Vestas

Wind. It means the world to us.™

Perspektiver på Cybersikkerhed: OT

David Steele – Vestas Wind Systems

Introduktion

Hvad er OT ift. IT?

- OT = Operationel Teknologi
  - Definition: *Operativ teknologi (OT) består af hardware og software, som registrerer eller forårsager en handling gennem direkte overvågning og/eller kontrol af industrielt udstyr, aktiver, processer og "events" (begivenheder).*

- Forskellen mellem IT og OT?
  - OT enheder styrer noget i den fysiske verden. IT systemer håndterer data.
  - OT styres typisk af IACS (Industrial Automation & Control Systems)
    - IACS består af: Control systemer (computere og PLCer), netværk, SCADA systemer, HMI (Human Machine Interfaces), osv.
  - Konsekvensen af tab af funktionalitet / funktionsfejl
    - Fysisk effekt
    - Potentiel HW skade
    - Kritisk Infrastruktur

Konsekvenser af Funktionstab / Funktionsfejl på OT

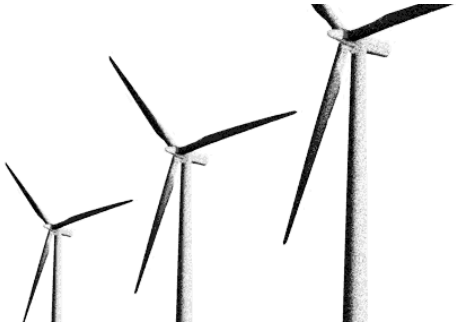
Byggekran
Tab af kontrol: Menneskelig skade
Tab af kontrol: evt. kollaps
Kollaps: evt. skade af nærliggende bygninger

Funktionstab: Nedetid, forsinkelse af projektet (€)
Kan kræve erstatning af kranen → ugers forsinkelse, høj omkostning

Fabrik
Funktionsfejl: produktionsstop
Funktionsfejl: skade af udstyr

Tabt produktion → tabt indtjening
Kritisk produkt → **Mangel på kritiske produkter** (f.eks. medicin, mad, osv.)

Vindturbine
Funktionsfejl: Menneskelig skade



Funktionsfejl: Nedetid,
Tabt energiproduktion,
→ Ustabilitet/fejl i elnettet
→ **Evt. Kollaps af elnettet**
HW skade: lang genoprettelsestid

Vandforsyning og Vandrensningsanlæg
Funktionsfejl: Forurenet drikkevand, ubehandlet spildevand sendt ud i naturen. Evt. skade på vandværket

Ingen/forurenet drikkevand
→ **vandforsyningskrise**
I tilfælde af skade:
lang genoprettelsestid

Kritisk Infrastruktur Områder

Særlige OT områder er oplagte mål for cyberangreb,

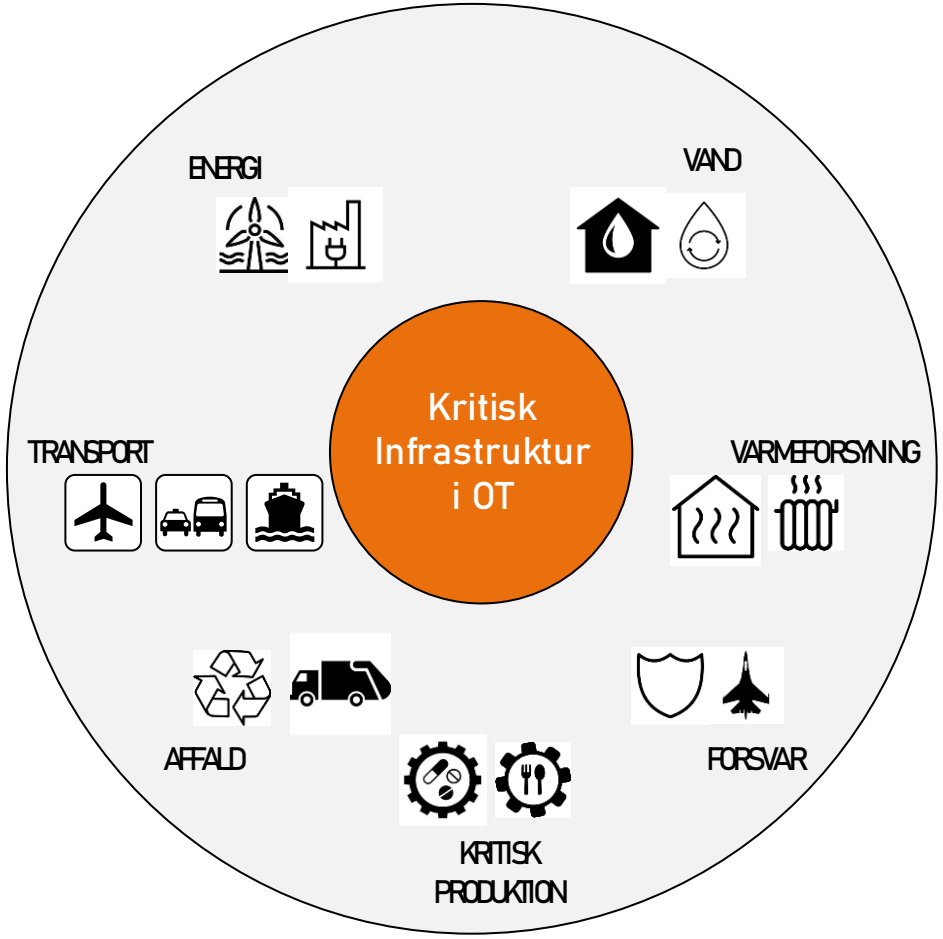
- Alvorlig trussel mod offentligheden
  - Madproduktion / vandforsyning
  - Sundhedskritiske områder
  - Elproduktion
  - Affaldshåndtering
- Erhvervs-kritisk (f.eks. Skibstransport)
- Forsvars-kritisk

Skade af OT systemer:

- Genopretning af IT systemer + sikkerhed,
- **Reparation, erstatning af industriel HW under kontrol → evt. lang genopretningstid**

Eksempel: Maj 2021: Cyberangreb på olieforsyningsnettet i USA

- Tabt olieproduktion på 2.5 millioner tønder / dag i omkring en uge. → lang nedetid



Egenskaber som er typiske for OT Områder

Hvad skal man være særlig opmærksom på indenfor OT

- Komplekse systemer med enheder som ofte består af mange almindelige og ”smart” komponenter
  - Smart sensorer, omskifter, ventiler, aktuatorer osv.
- Distribuerede systemer (”Distributed Systems”)
  - Kompleksitet
  - Lokal kontrol af aktuatorer (f.eks. Sporskifter på jernbane eller substations komponenter i elnettet.)
- Mange forskellige interessenter i kontakt med systemet:
  - Installation
  - Drift
  - Service
- Forskellige myndigheder som styrer forskellige aspekter af det samme system, f.eks. Elnettet, jernbanen
- Internationale systemer med forskellig lovgivning på cybersikkerhedsområdet, sprog, osv.

→ IEC 62443 serien er tiltænkt disse komplekse scenarier

IEC 62443 Serien

”Industrielle kommunikations netværker – Netværk og System Sikkerhed”

- IEC 62443 er den største cybersikkerhedsstandard i IEC regi.
- Mål: ”at forbedre sikkerhed, tilgængelighed, integritet, fortrolighed af komponenter og systemer brugt i industri-automation og kontrol, og at udgive kriterier for anskaffelse og implementering af sikker industri-automation og kontrolsystemer.”
- Mål-publikum:
  - Slutbrugere
  - Ejeren af aktiverne (”Asset Owner”)
- Dækker meget bredt (alle type enheder og systemer)
- Tilgang:
  - Bygger ovenpå idéer fra andre standarder (bl.a.. IEC/ISO 27000 serien)
  - Fokus på forskelle mellem ”almindelige” IT cybersikkerhed og systemer med Industrielle Automation og Kontrol Systemer (IACS), såsom: Sundhed, Mennesker-sikkerhed/HSE, same integration med risiko analysen for hele projektet/produktet.
  - Delt op i 4 ”strømme” med pt. 13 sektioner.
- Findes også i ”ISA” (”International Society of Automation”) udgave med stort set det samme indhold.
- Integreres på alle andre aspekter af produktets/projektets livscyklus.

