CASE STUDY

Stressfrei durch die Radio Equipment Directive

So meistern Sie Schritt für Schritt die neuen Cybersecurity-Anforderungen

Inhalt

Drahtlose Technologien sind aus unserem Alltag nicht mehr wegzudenken.

Bildquelle: KI-generiert mit Unterstützung von ChatGPT

Vom Smartphone bis zum IoT-Sensor – sobald ein Gerät per Funk mit anderen Systemen kommuniziert, greift in Europa die Radio Equipment Directive (RED). Diese EU-Richtlinie (2014/53/EU) legt fest, welche Anforderungen Funkanlagen erfüllen müssen, bevor sie in den Verkehr gebracht werden dürfen.

Ab August 2025 werden die Cybersecurity-Anforderungen der RED mit der Normenreihe EN 18031 konkretisiert und verpflichtend. Für Hersteller bedeutet das: Wer weiterhin CE-konforme Funkprodukte anbieten will, muss nicht nur Technik, sondern auch neue Prozesse und die entsprechende Dokumentation im Griff haben.

In dieser Case Study zeigen wir, wie die EN 18031 in der Praxis angewendet wird und wie wir Sie Schritt für Schritt bei der Einhaltung der neuen Cybersecurity-Anforderungen unterstützen.

Dafür betrachten wir ein fiktives, aber praxisnahes Embedded-System – den „RoDAkku" (= Roller Daten Akkulumierer). Dieses Modul wird in E-Rollern verbaut und sammelt dessen Betriebsdaten über den CAN-Bus. Zusätzlich erfasst er Standortdaten (GPS), die jedoch nicht verarbeitet werden. Diese Informationen werden stündlich per LTE-M/NB-IoT in die Cloud übertragen.

Radio Equipment Directive

Die EU-Richtlinie 2014/53/EU regelt die Anforderungen an Funkanlagen und drahtlose Geräte, die auf den Markt der Europäischen Union gebracht werden. Ihr Ziel ist es, Sicherheit, Effizienz und die harmonisierte Nutzung des Funkspektrums sicherzustellen. Neben der klassischen Produktsicherheit umfasst die RED auch elektromagnetische Verträglichkeit, effiziente Frequenznutzung und – zunehmend wichtig – Cybersecurity.

Ihre Abkürzung durch die RED

TQ unterstützt Sie bei allen notwendigen Schritten. Kontaktieren Sie uns jetzt und profitieren Sie von der Erfahrung unserer Cybersecurity-Experten.

Jetzt Kontakt aufnehmen

Welche Produkte sind betroffen?

Wichtig hierbei ist folgende Unterscheidung: **RED ist nicht gleich EN 18031**. Die RED gilt grundsätzlich für alle Produkte mit Funkschnittstelle, unabhängig davon, ob die neuen, konkretisierten Cybersecurity-Anforderungen der EN 18031 zur Anwendung kommen.

Das bedeutet: **Ihr Produkt könnte durchaus unter die RED fallen, ohne dass die zusätzlichen Vorgaben aus der Norm erfüllt werden müssen.** Um dies zu prüfen, lohnt sich zunächst ein Überblick über die Richtlinie 2014/53, die insbesondere in Artikel 3 (d-f) grundlegende Anforderungen an Cybersecurity enthält.

- Schutz des Netzes
- Schutz personenbezogener Daten
- Schutz vor Betrug

2022 wurde die Richtlinie mit der Delegierten Verordnung (EU) 2022/30 präzisiert. Diese führt unter anderem aus:

- **Artikel 3(d):** gilt bei direkter oder indirekter Kommunikation mit dem Internet
- **Artikel 3(e):** betrifft personenbezogene Daten oder konkret Kinderspielzeug und Wearables
- **Artikel 3(f):** betrifft Systeme mit Geldverarbeitung

Die konkreten Anforderungen wurden im August 2024 mit den Normen EN 18031-1 (zu 3d), EN 18031-2 (zu 3e) und EN 18031-3 (zu 3f) veröffentlicht.

Ist der RoDAkku von den neuen Cybersecurity-Bestimmungen betroffen?

Da er per Funk Daten sendet, fällt er klar unter die RED. Nun ist zu prüfen, ob Artikel 3 d-f ebenfalls greifen und das System damit eine oder alle der Normen EN 18031 erfüllen muss.

