Cybersecurity Lifecycle Implementation at Maquet Critical Care

Jerker Åberg, Director Regulatory affairs, Maquet Critical Care AB, jerker.aberg@getinge.com

GETINGE

Agenda

1. Regulatory Landscape – Three pillars for Cybersecurity
2. Management System Plan
3. IEC 81001-5-1: Security in the Product Life Cycle
4. FDA Premarket Cybersecurity Guidance (2025)
5. MDCG 2019-16: EU Cybersecurity Guidance
6. Checks along the way
7. Current Status and Way Forward
8. Key Learnings

Regulatory Landscape: Three Pillars of Cybersecurity Compliance

IEC 81001-5-1:2021 (International Standard)

- Defines processes from development through maintenance and decommissioning
- Referenced as state-of-the-art by both EU and FDA
- Annex F provides pathway for Transitional Health Software (legacy devices)

FDA Premarket Cybersecurity Guidance (FEB 2026)

- Quality System Considerations and Content of Premarket Submissions
- Applies to 510(k), PMA, De Novo, and HDE submissions

MDCG 2019-16 Rev.1: EU Guidance on Cybersecurity for Medical Devices

- Implements MDR/IVDR cybersecurity requirements (GSPR)
- Covers full lifecycle: pre-market design through post-market surveillance

Management System Plan

GETINGE

MSP: Activities and Timeline

A. Substantial Change Assessment (Completed 2021-10-31)
- Implementation determined not to be a substantial change

B. QMS Gap Analysis (Completed 2022-07-28)
- Gaps identified and documented

C. QMS Pre-Release (Completed 2023-04-30)
- Initial SOP release for Legal Internal Audit and product gap analysis guidance

D. QMS Update Round 1 (Completed 2023-07-10)
- Required SOPs to enable Transitional Health Software (THS) releases

E. QMS Update Round 2 (Completed 2023-09-01)
- Remaining SOPs for full IEC 81001-5-1 compliance

F. Product THS GAP Analysis (Completed 2024-09-10)
- Servo and Flow analyzed and addressed with rationale for continued use

G. Training (Completed 2023-11-30)
- Self-study + classroom training by cybersecurity program

H. Production Environment Analysis (Ongoing) – Part of NIS2

I. SW Dev Environment Analysis (Ongoing) – Part of NIS2

Management System Plan, MSP = Kvalitetsplan

- Organized way to handle complex changes that spans over many procedures and products.
- Way to ensure and present compliance during the ongoing change.

Health Software and health IT systems, safety effectiveness and security
IEC 81001-5-1:2021 Security - Activities in the Product Life Cycle

GETINGE

IEC 81001-5-1:

QMS Gap Analysis

– Gaps in MCC QMS vs IEC 81001-5-1.

– Analysis of all devices including SaaP in healthcare, medical devices with SiMD (Servo, Flow), and products with SW in healthcare environments (Connectivity X/P-nodes).

QMS Updates

Three rounds of SOP updates completed 2023-2024 covering Threat modelling and risk handling, secure development, vulnerability management, and security testing procedures.

Environment Analysis overlapping with NIS2

Production environment analysis in progress.

SW development environment analysis.

Other support systems

GETINGE

IEC 81001-5-1 Annex F: Transitional Health Software

Gap Analysis Required

We performed a gap analysis of deliverables against clauses pointed out in annex F. Document system-level security requirements.

Security Risk Assessment

Assess and evaluate security risk by documenting the security context and threat model. Control security risk with compensating controls where needed.

Rationale for Continued Use

Document version of transitional SW with rationale for continued use. Establish plan to migrate to full conformance.

Post-Release Activities

Full post-release activities are required even for transitional software.