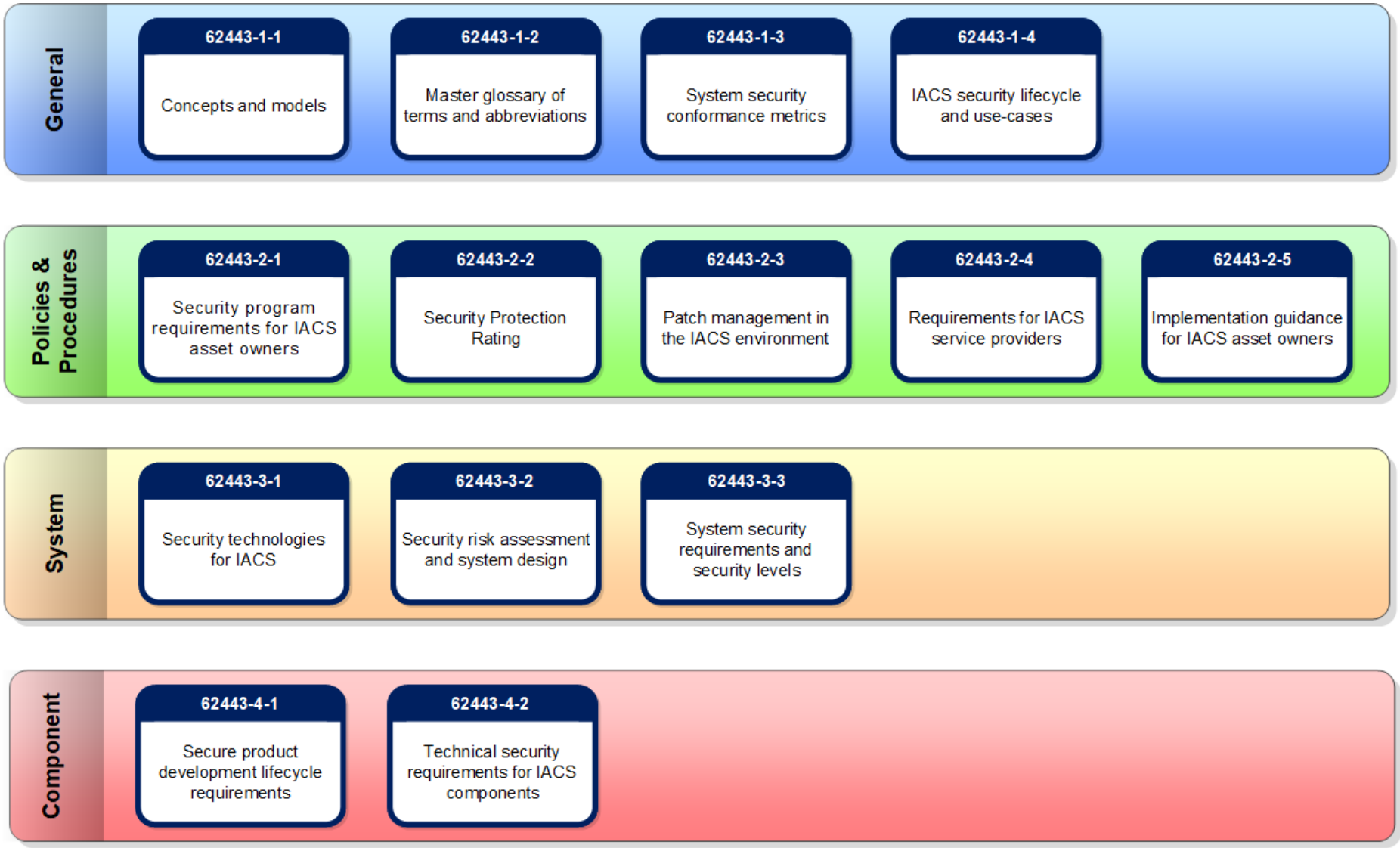
IEC 62443 Struktur

Overordnede rammer og definitioner

“Management” Niveau (dvs. Cybersikkerheds organisation)

System Niveau, inkl. risikovurdering

Produktudvikling

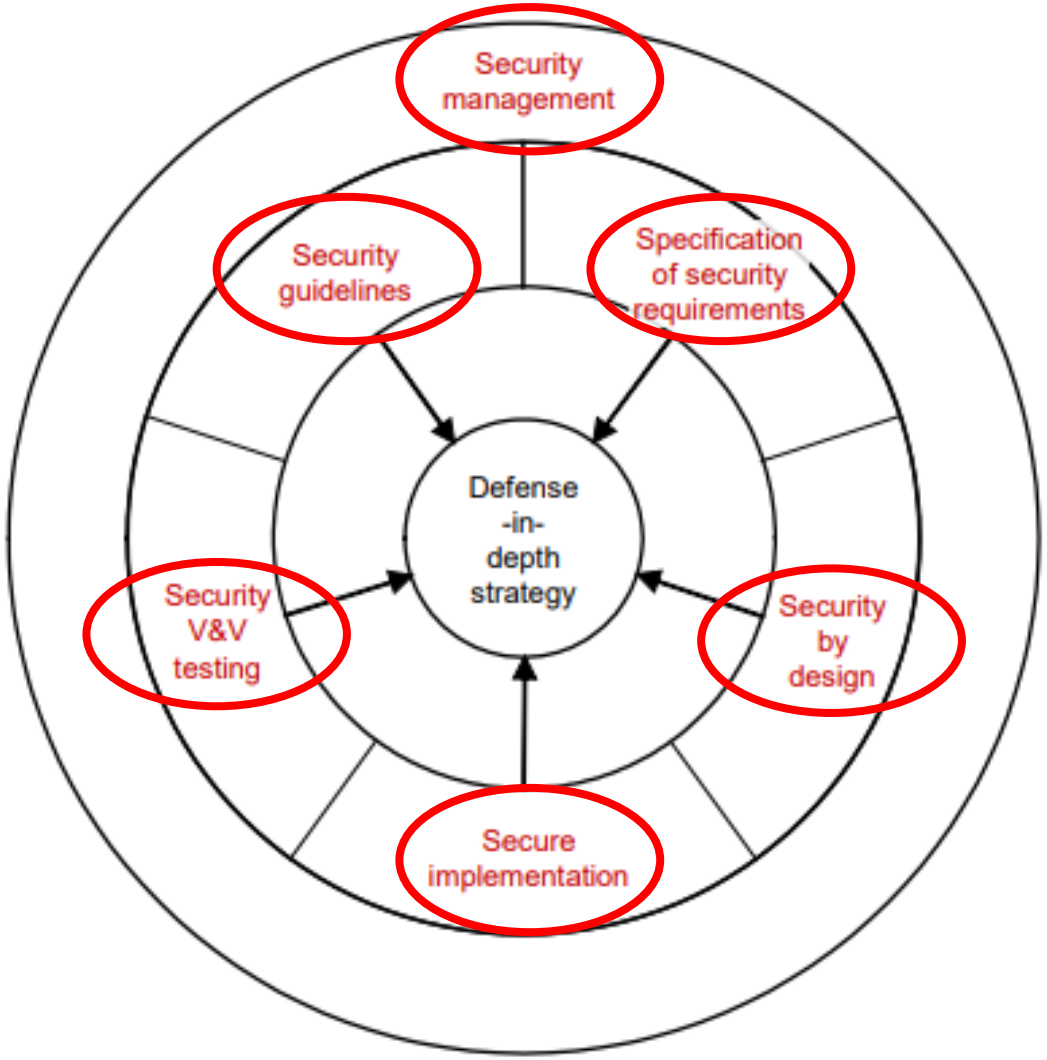


Vestas

”Defense-in-Depth” Strategi

Indlejring af Cybersikkerhed på alle niveauer i firmaet

- IEC 62443 livscyklus er baseret på et sammenhængende system med ”lag”
- Management delen er grundstenen:
  - Styr på cybersikkerhed i alle faser
  - Sikre at intet er blevet overset
- Guidelines sikrer at alle afdelinger arbejder sammen.
- Kravstyring, for at opnå det ønskede sikkerhedniveau (SL)
- Sikkerhed indtænkt på designstadiet, ikke kun ”bagefter”
- Sikker implementation, hvor cybersikkerhedstrusler håndteres på alle softwareniveauer (ikke ”skildpadde”-løsningen)
- Validering mod bl.a. brugstilfælde og kendte svagheder (interne og kendte eksterne, såsom CERT)
- Verifikation ift. cybersikkerhedskrav og beskyttelse imod kendte svagheder.



