Xertified point of view: ISA/IEC 62443

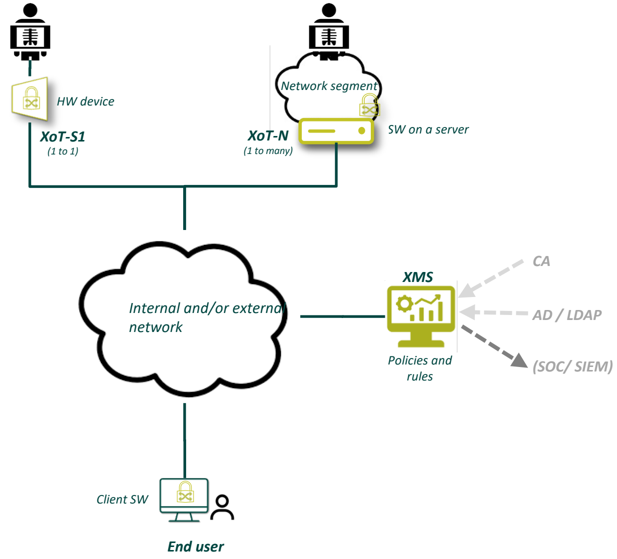
Xertified

XoT technology™ basics

The digital lock 3.

Allow/deny access 2.

The digital key 1.



- A digital lock, **preventing** unauthorised access
- Secures critical devices **within minutes**
- Requires **no configuration** of clients or protected devices
- Brings undeniable digital identities to **legacy systems and new devices**
- **Secures the traffic** between devices and users
- High level security for **any type of device**
- **Multi-layered security** with encryption, digital identities, authentication and traceability

What is ISA/IEC 62443

The ISA/IEC 62443 series of standards, based on ISA-99, is a collaborative effort between several regulators, the main ones being:

- IEC TC65 / WG10
- ANSI / ISA-62443
- ISO / IEC-JTC1-SC27

The motivation to pay close attention to the security of industrial automation and control systems is a consequence of various malicious attacks, from the events of 9/11 in the United States to a widespread threat in all industrialized countries. If adversaries can learn how to operate sophisticated airplanes, it is likely that they can learn how control systems in critical infrastructures such as water supply, power stations, and transportation, as well as sensitive facilities such as chemicals, food processing, and pharmaceuticals.

This prompted the need for best practices, benchmarks, tools, and assessment services for the world of process control, initially started by ISA-99.

ISA/IEC 62443 concepts

The security of industrial control systems is based on three main areas of the organization:

- people
- procedures (process)
- technology used

These three pillars of cybersecurity must meet the following general requirements:

- Must not affect the security functions of industrial systems,
- Apply countermeasures to achieve the required level of security, or even prevent attacks

Principle of least privilege

Only give users the rights they need to perform their work, to prevent unwanted access to data or programs and to block or slow an attack if an account is compromised.

Defence in depth

Delay or prevent a cyber attack in the industrial network. Requires that systems is separated into groups called “zones” that will be able to communicate with each other through communication channels called “conduits”.

Risk analysis

Addresses risks related to production infrastructure, production capacity (production downtime), impact on people (injury, death), and the environment (pollution)

Adherence to ISA/IEC 62443

ISA/IEC 62443 establishes 7 Foundational Requirements (FR):

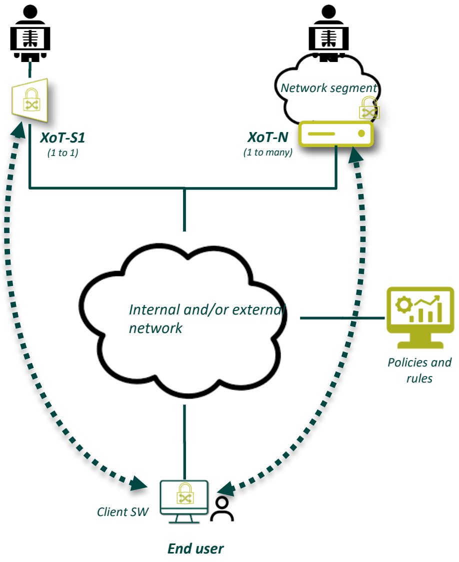
FR	Directly	Indirectly
1 – Identification, Authentication control and Access control (AC)	✓	
2 – User Control (UC)	✓	
3 – Data Integrity (DI)	✓	
4 – Data Confidentiality (DC)	✓	
5 – Restrict Data Flow (RDF)		✓
6 – Timely Response to Events (TRE)		✓
7 – Resource Availability (RA)		✓

Foundational Requirement 1

Access Control (AC)

The core of XoT technology – using undeniable digital identities for authentication and access control

Authentication / digital identity



What is FR 1?

FR1 - Identification, Authentication Control and Access Control (AC)

Identifies and authenticates all users (human, process, and equipment) before allowing access to the Industrial Automation and Control System (IACS)

FR 1 vs XoT technology

Built on zero trust and undeniable digital identities to only allow trusted users access to trusted devices

Based on:

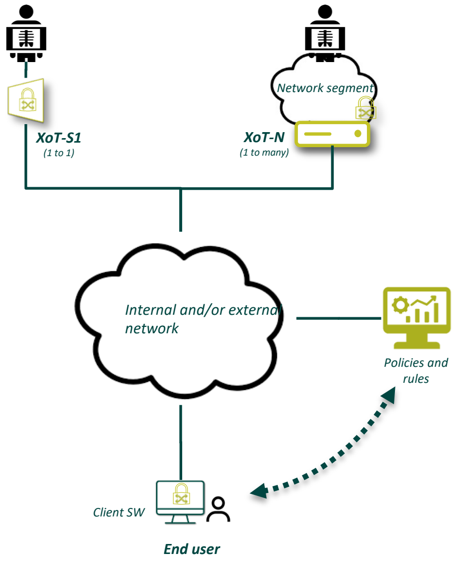
- PKI
- Undeniable digital identities
- Connection to customer user groups through AD/IAM/PAM or similar
- Continuous authentication, even during active sessions
- Allowing client and device to authenticate each other, bi-directionally

Foundational Requirement 2

User Control (UC)

Only trusted users (or devices) can access trusted devices. Man->machine & machine->machine

Policy based security



What is FR 2?

FR2 – Securing privileges for trusted users

Ensures that all identified users (human, process, and device) have privileges to perform the required actions on the system and monitors the use of those privileges

FR 2 vs XoT technology

Uses policies and rules, set by each customer to control access rights

Access rights to devices and resources can be set based on:

- Location of the protected device/resource
- Location of the user
- Type of device/resource
- Date/time

Trusted users are :

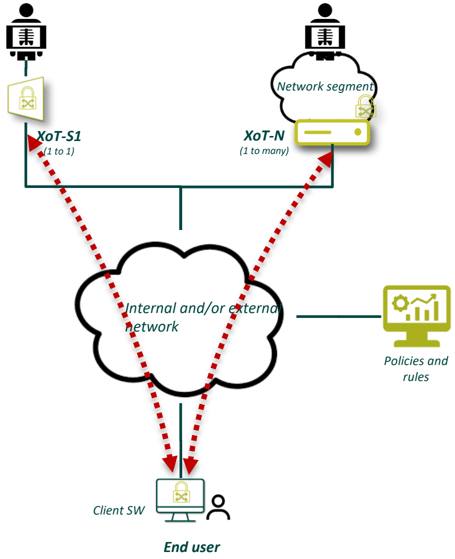
- LDAP/AD systems
- Identity Access Management (IAM)
- Privileged Access Management (PAM)

Foundational Requirement 3

Data Integrity (DI)

Secure communication with end-to-end uninterrupted encryption

Multi-layered encryption



What is FR 3?

FR3 – Data Integrity

Ensures the integrity of equipment and information (protection against unauthorized changes) in communication channels and storage directories.

FR 3 vs XoT technology

Uses two layers of encryption, one for access control and one for data communication

Equipment / devices are protected through rigid access control:

- Allowing trusted users access based on role and associated policies
- Blocking all other users and warning when someone tries to breach the security

Information is protected through end-to-end encryption of all data in motion:

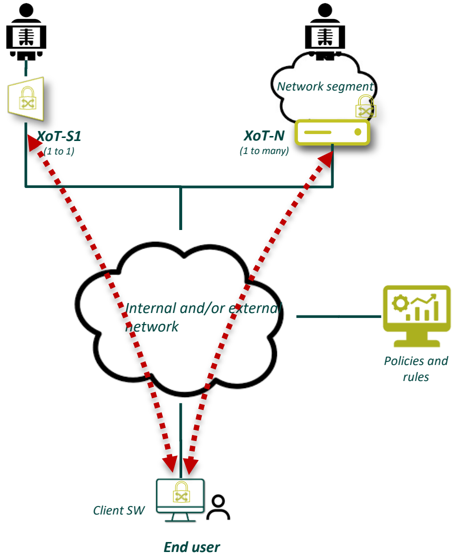
- PKI to secure the user identity and enable challenge-response methodology
- Wireguard with session-based keys for all communication between the equipment and the end user

Foundational Requirement 4

Data Confidentiality (DC)

End-to-end encryption secures any type of communication. Access control limits data propagation

Authentication / digital identity



What is FR 4?

FR4 – Data Confidentiality

Ensures that information flowing through communication channels and storage directories is not distributed

FR 4 vs XoT technology

Secures the data in transit but NOT the data in storage

Information is protected through end-to-end encryption of all data in motion:

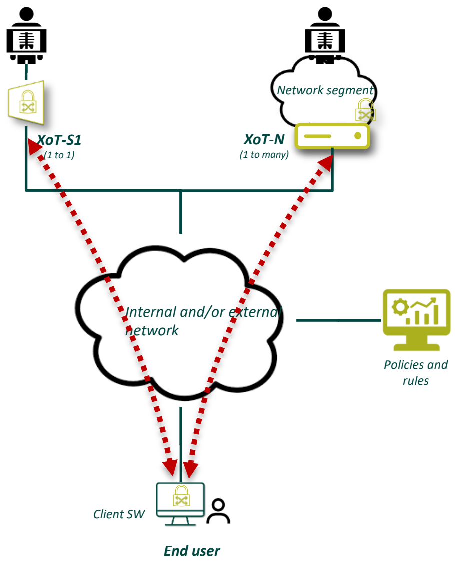
- PKI to secure the user identity and enable challenge-response methodology
- Wireguard with session-based keys for all communication between the equipment and the end user

Foundational Requirement 5

Restrict Data Flow (RDF)

Data can only flow between resources and users that are known and trusted

Trusted user->trusted device



What is FR 5?

FR5 – Data Confidentiality

Segments the system into zones and conduits to avoid unnecessary data propagation

FR 5 vs XoT technology

Ensures that only trusted users can access critical devices and any related information

By using strict access control, the flow of information is significantly reduced and can be strictly controlled:

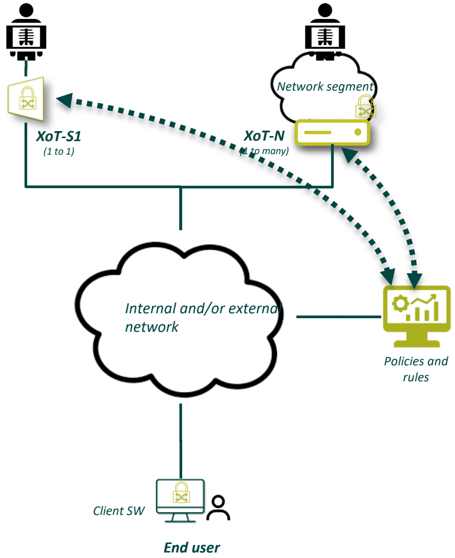
- PKI to secure the user identity and enable challenge-response methodology
- Data can only flow between trusted users and trusted devices
- Policy based security that can create desired segmentation without creating zones

Foundational Requirement 6

Timely response (TRE)

The system collects logs and alarms that can be analysed by a 3rd party SIEM system in close to real-time

Trusted user->trusted device



What is FR 6?

FR6 – Timely Response to Events

Responds to security breaches with timely reporting and timely decision making

FR 6 vs XoT technology

Logging certain events and alarms and can complement SIEM systems in collecting additional data and thereby support decision making

Each XoT HW or SW unit will log a series of events and alarms that will be sent to the management system continuously, e.g.:

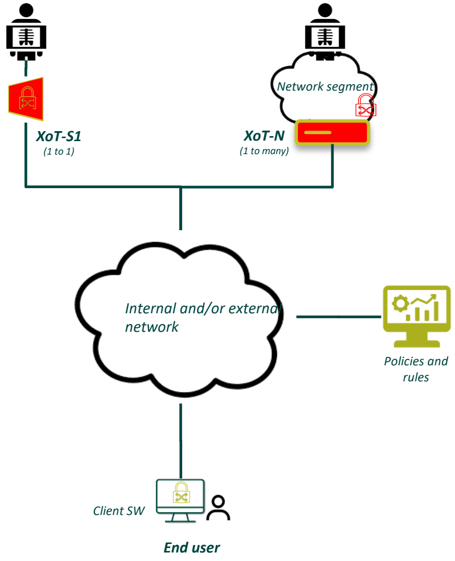
- Power outage
- Loss of connection
- Changes in traffic patterns/behaviour
- Access attempts from non-trusted users
- Access made by trusted users
- Data sent (amount and destination)

Foundational Requirement 7

Resource availability (RA)

No traffic can pass the digital lock and any device behind will remain unaffected by a DDoS attack

Blocking DDoS attacks



What is FR 7?

FR7 – Resource Availability

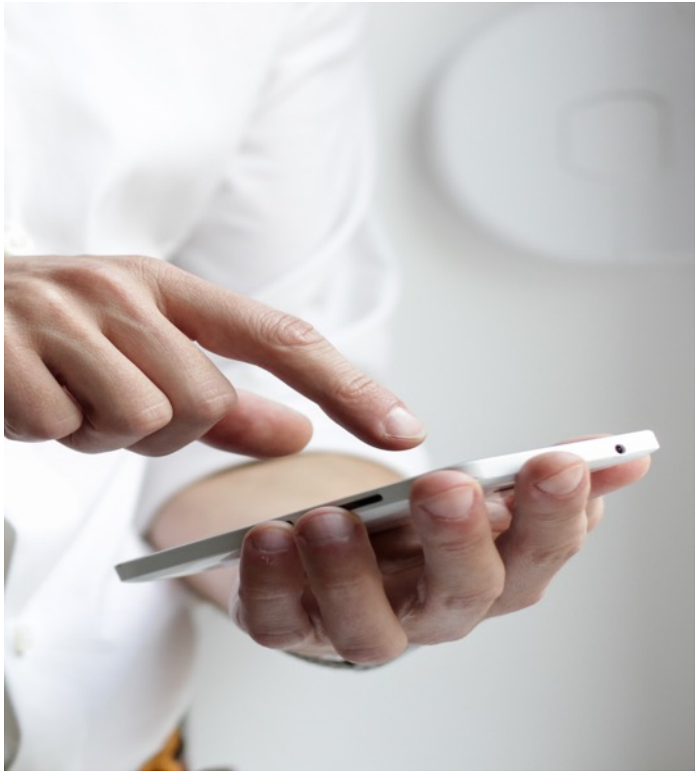
Ensures system and asset availability during denial-of-service attacks

FR 7 vs XoT technology

XoT technology prevents breaches and attacks but does not in itself ensure resource availability

The XoT solution withstands DDoS attacks as it functions on its own without a management system (XMS). There are no single-point-of-failure, and this significantly reduces effects from denial-of-service attacks:

- The system as such cannot be stopped
- Only the targeted and specific XoT HW or SW unit can be exposed to the attack
- With duplicate routes to a critical system the effects can be significantly reduced
- The secured device can continue to operate but may suffer from limited communication temporarily, unless redundant communication methods are in place



Everything connected can be exposed.

Until now.