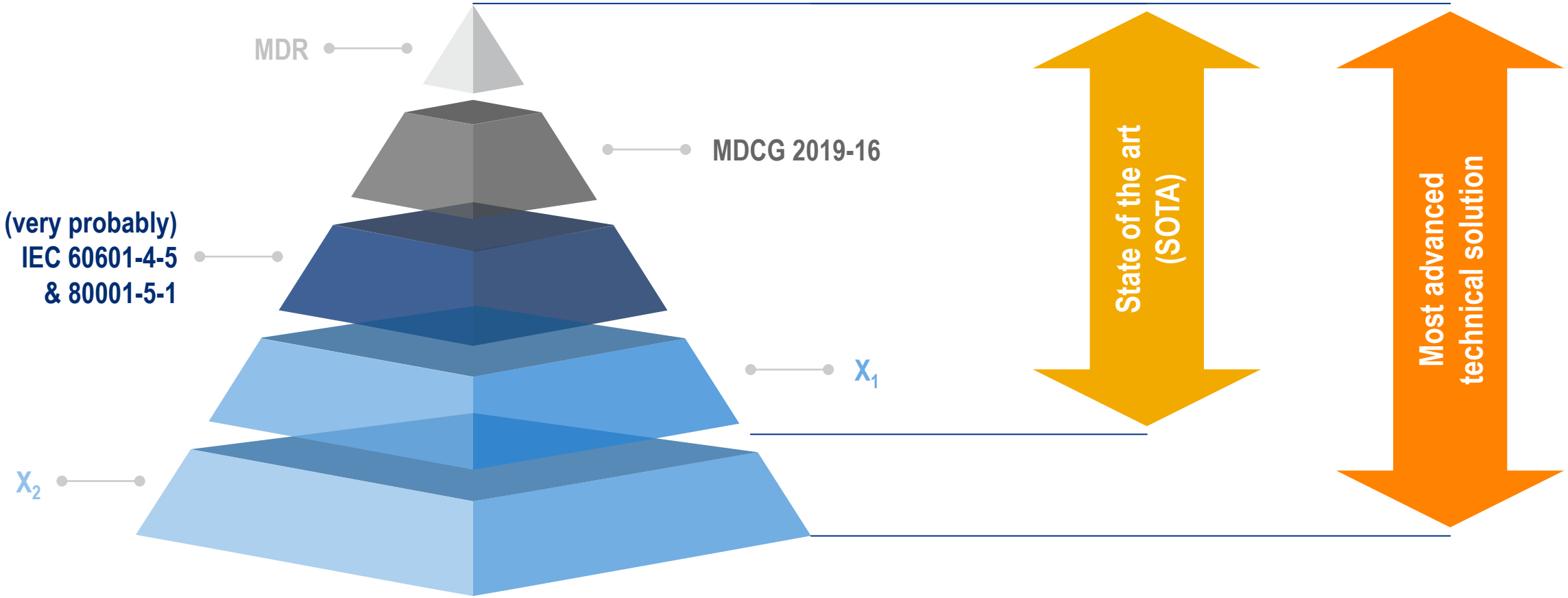
Medical device requirements

- 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


MDR
MDCG 2019-16
(very probably)
IEC 60601-4-5
& 80001-5-1
X1
X2
State of the art
(SOTA)
Most advanced
technical solution