Vestas

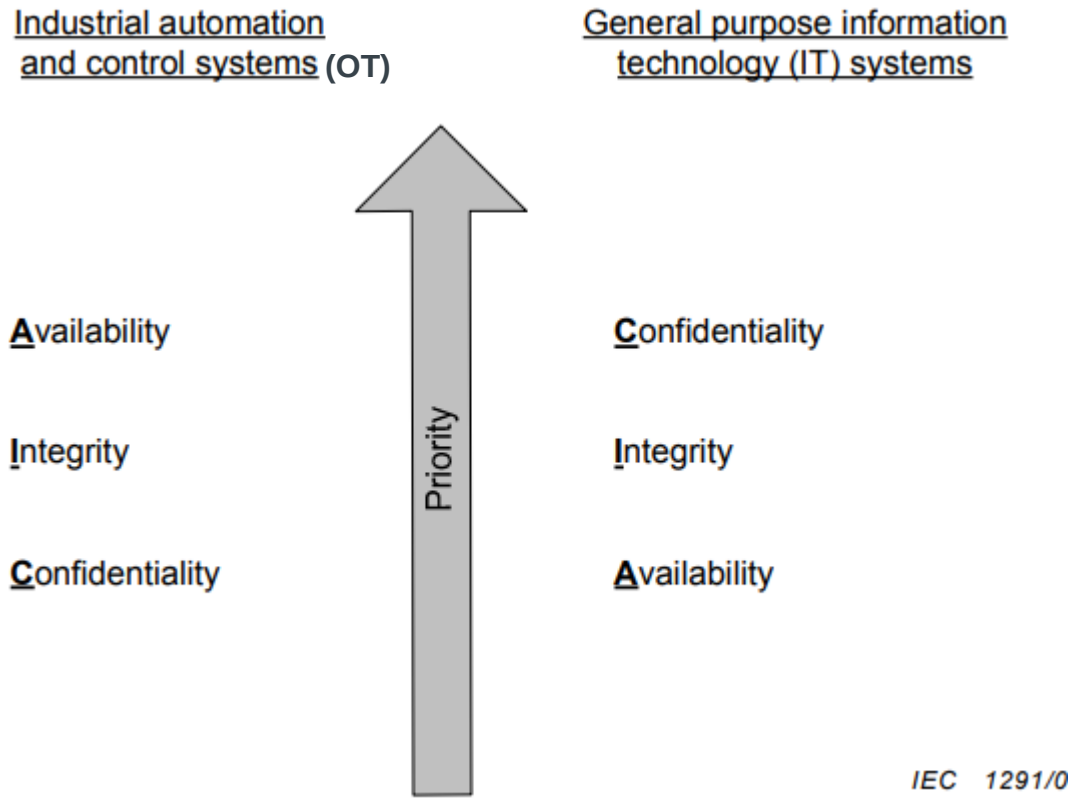
OT vs. IT: IEC 62443

Dækning af OT Aspekter

- Cybersikkerhed standarder dækker typisk tre forskellige områder:
  - Fortrolighed
  - Integritet
  - Tilgængelighed

- Med IACS / OT systemer er prioriteterne ofte anderledes end med IT systemer.

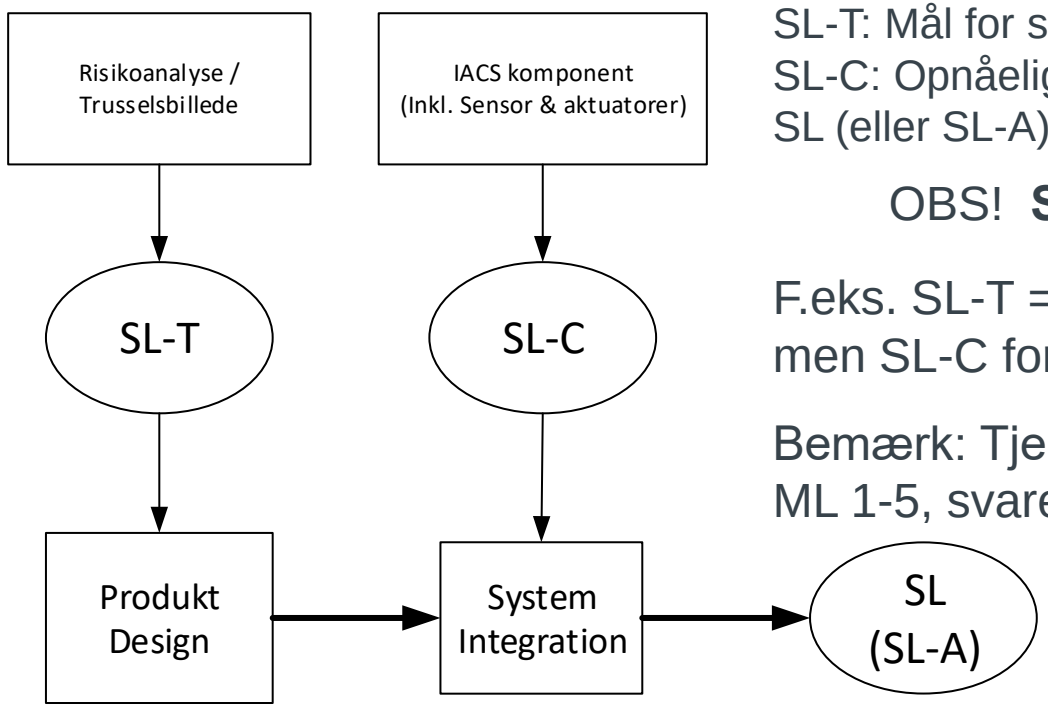
- Integritet og, især, tilgængelighed er ofte vigtigst, dvs. fortsat drift af produktet uden afbrydelse, pga. konsekvensen i tilfælde af funktionssvigt.
  - Alvorlige trusler mod offentligheden
  - Enorme pengetab så længe systemet er nede.



IEC 62443 – Sikkerhedsniveauer (SL, SL-T, SL-C)

OT-fokus

Sikkerhedsniveau	Forsætlighed	Midler	Resourcer	Færdigheder	Motivation
SL-0	Ingen (Ingen sikkerhed)	N/A	N/A	N/A	N/A
SL-1	Skødeløse eller tilfældig	Enkle	N/A	N/A	N/A
SL-2	Forsætlig	Sofistikerede	Lav	Generiske	Lav
SL-3	Forsætlig	Sofistikerede	Moderate	IACS-specifikke	Moderate
SL-4	Forsætlig	Sofistikerede	Høj	IACS-specifikke	Høj



SL-T: Mål for sikkerhedsniveauet
SL-C: Opnåeligt sikkerhedsniveau
SL (eller SL-A): Opnået sikkerhedsniveau

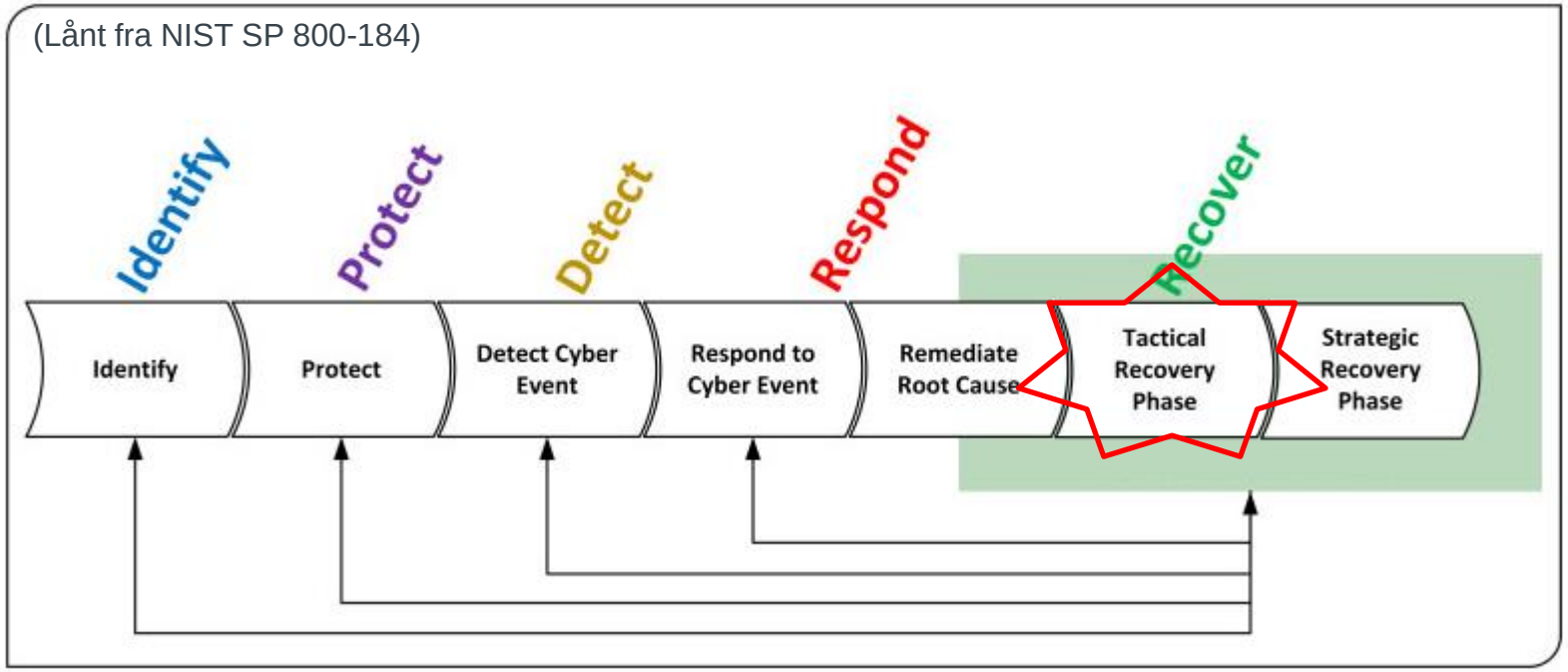
OBS! **SL ≤ Mindst SL-C**

F.eks. SL-T = SL-3,
men SL-C for ét komponent = SL-1 → SL = maks. SL-1.

