

MDR und MepV:

Wie bekommt man Cyber-Sicherheit, Zulassung und Datenschutz unter einen Hut?

Information Security in Healthcare
Keynote

14. Juni 2023

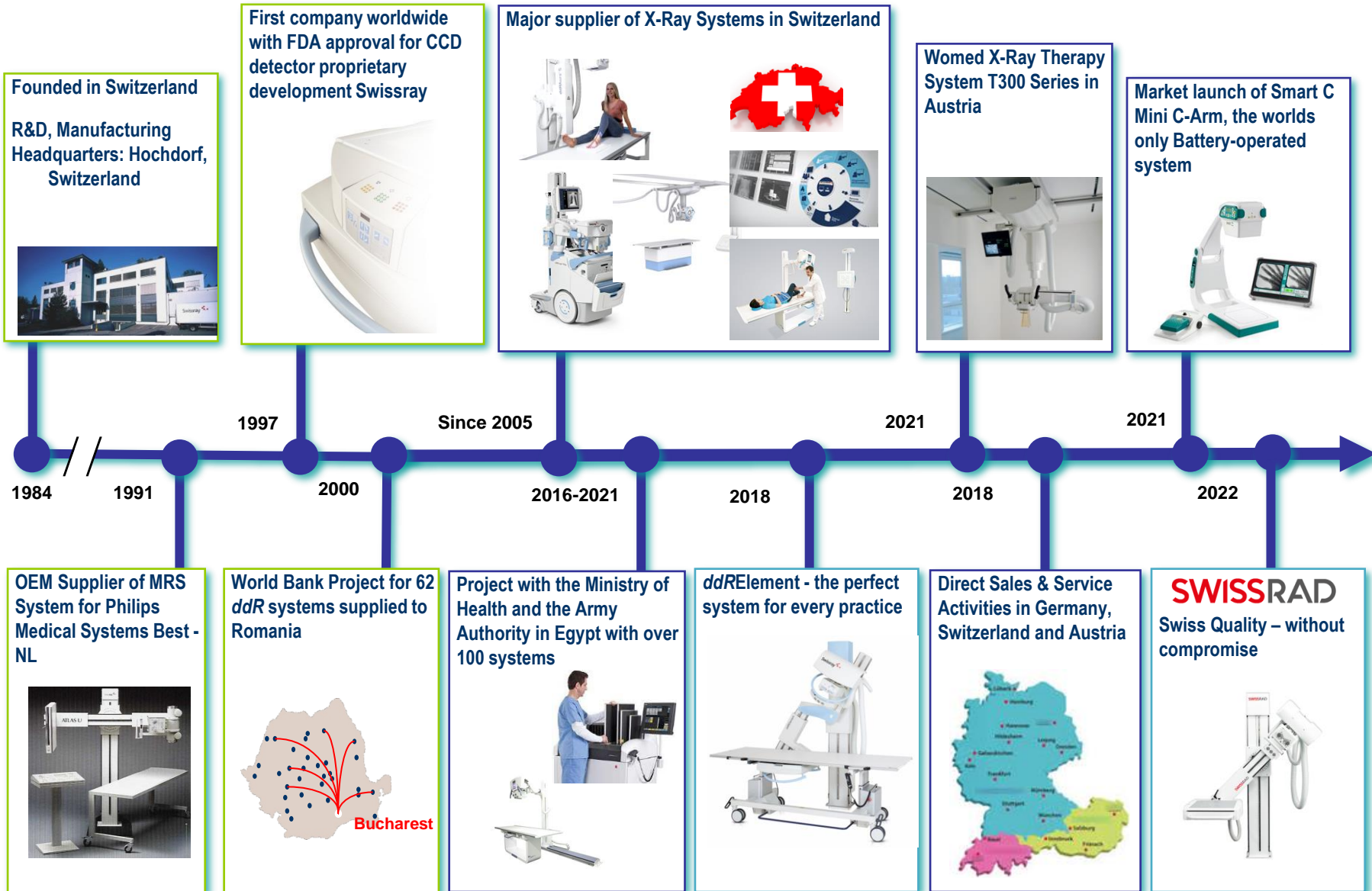
Martin Darms, CTO, Swissray Technologies AG