RED 3d: Kommuniziert der RoDAkku über das Internet?
✓ **Trifft zu:** EN 18031-1 relevant

RED 3e: Verarbeitet der RoDAkku personenbezogene Daten oder fällt er in die Kategorie Kinderspielzeug oder Wearables?
✗ **Trifft nicht zu:** EN 18031-2 nicht relevant

RED 3f: Trägt der RoDAkku zu einem Geldfluss bei
✗ **Trifft nicht zu:** EN 18031-3 nicht relevant

Das Produkt ist betroffen. Was nun?

Die Normenreihe EN 18031 umfasst zahlreiche Anforderungen, die sich wiederum in verschiedene Unterkategorien gliedern – angefangen bei Access Control Mechanisms (ACM) über Themen wie Update- und Storage-Mechanismen bis hin zu Cryptography (CRY).
Bevor wir jedoch in die Bewertung der einzelnen Kategorien für unser Beispielprodukt einsteigen, empfiehlt sich an dieser Stelle eine methodische Vorbereitung.

Grundsätzlich gilt:
In der Praxis sollte die Einschätzung durch Fachleute überprüft werden. Wenden Sie sich hierfür gerne direkt an unsere TQ-Experten.

Ist Ihr Produkt betroffen?

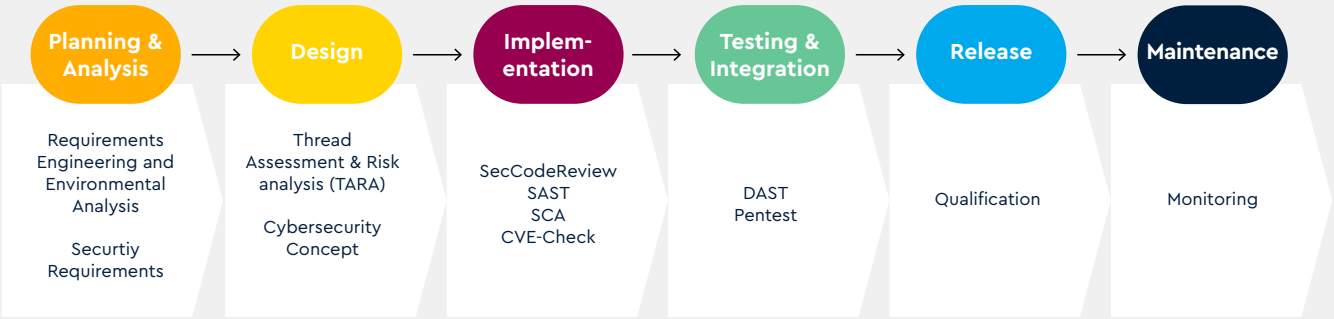
Finden wir es gemeinsam heraus! Unsere Cybersecurity-Experten prüfen Ihr Produkt und geben Ihnen konkrete Handlungsempfehlungen.

Jetzt Kontakt aufnehmen

Secure Software Development Life Cycle

Ein zentrales Element ist der Secure Software Development Life Cycle (SSDLC), wie er unter anderem von OWASP beschrieben wird. Der SSDLC stellt sicher, dass Cybersecurity nicht erst am Ende des Entwicklungsprozesses berücksichtigt wird, sondern von Anfang an in alle Phasen integriert ist – von der Planung über das Design und die Implementierung bis hin zum Test und zur Wartung.

Das Selbstassessment nach der EN 18031 ist formal gesehen erst spät im Lebenszyklus angesiedelt, da es Teil der finalen Qualifikation des Produkts ist (s. Grafik). Um jedoch zu vermeiden, dass Sicherheitslücken oder unzureichende Maßnahmen erst in dieser späten Phase auffallen, empfiehlt es sich, frühzeitig Cybersecurity miteinzubeziehen und dafür mit einer Threat Assessment and Risk Analysis (TARA) zu starten.



Thread Assessment and Risk Analysis (TARA)

Der Begriff stammt aus der Automotive-Welt, findet sich aber auch in der EN 18031-1 (Anhang A.2.3) wieder: Hier ist von Bedrohungsmodellierung und Sicherheitsbeurteilung die Rede. Dieser Schritt ist zwar unter der RED nicht verpflichtend, erleichtert jedoch das Verständnis potenzieller Angriffsflächen und stärkt die Verteidigungsmaßnahmen – ein zentraler Punkt im kommenden Cyber Resilience Act (CRA).

Der Cyber Resilience Act (CRA) wird ebenfalls in naher Zukunft verpflichtend und erweitert die Anforderungen an Cybersecurity für zahlreiche Produkte erheblich.