Bemærk: Tjenesteudbydere: Dækket af "Modenhedsmodel" ML 1-5, svarende nogenlunde til CMMI niveauet.

OT vs. IT: Genoprettelsesfase / ”Recovery Phase”

(Lånt fra NIST SP 800-184)



Genoprettelsesfasen: Vigtig (også i IT verden) men ofte overset og underudviklet. → “Blue Team”
https://en.wikipedia.org/wiki/Blue_team_(computer_security)

I OT verden er den ekstremt vigtig!!!

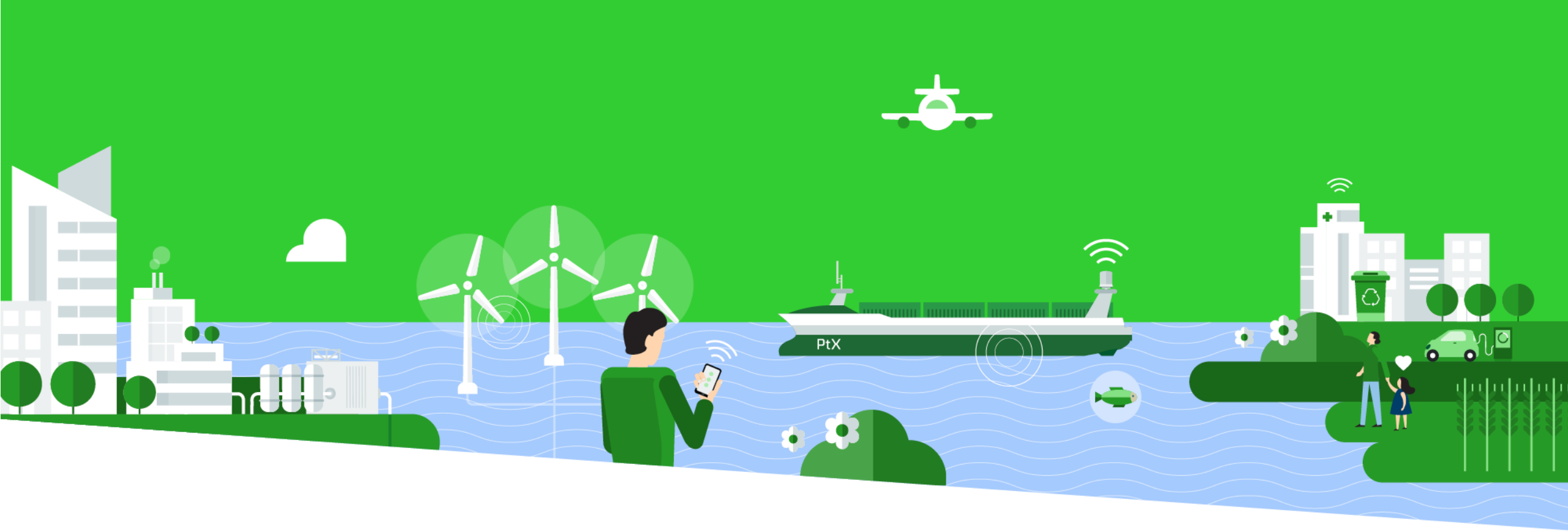
- IT verden (typisk):
  - Stop angrebet, fjern truslen, geninstallerer software, restore data.
  - (Niveauet af skade på IT udstyr er typisk lille.)
- OT verden, alt fra IT ovenfor, plus:
  - **Kontrol og erstatning af fysisk udstyr under kontrol**
  - **Kan tage måneder eller år i alvorlige tilfælde og koste en formue at erstatte (f.eks. stort elværk)**

Cybersikkerhed set fra et OT Perspektiv: IEC 62443 og Tilgængelighed

Konklusion

- OT enheder: styrer noget i den fysiske verden. IT systemer: håndterer data.
- OT styres typisk af IACS (Industrial Automation & Control Systems)
- Konsekvenserne af tab af funktionalitet / funktionsfejl er forskellige mellem OT og IT:
  - Med OT: Fysisk effekt, potentiale HW skade, evt. kritisk Infrastruktur
- OT: meget oplagt mål for cyberangreb, pga. mulighed for trusler mod offentligheden, ofte erhvervskritisk, mv.
- OT: ofte stor kontaktflade til operatører, servicepersonale, osv., nogle gange over landegrænser

- IEC 62443 dækker meget bredt og er egnet til OT systemer med IACS
- Godt Startpunkt: IEC 62443-4-1 (Krav til livscyklus for sikker produktudvikling)
- Centralt element IEC 62443: ”Defense-in-Depth” hvor alle organisationslag og afdelinger bidrager til cybersikkerhed
- IEC 62443s forskellige sektioner tager hensyn til forskellige roller, såsom ”Aktiver ejer”, ”System Integrator”, ”Prod. Udvikler”,
- Genoprettelsesfasen er særlig vigtig i OT mht. at sikre optimal tilgængelighed.