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

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

IEC 81001-5-1:2021

CONTENTS

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

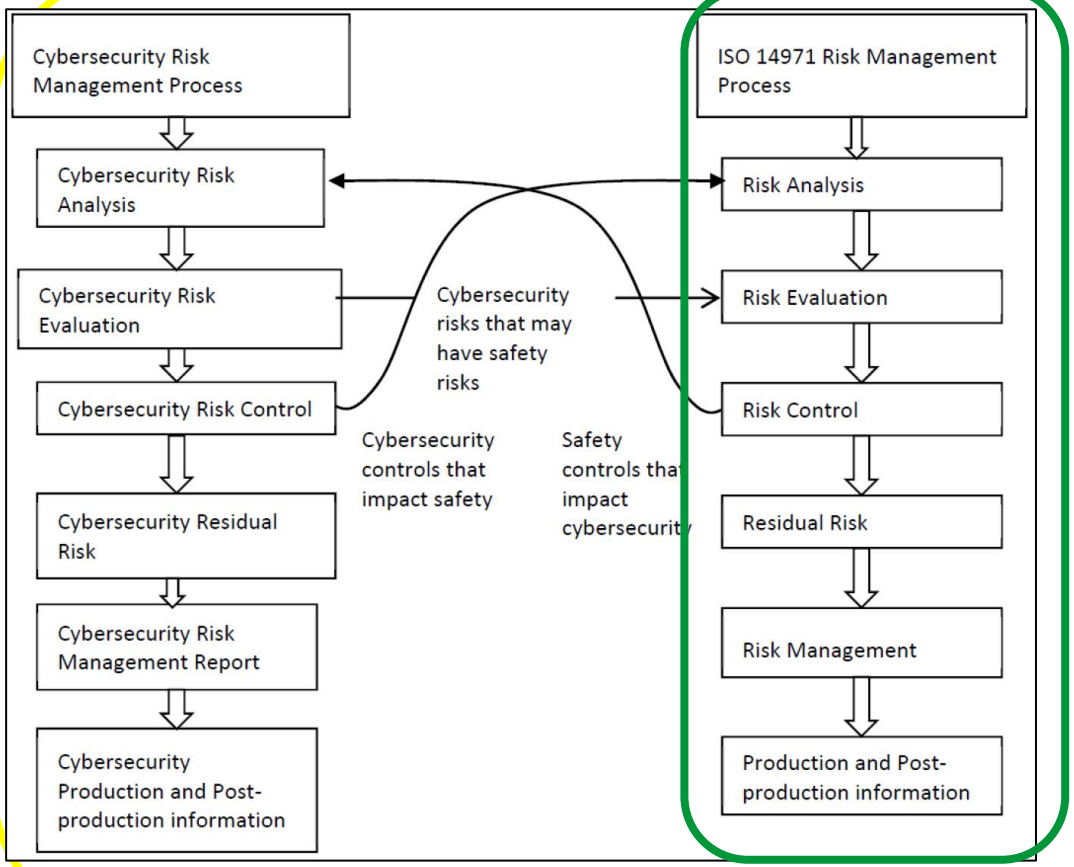
81001-1-5-1

cl 7.2

cl 7.3

cl 7.4

cl 7.5



MDCG 2019-16

No separate security risk process

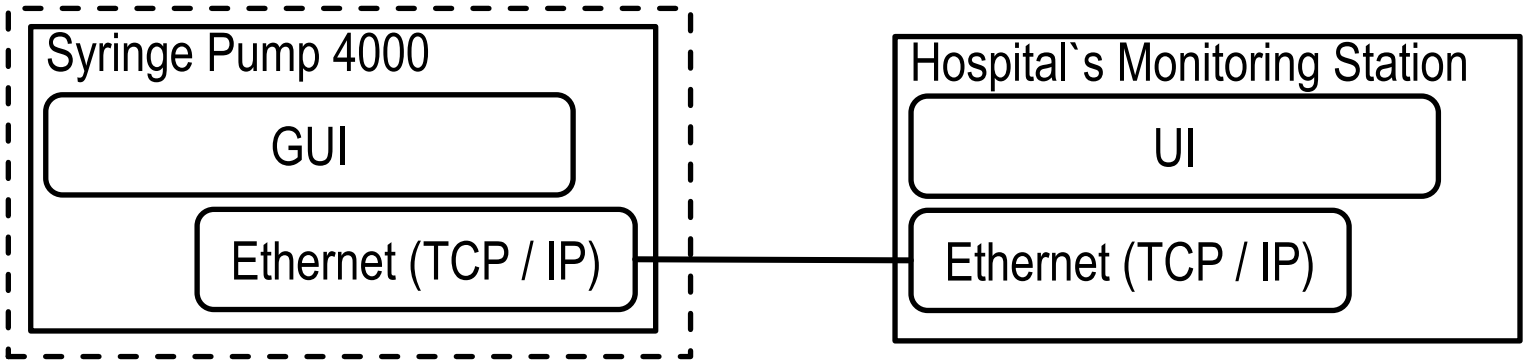
MDCG 2019-16

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


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

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 to 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

Germany & Europe

Trainings, Security Concept Evaluation and Cybersecurity testing capabilities

USA

Trainings (Presential & Online), Security Concept Evaluation

Available (Partners)

Abtin Rad

abtin.jamshidirad@tuvsud.com

Japan

Trainings (Online), Security Concept Evaluation

–

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

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