Inhalt

- Vorstellung Swissray
- MDR / MepV
 - Zulassungsprozess und gesetzliche Grundlagen
 - Was ist zu beachten?
- Import / Vertrieb von amerikanischen medizinischen Produkten (FDA-Approved)
 - Was ist zu beachten?
 - Erfahrungsbericht
- Q & A

History of Innovation and Growth



EU Zulassungsprozess für Medizinprodukte



Gesetzliche Anforderungen

Regulatory Requirements

- [EU MDR Annex I](#)
- [MDCG 2019-16: Guidance on Cybersecurity for Medical Devices](#)
- [IMDRF: Principles and Practices for Medical Device Cybersecurity, 2020](#)
- [Principles and Practices for the Cybersecurity of Legacy Medical Devices, 2023](#)
- [Medizinprodukteverordnung \(MepV\), Art. 74 Cybersicherheit](#)
- EU Datenschutzgrundverordnung DSGVO / CH Neues Datenschutzgesetz revDSG

Security Risk Analysis

- ISO 14971-2019: Risk management to medical devices
- AAMI TIR-57: Principles for Medical Device Security-Risk Management

Security by Design

- IEC 62304: Medical device software: Software lifecycle processes
- IEC TR 60601-4-5 (tailoring of IEC EN 62443-4-2): Product requirements for cybersecurity medical device requirements
- ISO/IEC 80001-5-1 (tailoring of IEC EN 62443-4-1): Process standard for Cybersecurity, Health informatics safety, security and effectiveness

Was bedeutet die MDR/MepV für die Zulassung, den Vertrieb und Betrieb von Medizinprodukten in der Schweiz?

Zwei EU MDR “Take-aways” für Hersteller

1. Das Sicherheitsrisikomanagement muss im Rahmen der MDR durchgeführt werden.

Der Sicherheitsrisikomanagementprozess umfasst dieselben Elemente wie der Sicherheitsrisikomanagementprozess. Ein guter Ansatz besteht darin, die bestehende Risikomanagementmethodik und -anforderungen aus [ISO 14971](#) auf Sicherheitsrisiken auszuweiten. Eine der aussergewöhnlichsten Techniken zur Bewertung von Sicherheitsrisiken, die Bedrohungsmodellierung, ist ein systematischer Ansatz und eine unschätzbare wertvolle Technik zur Durchführung des Sicherheitsrisikomanagements.



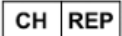


2. Penetrationstests und Schwachstellenscans müssen im Rahmen der MDR durchgeführt werden

Die MDCG-Richtlinien beziehen sich auch auf sicheres Design und Herstellung und das wichtigste Mittel zur Sicherheitsüberprüfung und -validierung ist das Testen. Zu den Methoden können Sicherheitsfunktionstests, Fuzz-Tests, Schwachstellen-Scans und Penetrationstests gehören. Ein Penetrationstest ist ein Muss, idealerweise mit externem Fachwissen und Nachweisen über die Durchführung von Schwachstellenscans.

Was bedeutet die MDR/MepV für die Zulassung, den Vertrieb und Betrieb von Medizinprodukten in der Schweiz?

CH – Bevollmächtigter

Swissmedic hat ein [Merkblatt](#) herausgegeben, welche die Pflichten der Hersteller, CH-REP, Importeure und Händler auflistet.