IoT security

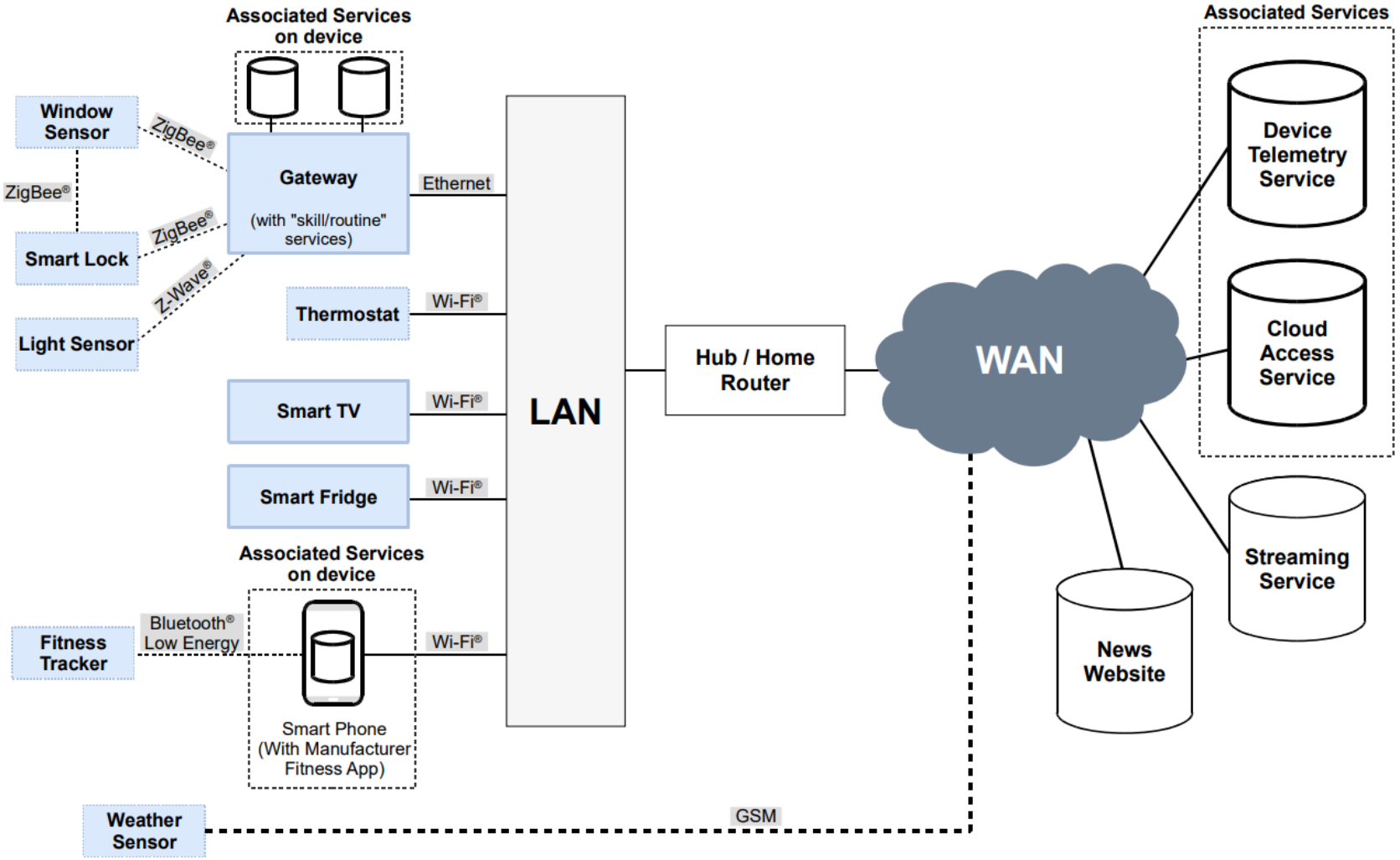
Jeppe Bjerre

Compliance specialist

FORCE Technology

3 October, 2022

Scope – IoT



Source: ETSI EN 303 645

ETSI EN 303 645

3 October, 2022

EN 303 645

EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements

Source: ETSI EN 303 645

EN 303 645

5.1 No universal default passwords

Provision 5.1-1 Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

NOTE: There are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. However if they are used, following best practice on passwords is encouraged according to NIST Special Publication 800-63B [i.3]. Using passwords for machine to machine authentication is generally not appropriate.

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT [i.17] and the practice needs to be discontinued. The above provision can be achieved by the use of pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization, or by some other method that does not use passwords.

EXAMPLE 1: During initialization a device generates certificates that are used to authenticate a user to the device via an associated service like a mobile application.

To increase security, multi-factor authentication, such as use of a password plus OTP procedure, can be used to better protect the device or an associated service. Device security can further be strengthened by having unique and immutable identities.

Source: ETSI EN 303 645

EN 303 645

5.13 Validate input data

Provision 5.13-1 The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

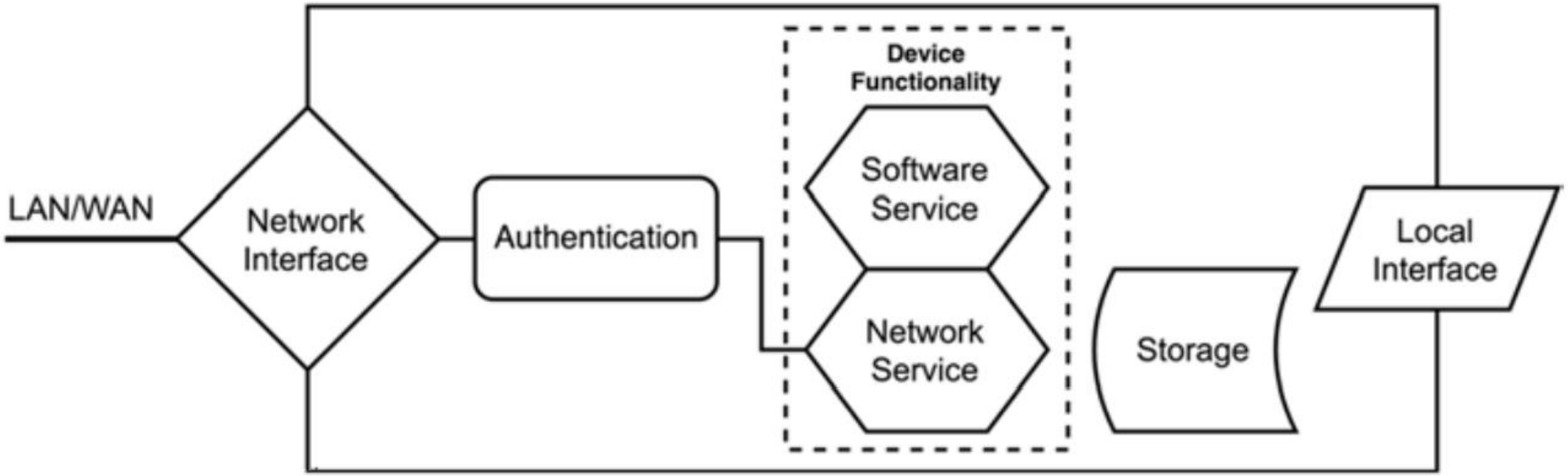
Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools such as fuzzers can be used by attackers or testers to exploit potential gaps and weaknesses that emerge as a result of not validating data.

EXAMPLE 1: The device receives data that is not of the expected type, for example executable code rather than user inputted text. The software on the device has been written so that the input is parameterized or "escaped", preventing this code from being run.

EXAMPLE 2: Out of range data is received by a temperature sensor, rather than trying to process this input it identifies that it is outside of the possible bounds and is discarded and the event is captured in telemetry.