TQ unterstützt Sie schon jetzt dabei, Ihre Prozesse und Produkte fit für den CRA zu machen – mit praxisnaher Beratung, Workshops und gezielten Analysen. Sprechen Sie uns an!

In der Praxis bewährt sich eine Kombination aus OWASP Threat Modeling und MITRE EMB3D Threat Model mit folgenden Kernelementen:

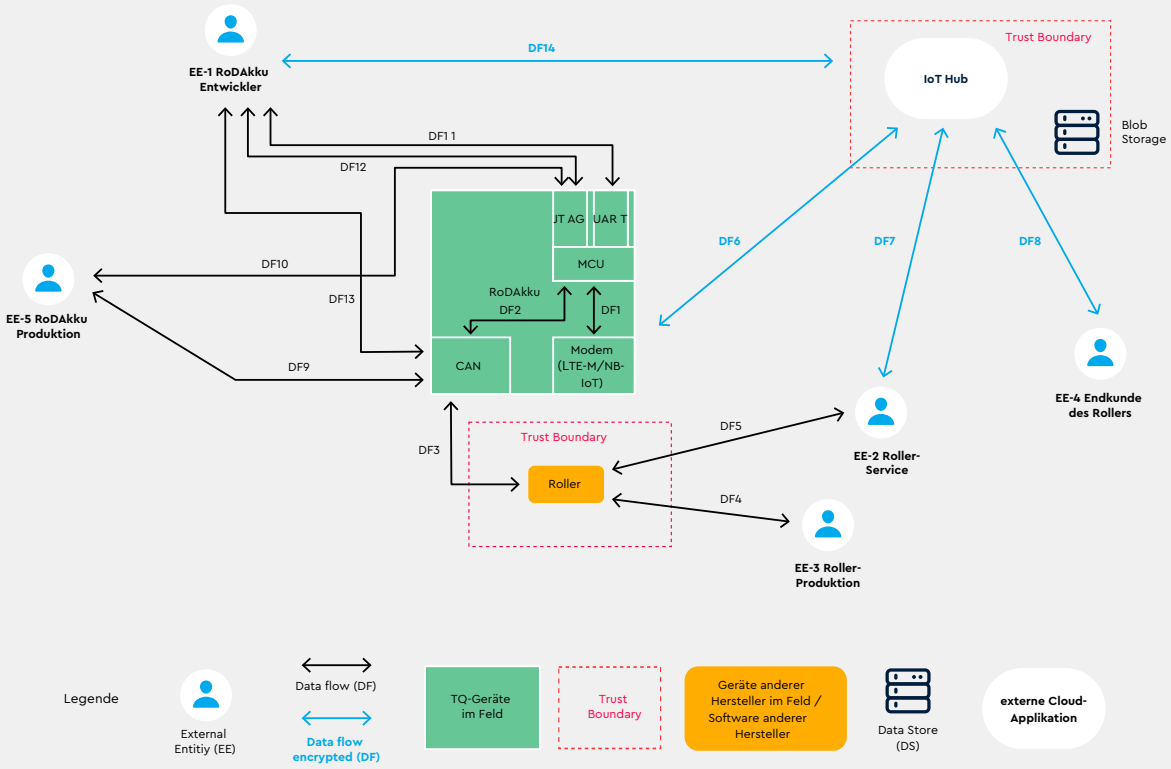
1. Systemübersicht (Komponenten, Datenflüsse)
2. Abhängigkeiten, Schnittstellen
3. Assets (schützenswerte Werte)
4. Use/Abuse Cases
5. Bedrohungen identifizieren & bewerten
6. Maßnahmen ableiten

Im Rahmen dieser Case Study betrachten wir vor allem die Punkte 1. (Systemübersicht) und 5. (Bedrohungsanalyse), sowie grundlegend dafür 3. (Assets).

Systemübersicht

Ein zentraler Bestandteil der TARA ist die Systemübersicht. Sie bietet eine klare Darstellung der wichtigsten Komponenten, Datenflüsse Schnittstellen und Interaktionen innerhalb des Produkts.

Für den RoDAkku bedeutet das: Wir zeigen, wie das Modul intern aufgebaut ist, welche internen und externen Kommunikationswege bestehen (z. B. CAN-Bus, LTE-M, Cloud-Anbindung) und welche externen Entitäten (z. B. Cloud-Dienste, Service-Systeme) eingebunden sind. Diese Übersicht bildet die Grundlage, um potenzielle Abhängigkeiten, Risiken und Angriffspunkte zu identifizieren – und ermöglicht es, gezielt Schutzmaßnahmen zu planen.