SWISSmedic		Merkblatt Pflichten Wirtschaftsakteure CH
	Produkt(e) (Art. 1 Abs. 1 MepV) Beinhaltet Medizinprodukte und deren Zubehör, sowie Produkte ohne medizinische Zweckbestimmung ⁵ . Hinweis: der Begriff Medizinprodukt umfasst auch In-vitro-Diagnostika und deren Zubehör ⁶ .	
	Hersteller (Art. 4 Abs. 1 Bst. f MepV, Art. 4 Abs. 1 Bst. e IvDV) Natürliche oder juristische Person, die ein Produkt herstellt oder neu aufbereitet beziehungsweise entwickeln, herstellen oder neu aufbereiten lässt und dieses Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet. Die Pflichten des Herstellers gelten auch für Personen, welche die Tätigkeiten gemäss Art. 16 Abs. 1 MDR bzw. Art. 16 Abs. 1 IVDR vornehmen; Art. 4 Abs. 1 Bst. f MepV / Art. 4 Abs. 1 Bst. e IvDV.	
	Bevollmächtigter ⁷ in CH (Art. 4 Abs. 1 Bst. g MepV, Art. 4 Abs. 1 Bst. f IvDV) Natürliche oder juristische Person in der Schweiz, die von einem im Ausland ansässigen Hersteller schriftlich beauftragt (Mandat) wird, in seinem Namen bestimmte Aufgaben gemäss MepV / IvDV wahrzunehmen. Hat der Hersteller eines Produktes seinen Sitz nicht in der Schweiz, so dürfen seine Produkte nur in Verkehr gebracht werden, nachdem ein Bevollmächtigter mit Sitz in der Schweiz mandatiert wurde ⁸ . Dies gilt auch für Hersteller mit Sitz in der EU/EWR. Die Benennung des Bevollmächtigten gilt mindestens für alle Produkte einer generischen Produktgruppe ⁹ .	
	Importeur (Art. 4 Abs. 1 Bst. h Mep, Art. 4 Abs. 1 Bst. g IvDV) Ein Importeur wird nicht «benannt» , sondern die Rolle ergibt sich aus der Tätigkeit, welche ausgeübt wird, wenn eine natürliche oder juristische Person in der Schweiz ein Produkt aus dem Ausland auf dem Schweizer Markt in Verkehr bringt.	
	Händler (Art. 4 Abs. 1 Bst. i MepV, Art. 4 Abs. 1 Bst. h IvDV) Wirtschaftsakteur in der Lieferkette, der ein Produkt bis zum Zeitpunkt der Inbetriebnahme auf dem Schweizer Markt bereitstellt, mit Ausnahme des Herstellers oder des Importeurs.	

CIA-Aspekte

Ziele der IT-Sicherheit

- **Confidentiality** Vertraulichkeit von z. B. personenbezogenen Daten
- **Integrity** Die Unverfälschtheit von Daten und Systemen
- **Availability** Die Verfügbarkeit von Daten und Systemen

MDR	Artikel 109 & 110	Vertraulichkeit und Datenschutz
MepV	Artikel 74	Cybersicherheit

[Manufacturer Disclosure Statement for Medical Device Security \(MDS2\)](#)

[Sicherheit von Medizinprodukten - Leitfaden zur Nutzung des MDS2 aus 2019](#)

Sicherheitsupdates bei med. Geräten

Dispelling the Myths	Understanding the Facts
<p>The FDA is the only federal government agency responsible for the cybersecurity of medical devices.</p> <p>Cybersecurity for medical devices is optional.</p> <p>Medical device manufacturers can't update medical devices for cybersecurity.</p> <p>Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.</p>	<p>The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.</p> <p>Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.</p> <p>Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.</p> <p>The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.</p>

The FDA's role in medical device cybersecurity, FDA fact sheet, Dispelling myths and understanding facts.
<https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf>. Zugriffen am 08.06.2023

Erfahrungsbericht

- Einzigartiges batteriebetriebenes System, welches FDA zugelassen ist
- Was hat es gebraucht, um diese med. Geräte in die Schweiz einzuführen?
 - CE-Zulassung

Surgical Mini C-Arm - Smart C

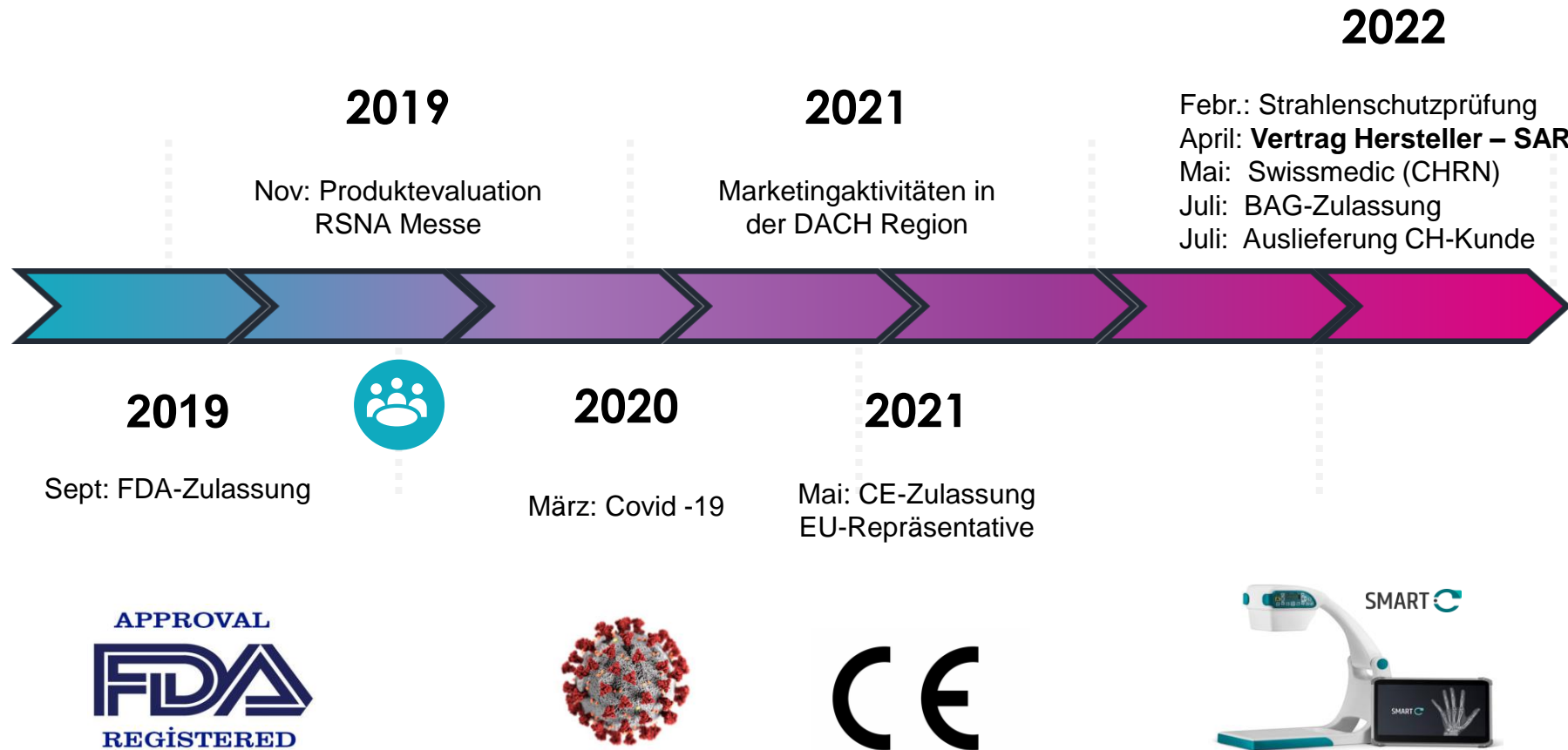
Unique mini C-arm Flexible and easily portable

The Smart C is the world's only battery-powered Mini C-Arm for use in the consulting room or operating room (OR) for foot and hand surgery. It delivers exceptional real-time image quality with minimal X-ray dose. The compact design allows the Smart C to be used in a variety of locations. The live X-ray images or the LIH are viewable on the tablet and can be stored in the PACS via the DICOM 3.0 interface. The Smart C works reliably and particularly quietly because no fans are installed.



Zeitliche Abfolge zum SAR

Swiss Authorized Representative (SAR, CH-REP)



Politik & Presse

CHRONOLOGIE

21.09.2020

STÄNDERAT

Zuweisung an die zuständige Kommission zur Vorberatung

30.05.2022

STÄNDERAT

Annahme

28.11.2022

NATIONALRAT

Annahme

Motion 20.3211 ([Müller Damian](#))

**Für mehr Handlungsspielraum bei der
Beschaffung von Medizinprodukten zur
Versorgung der Schweizer Bevölkerung**

Motion 20.3370 ([Rösti Albert](#))

**Zulassung von Medizinprodukten nach
aussereuropäischen Regulierungssystemen**

NACHRICHTEN

Schweiz: Künftig gilt auch FDA-Zulassung von Medizinprodukten

Künftig gilt FDA-Zulassung:

<https://medtech-zwo.de/aktuelles/nachrichten/nachrichten/schweiz-kuenftig-gilt-auch-fda-zulassung-von-medizinprodukten.html>

MEDIZINPRODUKTEVERORDNUNG

MDR-Probleme | Schweiz öffnet sich für FDA-System | BVMed: „Lösungen liegen auf dem Tisch – jetzt muss entschieden werden!“



© AdobeStock @artjazz

30.11.2022 | 93/22 | Berlin | **Der Bundesverband Medizintechnologie (BVMed) drängt im Vorfeld der EPSCO-Sitzung der EU-Gesundheitsminister:innen am 9. Dezember 2022 auf konkrete Verbesserungen der EU-Medizinprodukte-Verordnung (MDR). Hintergrund ist, dass aufgrund von**

Engpässen bei den Zertifizierungsstellen und dem erheblich gestiegenen bürokratischen Aufwand von 25.000 bis Mai 2024 benötigten Medizinprodukte-Zertifikaten bislang erst 2.000 MDR-Zertifikate ausgestellt sind. „Europa droht durch die MDR als Forschungs- und Produktionsstandort weit hinter die USA zurückzufallen, wenn jetzt nicht gehandelt wird“, befürchtet BVMed-Geschäftsführer und Vorstandsmitglied Dr. Marc-Pierre Möll. Jüngstes Warnzeichen: Das Schweizer Parlament hat am 28. November 2022 beschlossen, künftig auch die FDA-Zulassung von Medizinprodukten anzuerkennen.

Swiss MedTech unterstützt die Motion

<https://www.swiss-medtech.ch/news/motion-203211>

«Das wird sicher 2025, wenn nicht 2026 bis es im Gesetz verankert ist», Damian Müller.

[Quelle](#)

Was hat der amerikanische Hersteller nicht berücksichtigt?

- Die Umlaute ä, ö und ü fehlten in der ersten SW-Version
- In Deutschland sind einige Abnahme-Tests strenger als in der Schweiz
- Die DIN Norm 6862-2:2019 gibt es nur in Deutsch (!)
Bestimmte DICOM Tags werden für neue Systeme ab 2021 verlangt
- Benutzerhandbuch in den jeweiligen Landessprachen der EU

Lessions Learned – Take aways

- Wie reagiert der Hersteller auf Fragen zur Cyber Security
- Alle Aspekte der „CIA“ sind wichtig
- Die FDA erlaubt explizit, security updates, sofern der es nicht den „Intended Use“ verändert
- FDA zugelassene Systeme können (in naher Zukunft 2025?) auch ohne CE-Zulassung in der Schweiz eingeführt werden
 - Importeur / CH Repräsentativ

Swissray

Kontakt: +41 41 914 12 12

info@swissray-technologies.com

martin.darms@swissray-technologies.com

www.swissray-technologies.com

Darms Engineering

IT- Sicherheit im Gesundheitswesen

- Vulnerability Management
- Beratung und Implementierung von SaaS-Lösungen im Bereich Cybersicherheit in Spitälern
- Pentesting med. Geräten und Systemen (Black- und Whitebox-Tests)



**Ihr Partner
in der Radiologie**

für Systeme, Dienstleistungen
und IT Schutzsoftware

 **+41 41 914 12 30**

SWISSRAY 
TECHNOLOGIES

Swissray Technologies AG, Tatlenstrasse 25 - 6200 Hochdorf - Schweiz
info@swissray-technologies.com - www.swissray-technologies.com

DARMS ENGINEERING

info@darms.ch



Thank you for your time.