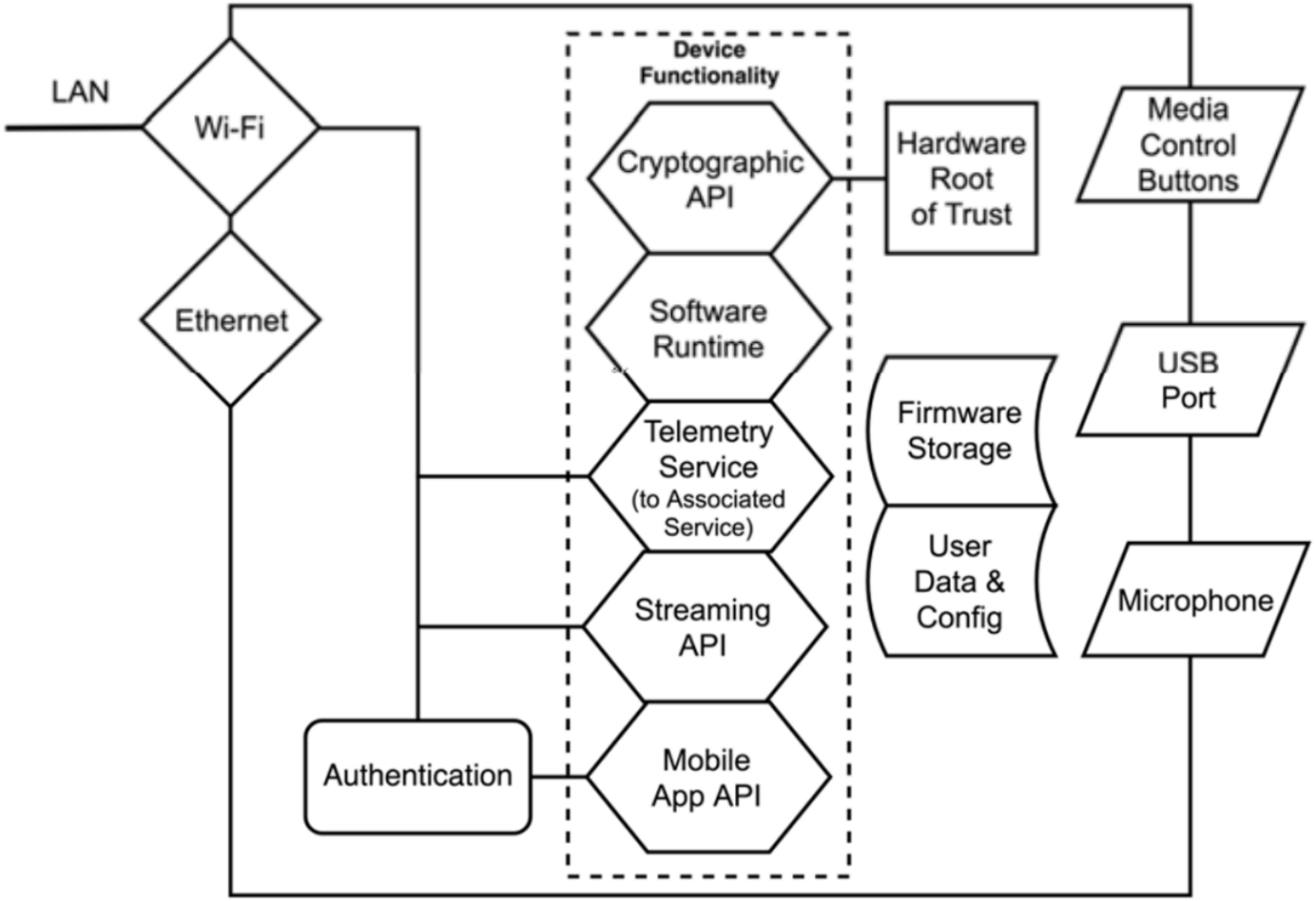
Source: ETSI EN 303 645

EN 303 645 – Example device - Simple



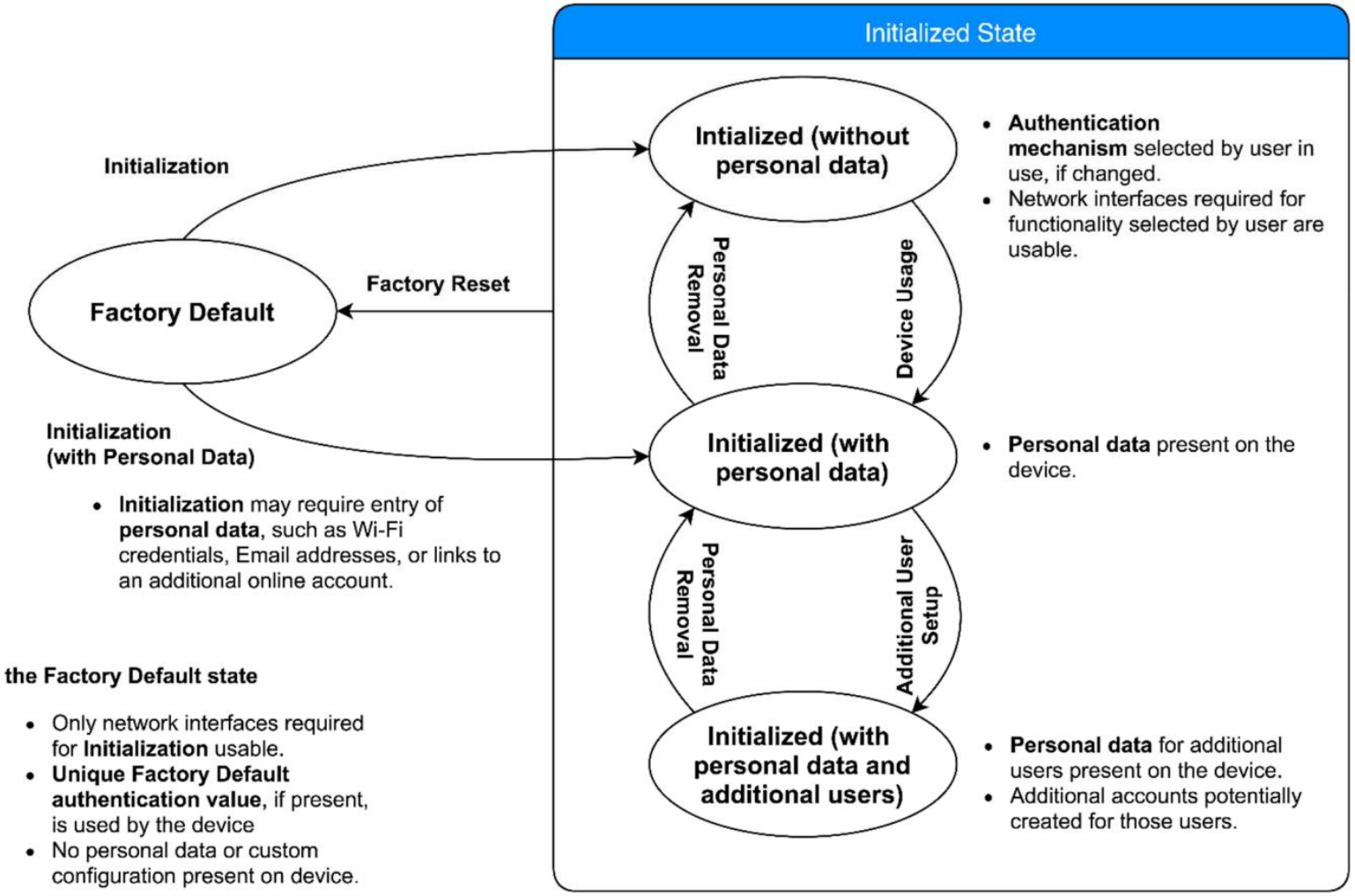
Source: ETSI EN 303 645

EN 303 645 – Example device - Sophisticated



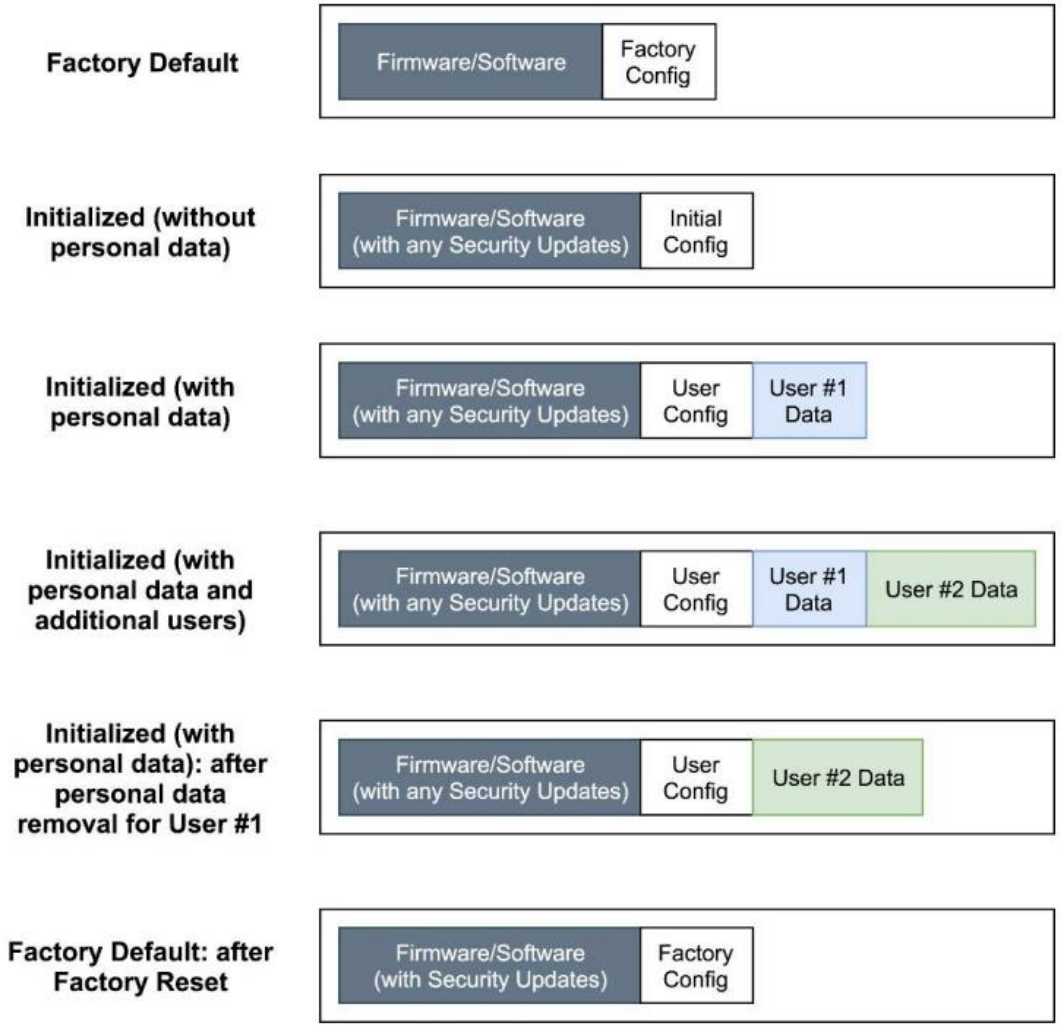
Source: ETSI EN 303 645

EN 303 645 – Device states



Source: ETSI EN 303 645

EN 303 645- Device storage



Source: ETSI EN 303 645

EN 303 645 – Implementation conformance statement

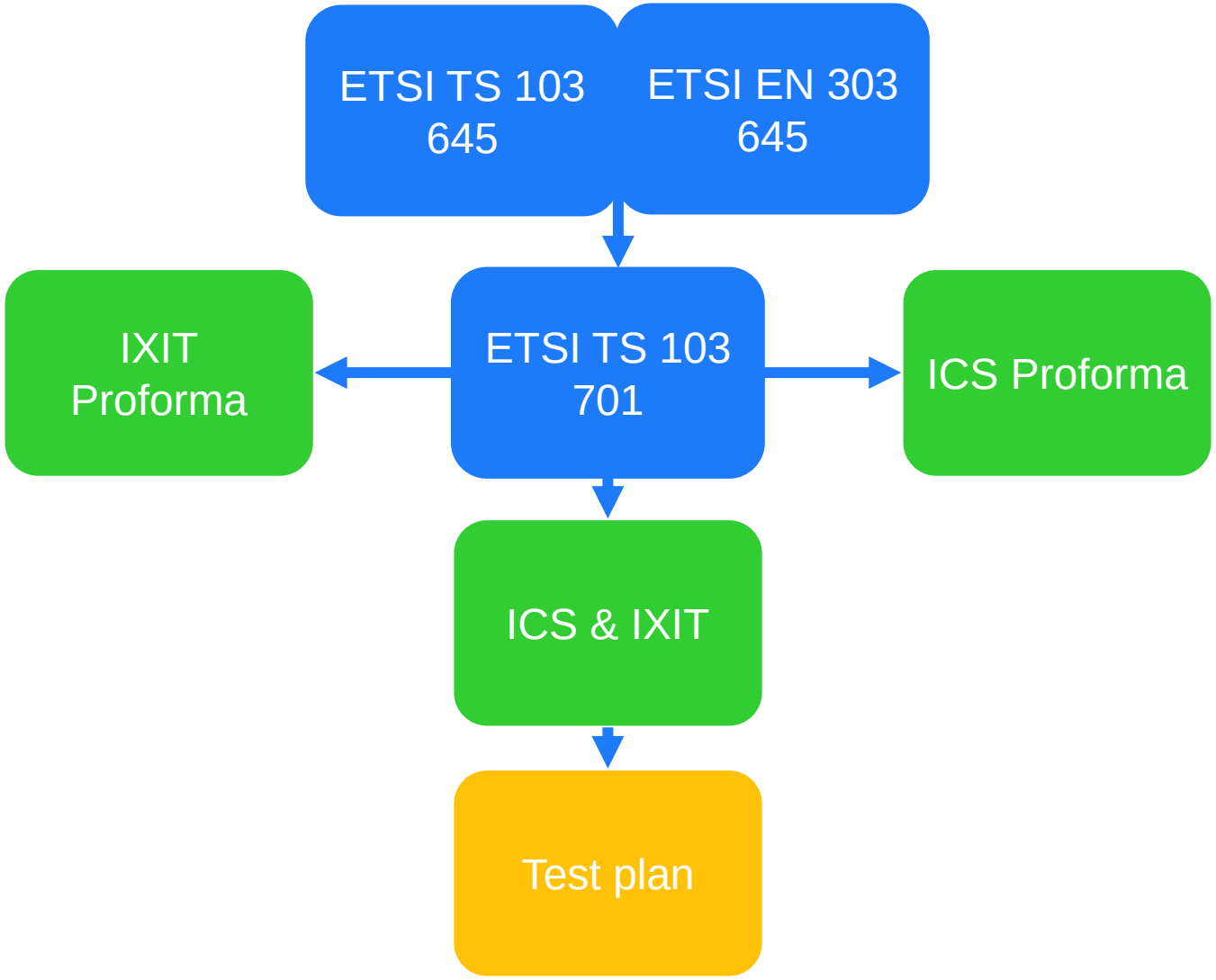
Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.1 No universal default passwords			
Provision 5.1-1	M C (1)		
Provision 5.1-2	M C (2)		
Provision 5.1-3	M		
Provision 5.1-4	M C (8)		
Provision 5.1-5	M C (5)		
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M		
Provision 5.2-2	R		
Provision 5.2-3	R		
5.3 Keep software updated			
Provision 5.3-1	R		
Provision 5.3-2	M C (5)		
Provision 5.3-3	M C (12)		
Provision 5.3-4	R C (12)		
Provision 5.3-5	R C (12)		
Provision 5.3-6	R C (9, 12)		
Provision 5.3-7	M C (12)		

Source: ETSI EN 303 645

ETSI TS 103 701

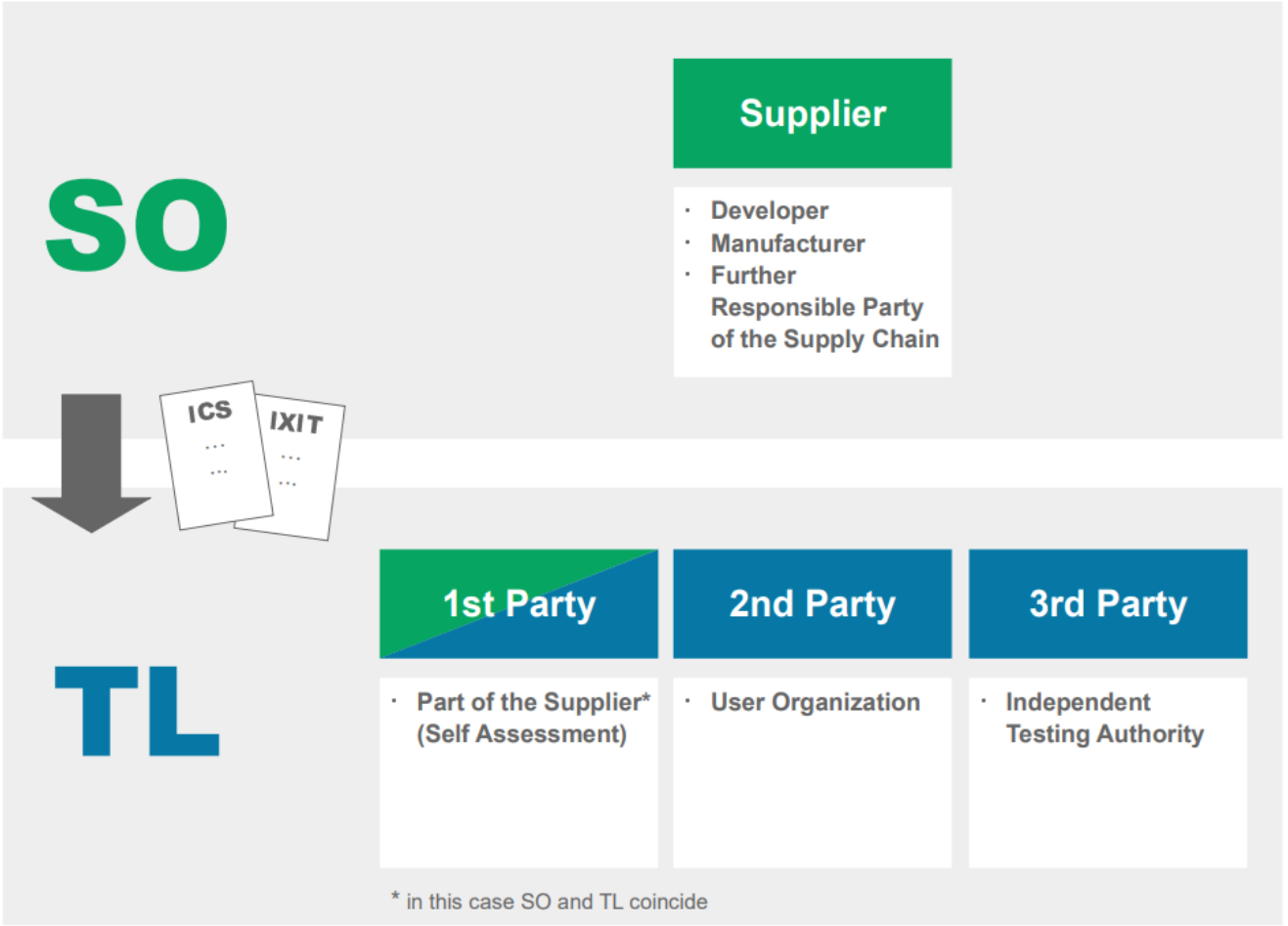
3 October, 2022

TS 103 701 – Test plan



ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention
AuthMech-1	A user can login over HTTPS at port 443 to gain access to the web frontend. (A user can request a login over HTTP at port 80 but is forwarded automatically to HTTPS on port 443.) The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	Username and password (pre-installed and used in initialized state).	The username is fixed "admin". The password is generated randomly and is unique per device. The password has a length of 16 and consists of upper case chars, lower case chars and numbers. The password is generated by use of /dev/urandom on a UNIX configuration system during manufacturing phase.	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via a form-based HTML interface by an internal PHP script in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 3 invalid login attempts the login interface is inaccessible for 5 minutes.
AuthMech-2	A device can exchange data with the DUT over HTTPS/SOAP on port 8085. The authentication via Basic-Auth is confirmed before any payload data over HTTP is exchanged. No payload is readable without providing correct access credentials. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	Username and password (set by user and used in initialized state).	*N/A (Authentication mechanism is password set by the user)*	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via an HTTP authentication framework (IETF RFC 7235 [i.8]) by the internal Apache Webserver in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2 with the TLS cipher suites: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 10 invalid login attempts user/password combination is disabled for further access.