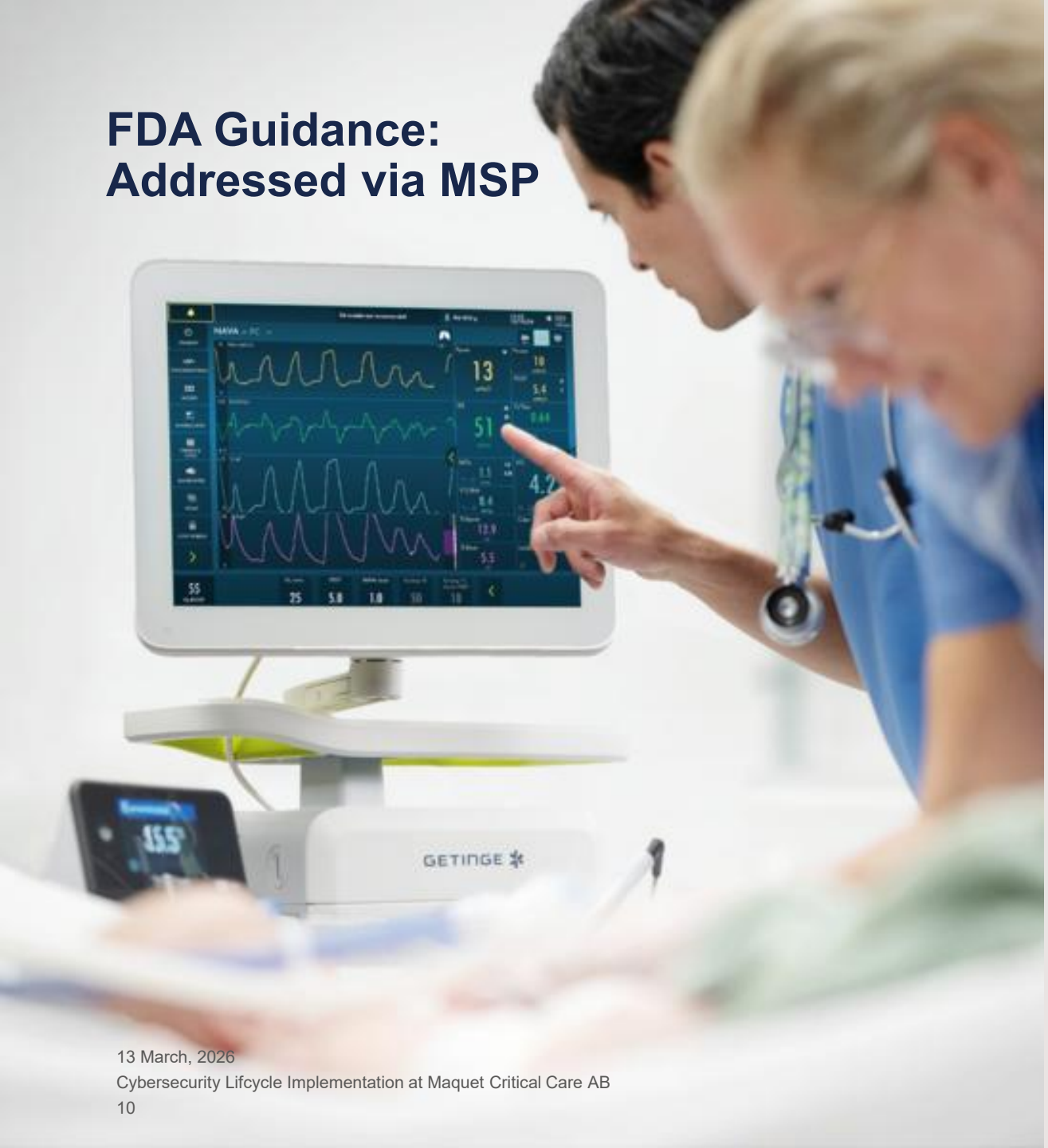
GETINGE

FDA Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submission

FEBRUARY 2026 What is new in the 2026 version: QMSR requirements (ISO 13485)

GETINGE

FDA Guidance: Addressed via MSP



SPDF Implementation (Secure Product Development Framework)

MCC QMS updated to embed secure product development across the lifecycle.

Security Architecture Views added to SW documentation

Global system view, multi-patient harm view, updateability/patchability view, and security use case views. Number of views scales with device complexity

Threat Modeling & Risk Assessment

Complete analysis with threat models for each product. Security Risk Management Report including Threat models, Attack trees, SOUP analysis, FMECA etc

Establish Security Controls (8 Categories)

Authentication, Authorization, Cryptography, Code/Data/Execution Integrity, Confidentiality, Event Detection/Logging, Resiliency/Recovery, Updatability/Patchability.

FDA Guidance: Testing and TPLC Management

Cybersecurity Testing

We have perform static/dynamic analysis, fuzz testing, penetration testing, SCA, and known vulnerability scanning. Testing scales with cybersecurity risk of the device.

TPLC Security Risk Management

Continuous vulnerability monitoring in post-release

Labeling and Transparency

Secure Operating Guidelines, SOG, including:

Customer security documentation, secure configuration guides, known vulnerability disclosure, and patch/update communication plans. SBOM

MDCG 2019-16: Cybersecurity for Medical Devices

GETINGE

MDCG 2019-16

GSPR Compliance

MCC QMS SOPs updated to integrate security risk assessment with safety risk management per ISO 14971. GSPR traceability maintained in technical documentation.

Pre-market Activities

Secure design, threat modeling, and security testing embedded in development process. THS concept implemented to show conformance for all products.

Post-market Processes

PMS procedures updated to include vulnerability monitoring and security update processes. PSUR has now cybersecurity content. We document quarterly CVE scanning reports. Procedure for information and update handling.

IFU and Labeling

Instructions for use updated with cybersecurity sections. Secure Operation Guidelines.

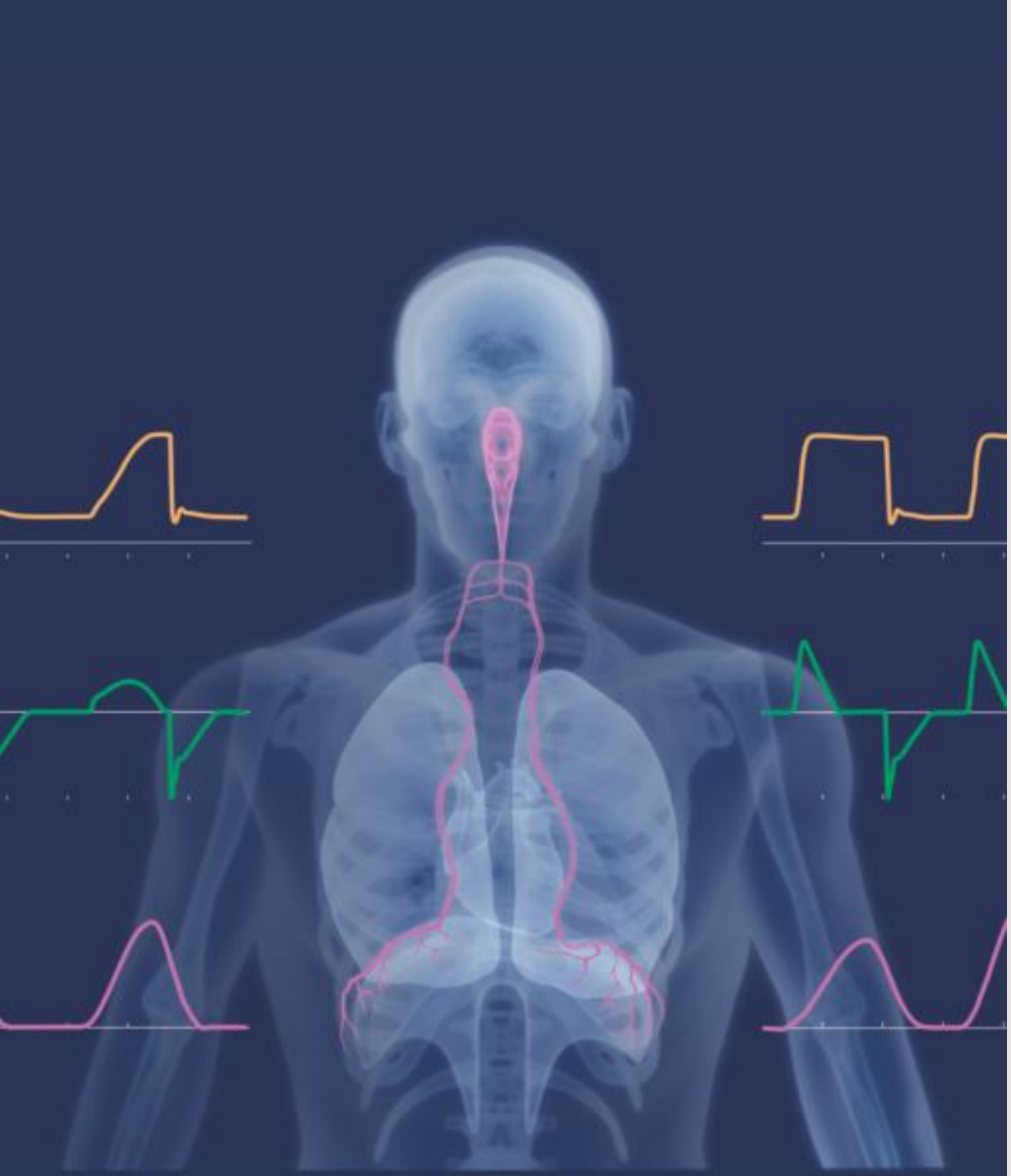
GETINGE

Checks, Future and Key Learnings

IEC 81001-5-1 Review

- Certified testlab to issue an accredited testreport for IEC 81001-5-1.
- Beneficial for 510(k)s as recognized by FDA.
- Good overall benchmark of the status

GETINGE



MedCrypt Second Opinion: Key Findings

Positive Findings

Plans for identified issues considered acceptable. Transitional SW concept is a reasonable approach. Risk-based secure coding accepted. Servo design has sufficient security capabilities. Security views documentation at right level.

Areas for Improvement

Improve motivation for risk management methodology. Analyze all internal interfaces. Individual risk analysis of each CVE with device and system impacts. KPIs on vulnerability timelines.

Patchability Feedback

Describe patching capability: when and how patches will be provided. Plan for mitigation may be acceptable.

GETINGE

Notified Body audits and reviews

Cybersecurity at audit

Has CVE scanning been performed according to plan? Has discovered vulnerabilities been assessed and addressed? Is cybersecurity part of Management review?

Penetration testing of products

Sampling of products during audits for PEN-testing at NB facilities.

Probable future

More detailed questions and findings in TD sampling and when assessing substantial changes where cyber security relevant products.

Current Status and way forward

Patchability Project

Enable customers to perform SW updates via Getinge portal. Requires world-wide coordination with Service organization and IT.

Encrypted Logs Project

Securing device log data through strengthening encryption. Part of the overall security hardening roadmap for MCC products.

Upcoming Submissions

Product documentation lifted during sustaining and new product development projects according to the updated QMS and FDA guidance with security views, SBOM, and testing evidence.

Key Learnings

Start early

For a larger organization with mature QMS and a substantial installed base, these activities takes time.

Identify relevant markets and regulations

Security requirements vary throughout the world:

1. US
2. EU
3. APAC (China)

Chose one standardization path

What standards/guidelines do your products, regulators and customer require.

Use a step-wise approach

Do not try to do everything from the beginning. There is still general acceptance for tangeble plans.

Integrate with current procedures and documents where practicable:

Updated Software descriptions

New Security Risk Management

GETINGE

GETINGE

PASSION FOR LIFE