Bedrohungsanalyse mit MITRE EMB3D (Auszug)

Um die potenziellen Risiken für unseren RoDAkku zu bewerten, nutzen wir das MITRE EMB3D-Framework. Dieses Framework bietet eine systematische Übersicht über bekannte Angriffsvektoren und Schwachstellen in Embedded-Systemen, unterteilt in die drei Bereiche Hardware, System Software und Application Software. Diese Kategorien helfen uns, Schwachstellen frühzeitig zu identifizieren, typische Angriffsvektoren zu verstehen und geeignete „Mitigation"-Maßnahmen zu planen.

So schaffen wir die Grundlage, um im weiteren Verlauf die Anforderungen der EN 18031 gezielt umzusetzen.
Die Bedrohungsanalyse mit MITRE EMB3D liefert uns für unser Beispielprodukt folgendes Ergebnis. Bei der Tabelle handelt es sich um einen Auszug an Bedrohungsszenarien, die sich für den RoDAkku ergeben und gesondert betrachtet werden sollten.

Potentielle Bedrohungen

Hardware

TID-101 - Power Consumption Analysis Side Channel
TID-102 - Electromagnetic Analysis Side Channel
TID-103 - Microarchitectural Side Channels
TID-105 - Hardware Fault Injection – Control Flow Modification
TID-106 - Data Bus Interception
TID-107 - Unauthorized Direct Memory Access (DMA)
TID-108 - ROM/NVRAM Data Extraction or Modification
TID-109 - RAM Chip Contents Readout
TID-110 - Hardware Fault Injection – Data Manipulation

Application Software

TID-302 - Install Untrusted Application
TID-303 - Excessive Trust in Offboard Management/IDE Software
TID-304 - Manipulate Runtime Environment
TID-305 - Program Executes Dangerous System Calls
TID-306 - Sandboxed Environments Escaped
TID-307 - Device Code Representations Inconsistent
TID-308 - Code Overwritten to Avoid Detection
TID-309 - Device Exploits Engineering Workstation
TID-310 - Remotely Accessible Unauthenticated Services
TID-311 - Default Credentials
TID-312 - Credential Change Mechanism Can Be Abused
TID-313 - Unauthenticated Session Changes Credential
TID-314 - Passwords Can Be Guessed Using Brute-Force Attempts
TID-315 - Password Retrieval Mechanism Abused
TID-316 - Incorrect Certificate V erification Allows Authentication Bypass
TID-317 - Predictable Cryptographic Key
TID-318 - Insecure Cryptographic Implementation
TID-319 - Cross Site Scripting (XSS)
TID-320 - SQL Injection
TID-321 - HTTP Application Session Hijacking
TID-322 - Cross Site Request Forgery (CSRF)
TID-323 - Path Traversal
TID-324 - HTTP Direct Object Reference
TID-325 - HTTP Injection/Response Splitting
TID-328 - Hardcoded Credentials
TID-329 - Improper Password Storage
TID-330 - Cryptographic Timing Side-Channel

System Software

TID-202 - Exploitable System Network Stack Component
TID-203 - Malicious OS Kernel Driver/ Module Installable
TID-204 - Untrusted Programs Can Access Privileged OS Functions
TID-205 - Existing OS Tools Maliciously Used for Device Manipulation
TID-206 - Memory Management Protections Subver- ted
TID-207 - Container Escape
TID-208 - Virtual Machine Escape
TID-209 - Host Can Manipulate Guest Virtual Machi- nes
TID-212 - FW/SW Update Integrity Shared Secrets Extraction
TID-213 - Faulty FW/SW Update Integrity Verification
TID-214 - Secrets Extracted from Device Root of Trust
TID-216 - Firmware Update Rollbacks Allowed
TID-217 - Remotely Initiated Updates Can Cause DoS
TID-218 - Operating System Susceptible to Rootkit
TID-219 - OS/Kernel Privilege Escalation
TID-220 - Unpatchable Hardware Root of Trust
TID-221 - Authentication Bypass By Message Replay
TID-222 - Critical System Service May Be Disabled
TID-223 - System Susceptible to RAM Scraping
TID-225 - Logs can be manipulated on the device
TID-226 - Device leaks security information in logs

Networking

TID-401 - Undocumented Protocol Features
TID-404 - Remotely Triggerable Deadlock/DoS
TID-405 - Network Stack Resource Exhaustion
TID-406 - Unauthorized Messages or Connections
TID-407 - Missing Message Replay Protection
TID-408 - Unencrypted Sensitive Data Communication
TID-410 - Cryptographic Protocol Side Channel
TID-411 - Weak/Insecure Cryptographic Protocol
TID-412 - Network Routing Capability Abuse

Assets

Assets spielen in der EN 18031 eine zentrale Rolle. Dabei handelt es sich um schützenswerte Werte eines Systems – also alles, was für die Vertraulichkeit, Integrität und Verfügbarkeit (vgl. CIA Triade CyberSec) besonders relevant ist.

Die Norm verlangt, dass diese Assets identifiziert, bewertet und mit geeigneten Schutzmaßnahmen gesichert werden. Hierbei unterscheidet die EN 18031 in ihren drei Teilen verschiedene Asset-Typen: EN 18031-1 behandelt Security und Network Assets, EN 18031-2 ergänzt Privacy Assets (z. B. personenbezogene Daten), und EN 18031-3 umfasst zusätzlich Financial Assets, die sich auf Zahlungs- und Finanzinformationen beziehen. In dieser Case Study konzentrieren wir uns auf die Anforderungen der EN 18031-1.

Cybersecurity: Die CIA-Triade

Betrachtet man die EN 18031-1 genauer, findet man darin folgende Definitionen von Security und Network Assets:

Definition Security Asset

Sicherheitswert ist ein sensibler Sicherheitsparameter bzw. vertraulicher Sicherheitsparameter oder eine Sicherheitsfunktion.
Bsp: Passwörter, Pin, Initialisierungsvektoren, Seed-Werte, Schlüssel allg. symmetrisch oder asymmetrisch, usw.

Der RoDAkku enthält demnach folgende Security Assets:

- ✓ Token zum Authentisieren gegenüber der Cloud
- ✓ Zertifikat zum Aufbau der TLS Verbindung zur Cloud

Definition Network Asset

Netzwerkwert ist die Konfiguration sensibler Netzwerkfunktionen bzw. Konfiguration vertraulicher Netzwerkfunktionen oder die Netzwerkfunktionen selbst.
Bsp: Zugriff aufs Netz (WLAN-Passwort), Einwahldaten, Schlüssel für das Netz, Monitoring und Loggingdaten, usw.

Beim RoDAkku lassen sich folgende Network Assets festhalten:

- ✓ eSIM Daten für Verbindungsaufbau
- ✓ Einwahldaten für Cloud

Anforderungen der Norm EN 18031

Nachdem die Assets definiert wurden, werfen wir einen Blick auf die Anforderungen der EN 18031. Die Normenreihe gliedert sich in mehrere Hauptkategorien, die wiederum in spezifische Unterkategorien unterteilt sind – jede mit eigenen Schwerpunkten und Detailanforderungen.

Nun gilt es, alle zuvor festgelegten Assets durch die Anforderungen der EN 18031-1, -2 und/oder -3 zu führen und zu klären, ob diese jeweils ausreichend erfüllt sind. Dieser Prozess wird von Entscheidungsbäumen unterstützt.

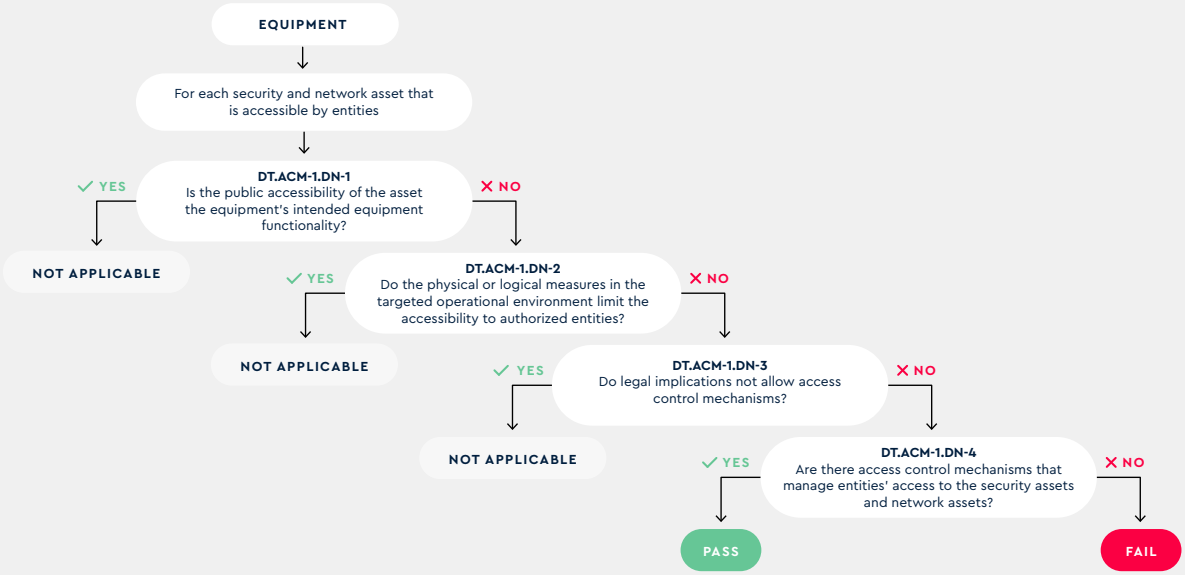
Hier ein Überblick der Normungsbehörde CEN/CENELEC:

Requirement	-1	-2	-3
ACM Access control mechanism	✓	✓	✓
AUM Authentication mechanism	✓	✓	✓
SUM Secure update mechanism	✓	✓	✓
SCM Secure communication mechanism	✓	✓	✓
SSM Secure storage mechanism	✓	✓	✓
LGM Logging mechanism	–	✓	✓
DLM Deletion mechanism	–	✓	
UNM User notification mechanism	–	✓	–
RLM Resilience mechanism	✓	–	–
NMM Network monitoring mechanism	✓	–	–
TCM Traffic control mechanism	✓	–	–
CCK Confidential cryptographic keys	✓	✓	✓
GEC General equipment capabilities	✓	✓	✓
CRY Cryptography	✓	✓	✓

Auszug aus Anforderungen der EN 18031–1 zum RoDAkku

ACM-1 Access Management

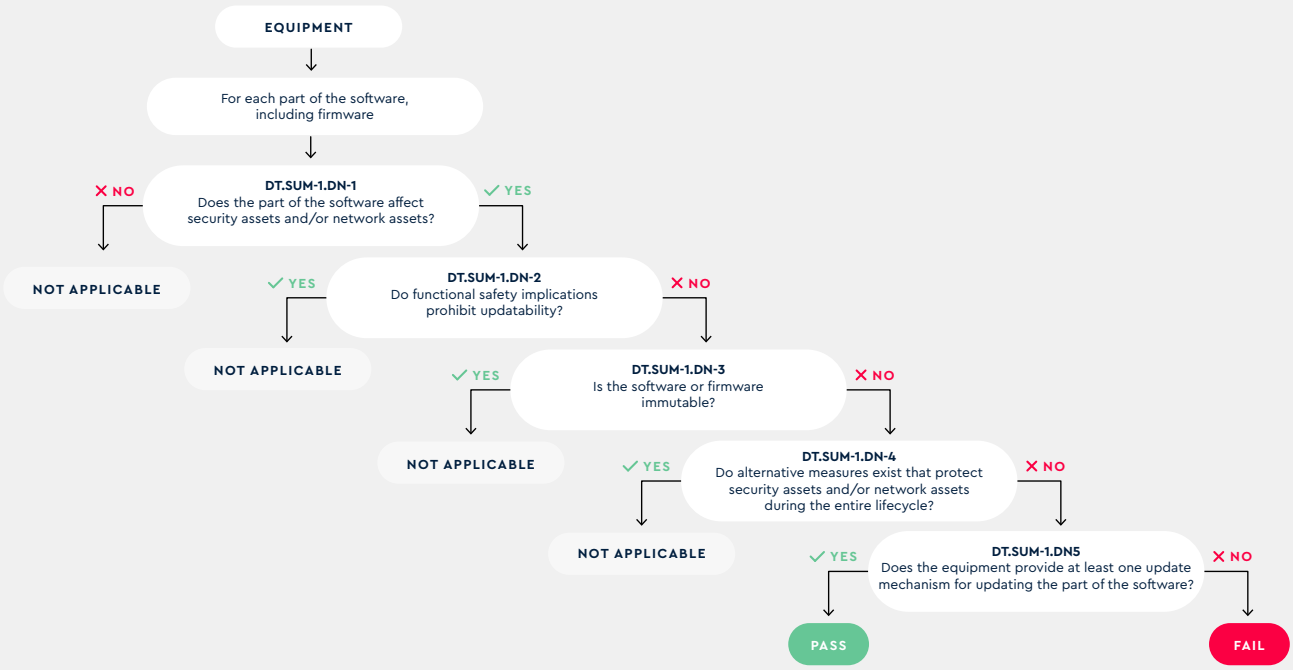
Beim Access Management (ACM-1) zeigt der Entscheidungsbaum, dass diese Kategorie nur dann relevant ist, wenn externe Entitäten Zugriff auf die definierten Assets haben. Im Fall des RoDAkku werden alle Assets bereits während der Produktion fest in das Produkt integriert und sind später von außen nicht zugänglich. Daher ist diese Anforderung für unser Beispiel nicht anwendbar (N/A). In der Folge entfällt auch ACM-2 sowie AUM (Access Use Management), da ein geregelter Zugriff auf die Assets schlicht nicht vorgesehen ist.



SUM-1 Secure Update Mechanism

Auch beim Secure Update Mechanism (SUM-1) zeigt sich schnell: Da unsere Assets fest in das System eingebrannt sind, hat die Software keinen Einfluss mehr auf diese sicherheitskritischen Werte.

Deshalb ist bereits am ersten Entscheidungspunkt klar, dass diese Kategorie für den RoDAkku nicht anwendbar ist (N/A). Folglich entfallen auch die weiteren Unterpunkte SUM-2 und SUM-3.

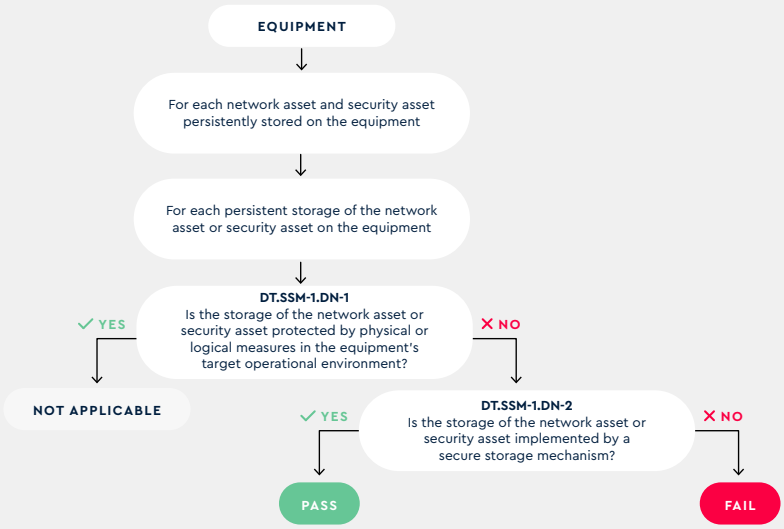


SSM-1 Secure Storage Mechanism

Beim Secure Storage Mechanism (SSM) gibt es grundsätzlich zwei Ansätze: Entweder bietet die Hardware bereits integrierte Mechanismen zum Schutz der Assets, oder der Schutz wird durch physische Maßnahmen sichergestellt. Im Fall des RoDAkku setzen wir auf Letzteres: Die sensiblen Assets werden direkt am Roller durch ein robustes, abschirmendes Gehäuse geschützt, sodass potenzielle Angreifer keinen Zugriff auf die Hardware und damit auf die gespeicherten Werte erlangen können.

Nach diesem Prinzip werden alle identifizierten Assets systematisch durch die relevanten Anforderungen der EN 18031-1 geführt.

Aufgrund der Komplexität und der Vielzahl an Details ist es empfehlenswert, die **Beurteilung durch erfahrene Experten** begleiten zu lassen. Wir stehen Ihnen hier gerne mit Fachwissen und konkreter Unterstützung zur Seite, um Ihr Projekt sicher und konform umzusetzen.



Assessment

Nachdem die Anforderungen der Norm an das Produkt nun Schritt für Schritt betrachtet wurden, kommen wir zum abschließenden Teil: das Assessment.

Hier wird systematisch geprüft und dokumentiert, ob und wie die Anforderungen der RED – insbesondere die aus der EN 18031 – im eigenen Produkt umgesetzt wurden. Es geht hier nicht nur darum, eine Checkliste abzuarbeiten, sondern nachzuweisen, dass die im Produkt eingesetzten Maßnahmen geeignet, vollständig und nachvollziehbar dokumentiert sind.

Ausführlicher formuliert umfasst die Bewertung folgende drei Ebenen:

- **Beurteilung der funktionalen Suffizienz**: Wie wurden die definierten Maßnahmen konkret im System umgesetzt und getestet?
- **Beurteilung der funktionalen Vollständigkeit**: Wurden alle vorgesehenen sicherheitsrelevanten Funktionen berücksichtigt oder liegen zusätzliche potenzielle Lücken vor? Wie wurde darauf getestet? Mit welchen Tools?
- **Konzeptuelle Beurteilung:** Ist die Dokumentation plausibel, vollständig und verständlich?

Das Assessment kann schnell umfangreich und ressourcenintensiv werden. Wir unterstützen Sie gerne bei der Durchführung aller notwendigen Tests.

Konformitätsbewertung

Nach Abschluss des Assessments folgt die formale Konformitätsbewertung. Seit der Veröffentlichung im Amtsblatt und dem EU-Durchführungsbeschluss 2025/138 gelten die Normen der EN 18031 als harmonisiert, sodass ein Selbstassessment möglich ist.
Wichtige Einschränkungen laut Beschluss:

- **EN 18031:** Die Begründungen und Leitlinien in den Normen gelten als Hilfestellung, sie begründen aber keine automatische Konformitätsvermutung.
- **EN 18031-1:** Ein Standardpasswort wie „kein Passwort" ist unzulässig.
- **EN 18031-2:** Ohne funktionierende Zugangskontrolle durch Eltern liegt keine Konformität vor (bei Produkten für Kinder).
- **EN 18031-3:** Für sichere Updates reicht es nicht aus, nur eine einzelne Schutzmethode einzusetzen.

Das bedeutet: Formal darf jedes Unternehmen ein Selbstassessment durchführen. In der Praxis stellt die Komplexität der erforderlichen Bewertungen jedoch viele Organisationen vor Herausforderungen.

Ausblick & Handlungsempfehlungen

Die RED stellt viele Hersteller vor große Herausforderungen. Die beispielhafte Betrachtung am RoDAkku zeigt deutlich, dass hier mit erheblichem Mehraufwand zu rechnen ist – sowohl in technischer als auch in organisatorischer Hinsicht.
Um Kosten, Ressourcen und Zeit zu sparen, lohnt es sich, die Unterstützung erfahrener Experten in Anspruch zu nehmen.

TQ bietet Ihnen dazu praxisnahe Unterstützung, abgestimmt auf Ihren Bedarf:

- **TechTalk Radio Equipment Directive:** Was Sie jetzt wissen müssen.
- **Workshop Radio Equipment Directive:** Heute vorbereiten. Morgen profitieren.
- **Persönliche Beratung** unserer Cybersecurity-Experten

Über den Autor

Ralf Wagner ist Produkt Cybersecurity Manager und hierbei u. a. verantwortlich für die Umsetzung der kommenden EU-Gesetze. Er ist Dipl.-Ing. (FH) für Kommunikationstechnik und Major d. R. beim Cyber- und Informationsraum der Bundeswehr. Hier entwickelte er auch sein Interesse an der Verteidigung des Cyberraumes und den Methoden, Werkzeugen und Taktiken von Hackern.

Das **Technologie-Unternehmen TQ-Group** bietet das komplette Leistungsspektrum von der Entwicklung, Produktion und Service bis hin zum Produktlebenszyklusmanagement. Die Dienstleistungen umfassen dabei Baugruppen, Geräte und Systeme inklusive Hardware, Software und Mechanik. Kunden können bei TQ sämtliche Leistungen modular als Einzelleistungen wie auch im Komplettpaket entsprechend ihrer individuellen Anforderungen beziehen. Standardprodukte wie fertige Mikrocontrollermodule (Minimodule), Antriebs- und Automatisierungslösungen ergänzen das Dienstleistungsspektrum.

Die TQ-Group beschäftigt an den Standorten Delling, Seefeld, Inning, Augsburg, Peiting, Durach im Allgäu, Wetter an der Ruhr, Chemnitz, Leipzig, Celje (Slowenien), Budapest (Ungarn), Shanghai (China), Shenzen (China) und Chesapeake (USA) insgesamt rund 2.100 Mitarbeiter.

Ihr Kontakt zu TQ

Wie bringen Sie Ihr Produkt schnell und einfach durch die Radio Equipment Directive? Wir liefern die Antwort. Kontaktieren Sie uns jetzt und profitieren Sie von unseren erfahrenen Cybersecurity-Experten.

ralf.wagner@tq-group.com
+49 3714 33151-36
tq-group.com/pcc

Entdecken Sie unseren kostenlosen Onepager zur Radio Equipment Directive und finden Sie in 60 Sekunden heraus, ob Ihr Produkt betroffen ist.

Zum Onepager