TS 103 701 – Test plan

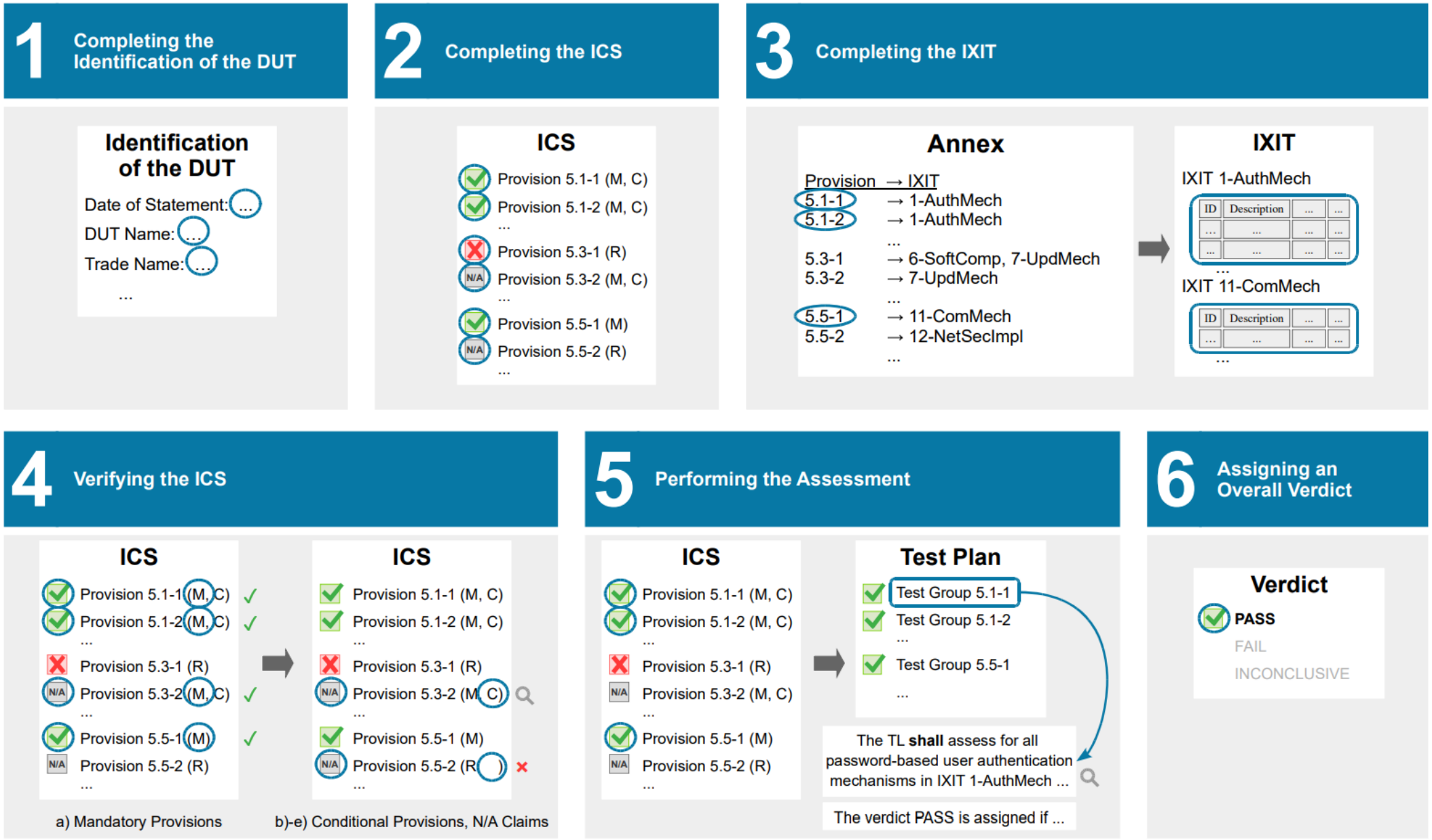


Source: ETSI TS 103 701

TS 103 701 – Test plan

- **Test Scenario (TSO):** named set of related test groups that describe how to assess the conformance of the DUT to a corresponding set of provisions as specified in ETSI TS 103 645 [1]/ETSI EN 303 645 [2]
- **test group:** named set of related test cases that describe how to assess the conformance of the DUT to a single provision as specified in ETSI TS 103 645 [1]/ETSI EN 303 645 [2] NOTE: The naming of test groups and their corresponding provisions coincide.
- **test case:** complete and independent specification of the test units required to achieve a specific test purpose NOTE: The specification is considered to be complete if it is sufficient to enable a test case verdict to be assigned unambiguously to each potentially observable test outcome. The specification is considered to be independent if it is sufficient to execute the test units in isolation from other test cases
  - Conceptual: Assessing conformity of the IXIT against the requirements of the provision (conformity of design); and
  - Functional: Assessing conformity of the DUT functionality, their relation to associated services or development/management processes against the requirements of the provision (conformity of implementation).

Source: ETSI TS 103 701



Source: ETSI TS 103 701

TS 103 701 – Example 5.1-1

5.1 TSO 5.1: No universal default passwords

5.1.1 Test group 5.1-1

5.1.1.0 Test group objective

The test group addresses the provision 5.1-1.

This test group addresses all states of the DUT with the exception of factory default.

TS 103 701 – Example 5.1-1

5.1.1.1 Test case 5.1-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the password-based authentication mechanisms.

Test units

a) The TL **shall** assess for all password-based user authentication mechanisms in IXIT 1-AuthMech where passwords are not defined by the user according to "Authentication Factor" and used in any state other than the factory default whether the "Password Generation Mechanism" ensures that passwords are unique per device.

Assignment of verdict

The verdict PASS is assigned if:

- each password of a password-based authentication mechanism being used in any state other than the factory default, that is not defined by the user, is unique per device.

The verdict FAIL is assigned otherwise.

TS 103 701 – IXIT

IXIT 1-AuthMech: Authentication Mechanisms

The completed IXIT lists all authentication mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 1: Sequential numbering ("AuthMech-1") or labelling scheme ("AuthMech-PswdWebIf").

- **Description:** Brief description of the authentication mechanism and its corresponding authorization process. It is indicated additionally whether the mechanism is used for user or machine-to-machine authentication and whether it is directly addressable from a network interface.

- **Authentication Factor:** The type of attribute used for authentication. For passwords it is indicated additionally whether the password is set by the user and used in the initialized state.

EXAMPLE 2: Password (set by user), password (pre-installed), biometric fingerprint.

- **Password Generation Mechanism:** If the authentication factor is a password, which is not set by the user: Description of the mechanism to generate the password. It is indicated additionally whether the password is unique per device and whether it is pre-installed.

Source: ETSI TS 103 701

TS 103 701 – Example 5.1-1

5.1.1.2 Test case 5.1-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the password-based authentication mechanisms concerning the completeness of the IXIT documentation a), the passwords defined by the user b) and the generation mechanisms c).

Test units

a) The TL **shall** functionally assess whether password-based authentication mechanisms that are not documented in IXIT 1-AuthMech are available via a network interface on the DUT or described in the user manual.

EXAMPLE: Network scanning tools allow for discovery of network-based authentication mechanisms.

b) For each password-based user authentication mechanism in IXIT 1-AuthMech, the TL **shall** functionally check whether the user is required to define all passwords that are user-defined according to "Authentication Factor" before being used.

c) The TL **shall** functionally assess whether all passwords of the DUT, that are not defined by the user according to "Authentication Factor" in IXIT 1-AuthMech and used in any state other than the factory default, do not violate the description of the "Password Generation Mechanism".

TS 103 701 – Example 5.1-1

Assignment of verdict

The verdict PASS is assigned if:

- every discovered password-based authentication mechanism is documented in the IXIT; and
- the user is required to define all passwords before being used, that are stated as defined by the user in the IXIT; and
- there is no indication that the generation of a not user-defined password of the DUT used in any state other than the factory default differs from the generation mechanism described in the IXIT.

Questions

Keep in touch

Jeppe Pilgaard Bjerre
Specialist
jpbj@force.dk
+4543251548
forcetechnology.com

Follow us on: