GIMELEC
Nous décuplons les énergies

OPC FOUNDATION

OPC UA Tech Day 2023 – OPC UA Security

LACROIX Vincent - Systerel

20/06/2023

Why Cyber-Security ?

Why we need to care about Cybersecurity ?

Some myths about ICS Cybersecurity persist in 2023:

1. ICS network are isolated then protected
2. Proprietary protocols are not at risk
3. Cybersecurity is not compatible with my availability constraints
4. Cybersecurity is expensive

These myths slow down the deployment of even simple defense mechanisms.

Source ANSSI: Managing_Cybe_for_ICS_EN.pdf

Threats remain at a high level

Why cyber-security ?
OPC UA answers
A broader view

See ANSSI 2022 Cyber threat panorama

1. Same level of hacking but different distribution
    1. Less attacks on public operators
    2. Increase on less protected operators
2. Constant Improvement of malicious actors capabilities
3. Increase in compromise attempts via peripheral equipment
4. A difficult environment (geopolitics and major events)
5. Exploitation of unpatched vulnerabilities still very common

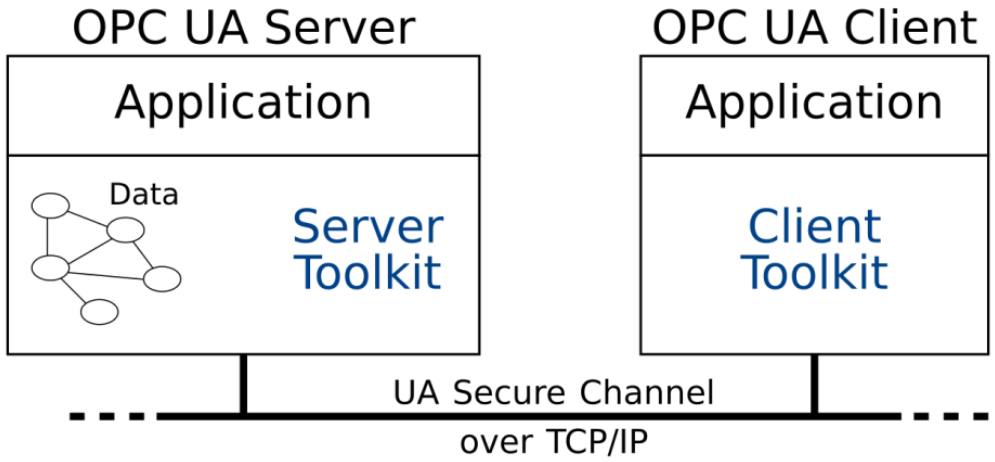
Source ANSSI: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

OPC UA answers

OPC UA Security objectives

Main concerns

- Confidentiality (encryption)
- Integrity (signature)
- Authentication (signature)
- Authorizations
- Audit



Security objectives

Security modes

- None
- Signature
- Signature and encryption

Policy \ Mode	None	Sign	SignAndEncrypt
None	✓		
Basic256		✓	✓
Basic256Sha256 [B]		✓	✓
Aes128Sha256RsaOaep [A]		✓	✓
Aes256Sha256RsaPss		✓	✓
ECC-*		✓	✓

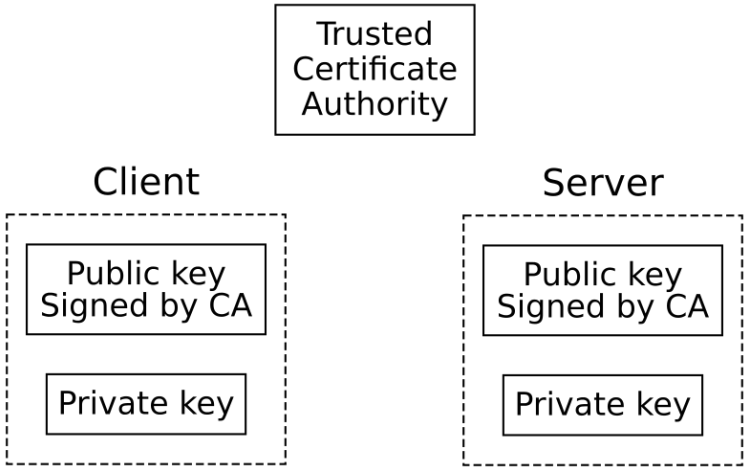
OPC UA Security Policies

- Security presets (algorithms, key lengths, renewal timeouts, ...)
- “None”: without security, always available
- “Basic256” / “Basic256Sha256” / “Aes128-…” / “Aes256-…”
  - OPN: asymmetric, RSA, always sign and encrypt
  - MSG: symmetric, AES-CBC
- ECC-*: elliptic curve algorithms => stick to RSA algorithms

Security: Public Key Infrastructure (PKI)

Authentication based on a Trusted Third Party

- Certificate Authority (CA) is trusted by all parties
- CA issues signed certificates for servers and clients
- Clients will verify that server's certificate is signed
- Servers will verify that client's certificate is signed
- Maintain a revocation list



OPC UA Security Configuration

PKI: certificate revocation list (CRL)

- Certificate signature expires

- But what if the private key has been compromised before expiration?
- → Certificate Revocation List of the Certificate Authority
- Equals a blacklist

- Must be configured beforehand
- Must be maintained by a side channel

- Must be present for each root and link, trusted or untrusted

Security objectives

Layers

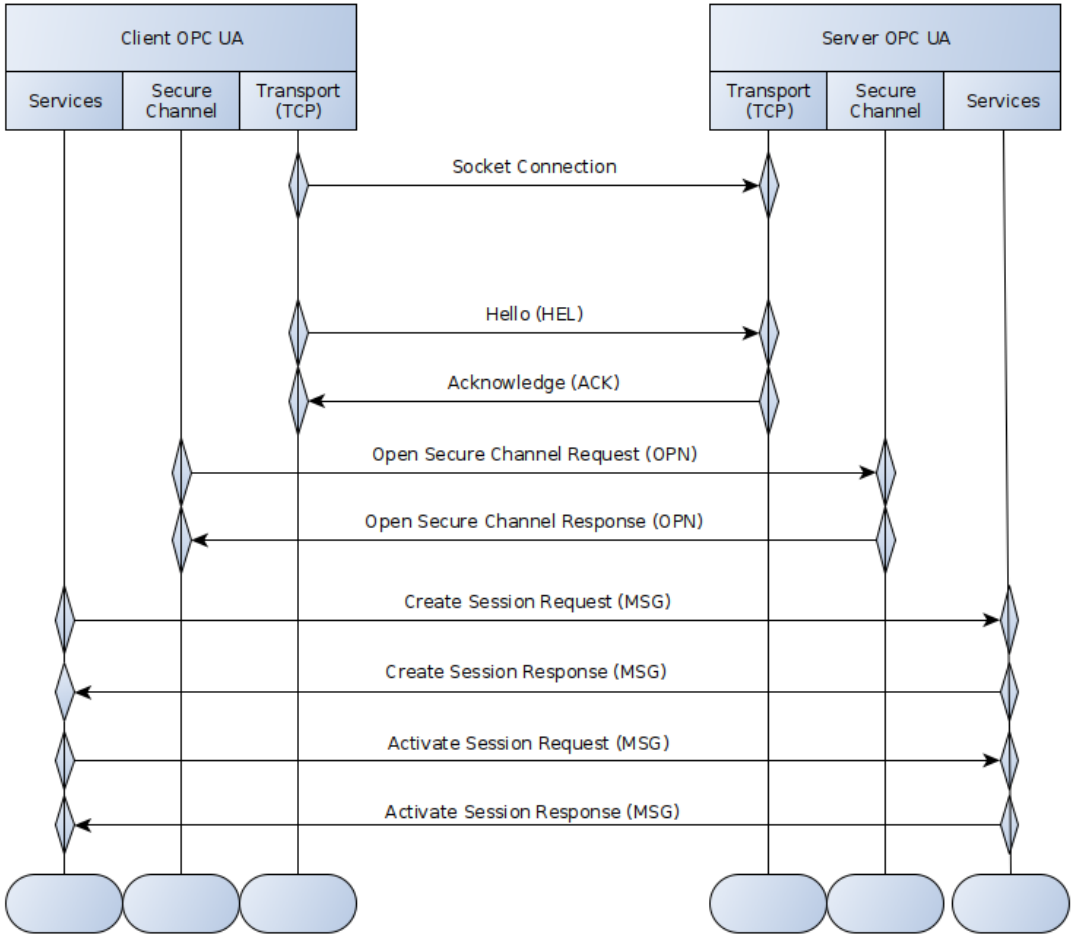
- OPC UA TCP: none
- Secure Conversation: confidentiality, integrity, “machine authentication” or “application authentication”
- Session: same application authentication as Secure Conversation
- Activate user on session: user authentication and authorization (e.g. UserAccessLevel)

Overview

- Asymmetric: OPN, [CreateSession], [ActivateSession]
- Symmetric: rest of the MSG chunks

Connection establishment overview

- Why cyber-security ?
- OPC UA answers
- A broader view



Security: Address Space

User authorizations

- Exposed in the address space
  - AccessLevel and UserAccessLevel (Read and Write services / Value attribute)
  - WriteMask and UserWriteMask attributes (Write service / other attributes)
  - Executable and UserExecutable (Call service)

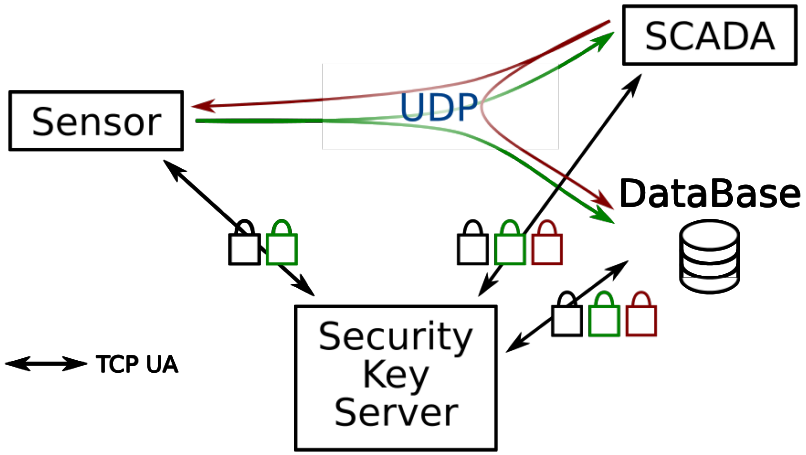
- Other services *might* implement user restrictions (see OPC UA roles)
  - E.g. Browse could return BadInvalidUser

Security: PubSub

Different transport layers

- Message layer (UADP or JSON, define headers and encoding)
- Transport layer (UDP multicast, Raw Ethernet, MQTT, AMQP)
- Security available on both levels (UADP, MQTT or AMQP)

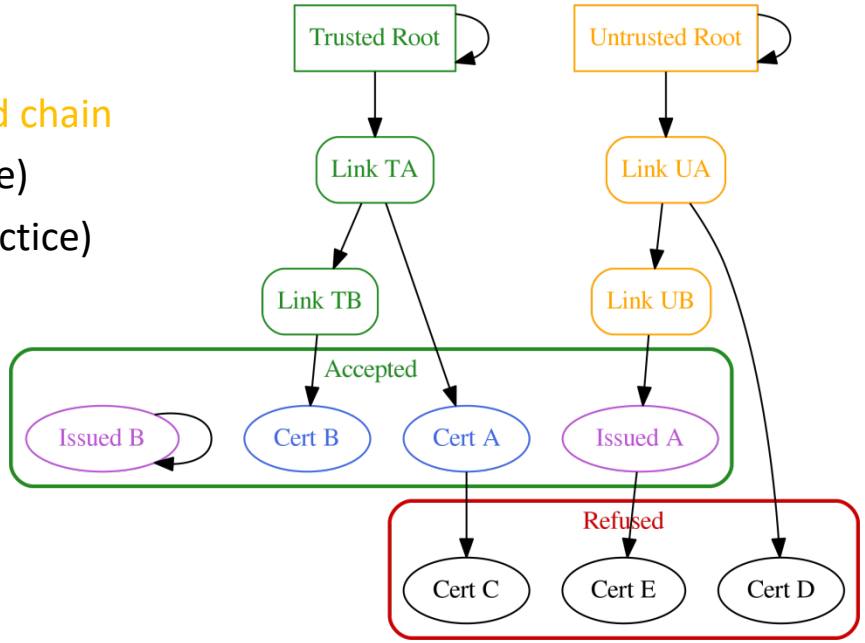
- UADP security: symmetric encryption, AES CTR 128 or 256, SKS



OPC UA Security: PKI Sum up

Accepted

- Signed by trusted chain
- Issued and signed by untrusted chain
- Self-signed issued (bad practice)
- Trusted links or Roots (bad practice)



Refused

- Link or Root misses CRL
- Signed by a link that is not trusted
- Signed by an issued certificate

Notes

- Also refused if invalid dates/signature/key length/signing algorithms
- Self-signed issued certificate: cannot be revoked

OPC UA Security Configuration

Certificate Manager, part of a Global Discovery Server (GDS)

- Certificate Manager eases security management
- Functionalities
  - Renewal: ask for a new Key and/or Certificate
  - Trust List Update: update the trusted and untrusted certificates
    - Should only fetch missing links
  - Revocation: update revocation lists
    - Very useful
- GDS are out of Nano/Micro/Embedded/Standard Server certification levels
- Initial provisioning: see part 21 – Device Onbording since revision 1.05

Roles mechanism

Introduced in revision 1.04

Basic principles

- An OPC UA session is associated to one or several roles
- A role is determined by:
  - User identity (name, X509, token, …) or group (anonymous, authenticated)
  - Application identity (Application URI part of X509 certificates)
  - Endpoint: URL, security mode & policy
- Permissions associated to roles include services:

  Browse, Read, Write, Subscription, Call, Node Management
- Different types of data are identified: « live », « configuration », « security », …

Well Known Roles

- Why cyber-security ?
- OPC UA answers
- A broader view

BrowseName	Suggested Permissions
Anonymous	The *Role* has very limited access for use when a *Session* has anonymous credentials.
AuthenticatedUser	The *Role* has limited access for use when a *Session* has valid non-anonymous credentials but has not been explicitly granted access to a *Role*.
Observer	The *Role* is allowed to browse, read live data, read historical data/events or subscribe to data/events.
Operator	The *Role* is allowed to browse, read live data, read historical data/events or subscribe to data/events. In addition, the *Session* is allowed to write some live data and call some *Methods*.
Engineer	The *Role* is allowed to browse, read/write configuration data, read historical data/events, call Methods or subscribe to data/events.
Supervisor	The *Role* is allowed to browse, read live data, read historical data/events, call Methods or subscribe to data/events.
ConfigureAdmin	The *Role* is allowed to change the non-security related configuration settings.
SecurityAdmin	The *Role* is allowed to change security related settings.

GIMELEC

OPC FOUNDATION

Auditing

OPC UA Auditing is based on two mechanisms

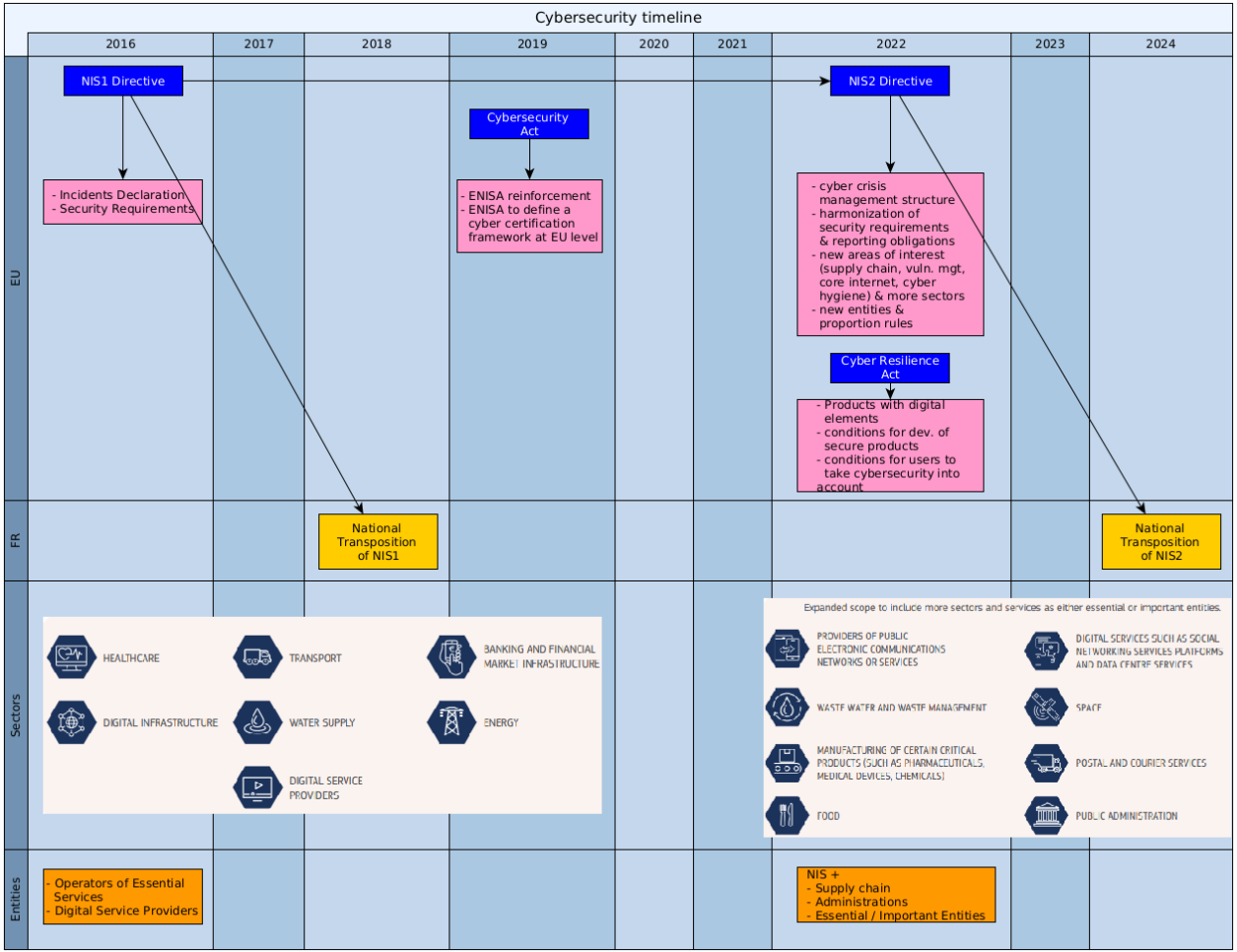
- Audit logs to provide traceability between clients requests and server responses. They shall be protected against unauthorized tampering.

- Capability to generate AuditEvents. Can be reported by:
  - Event Subscriptions,
  - PubSub,
  - Non OPC UA mechanism (Syslog)

A broader view

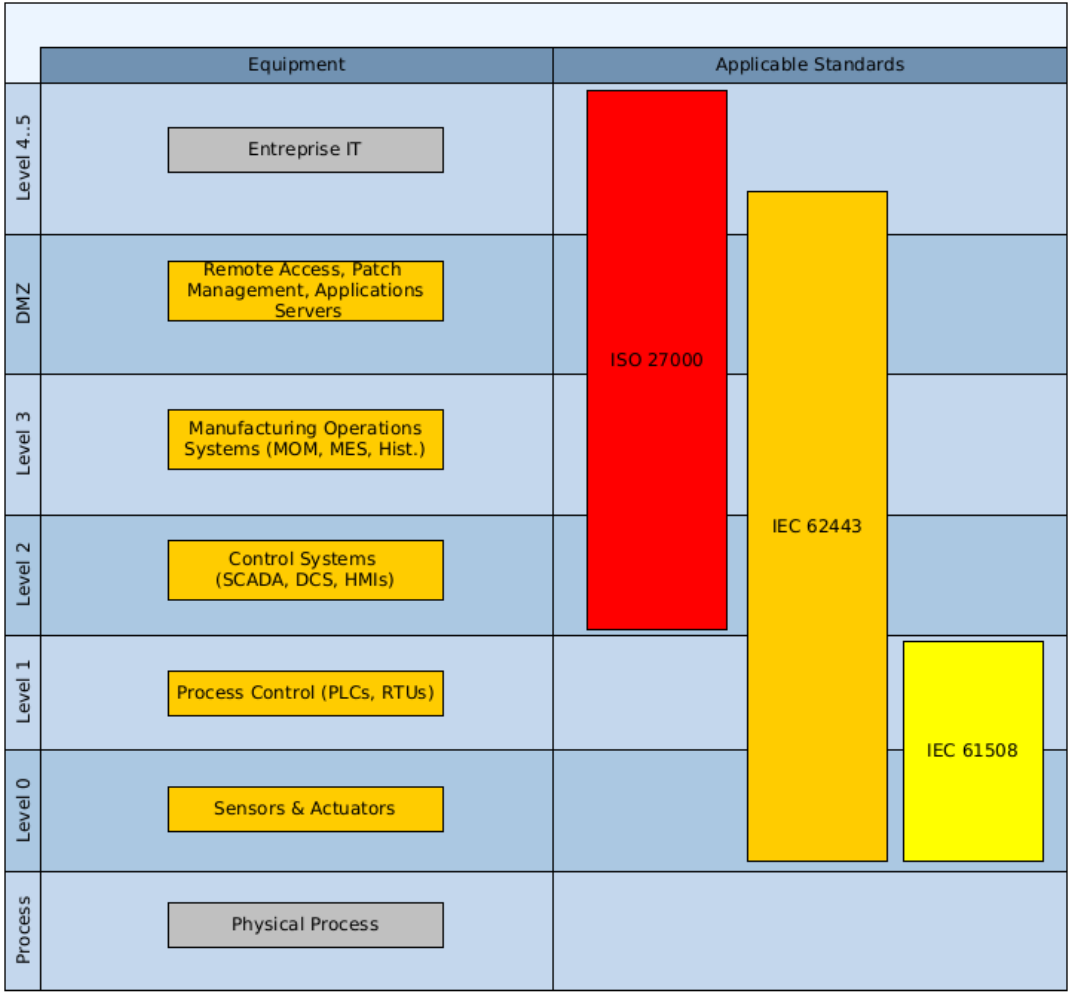
Regulatory environment and standards (EU)

- Why cyber-security ?
- OPC UA answers
- A broader view



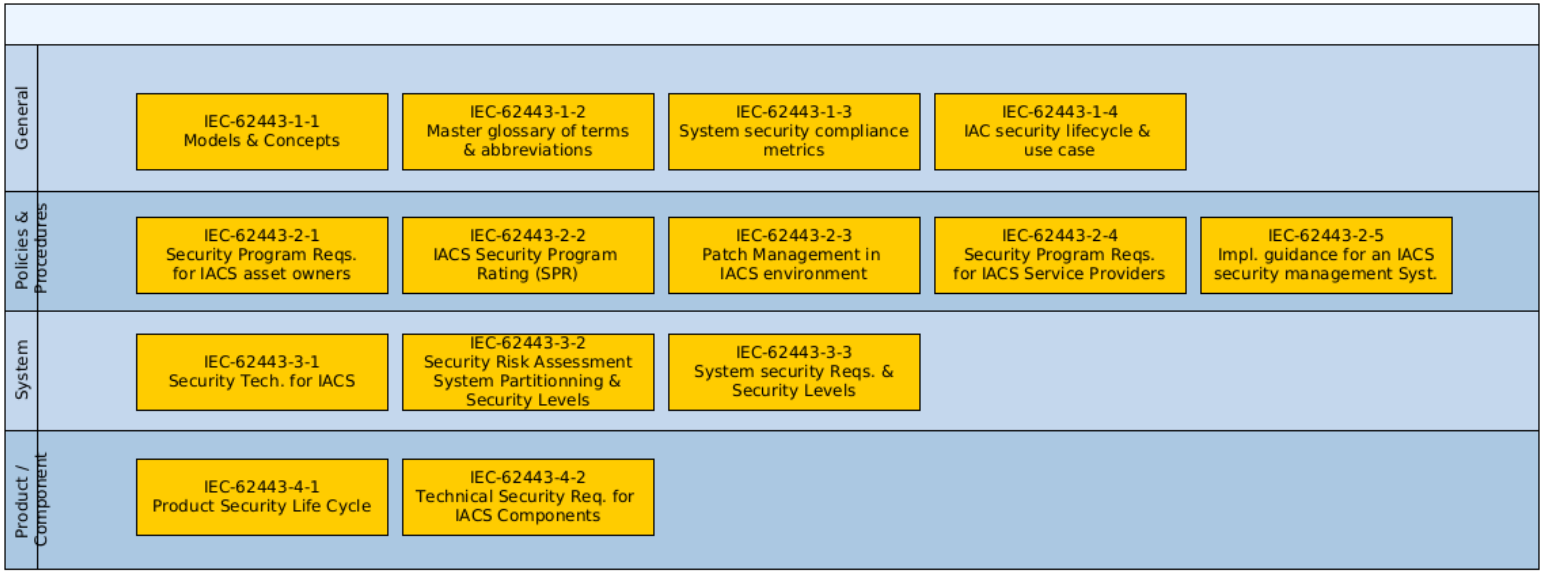
OPC UA vs IEC 62443

- Why cyber-security ?
- OPC UA answers
- A broader view



OPC UA vs IEC 62443-4-2

IEC 62443 Parts



OPC UA to IEC62443 mapping in Part 2 rev 1.05 Table A.2

Targeted level: SL-2

OPC UA vs IEC 62443-4-2

- Why cyber-security ?
- OPC UA answers
- A broader view

IEC 62443-4-2	nof reqs SL-1	nof reqs SL-2	OPC UA part 2	OPC UA part 4	OPC UA part 5	OPC UA part 6	OPC UA part 7	OPC UA part 12	OPC UA part 14	N/A OPC UA
FR1 Contrôle d'identification & d'authentification	8	12	6	10	0	5	15	1	1	CR 1.3: Account management CR 1.6: Wireless access management CR 1.7: Strength of password based authentication CR 1.10: Authenticator feedback CR 1.11: Unsuccessful login attempts CR 1.12: System use notification
FR 2 – Contrôle d'utilisation	8	9	17	19	4	4	8	0	0	CR 2.2: Wireless use control CR 2.5: Session lock CR 2.6: Remote session termination CR 2.9: Audit storage capacity CR 2.10: Response to audit processing failures
FR 3 – Intégrité du système	6	8	7	10	1	12	8	0	0	CR 3.4 RE (1): Authenticity of software and information CR 3.5: Input validation CR 3.6: Deterministic output CR 3.9: Protection of audit information
FR 4 – Confidentialité des données	2	3	12	2	0	7	9	0	0	CR 4.2: Information persistence
FR 5 – Transfert de données limité	1	1	2	3	0	0	2	0	0	
FR 6 – Réponse appropriée aux événements	1	2	0	0	0	6	0	0	0	CR 6.1: Audit log accessibility
FR 7 – Disponibilité des ressources	6	7	10	3	0	0	3	0	0	CR 7.3: Control system backup CR 7.4: Control system recovery and Reconstitution CR 7.6: Network and security configuration settings CR 7.7: Least functionality CR 7.8: Control system component inventory

BSI Analysis

First Analysis in 2016. Second analysis in 2022 (publication)

- Good points:
  - Good protection level against threats identified in Part 2 with Signed or SignedAndEncrypt security modes
  - Almost all points identified in first analysis have been treated by the Cybersecurity Working Group

- Point of improvement:
  - Complexity

"An overview of all cyber security-relevant concepts in OPC UA should be obtained by reading at least Parts 2, 3, 4, 5, 6, 7, 12 and 14."

  - Slow deployment without constraint:

"many of the security recommendations and requirements of the specification are not implemented in practice."

Note: PubSub is not part of the evaluation

Existing CVEs

Common Vulnerabilities and Exposures

- 60 for “opc ua”
- 10 for “opcua”

There are **60** CVE Records that match your search.

Name	Description
CVE-2023-32787	The OPC UA Legacy Java Stack before 6f176f2 enables an attacker to block OPC UA server applications via uncontrolled resource consumption so that they can no longer serve client applications.
CVE-2022-39823	An issue was discovered in Softing OPC UA C++ SDK 5.66 through 6.x before 6.10. An OPC/UA browse request exceeding the server limit on continuation points may cause a use-after-free error
CVE-2022-37453	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types.
CVE-2022-37013	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation OPC UA C++ Demo Server 1.7.6-537 [with vendor rollup]. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of certificates. A crafted certificate can force the server into an infinite loop. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-17203.
CVE-2022-37012	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation OPC UA C++ Demo Server 1.7.6-537. Authentication is not required to exploit this vulnerability. The specific flaw exis … erage this vulnerability to create a denial-of-servic…
CVE-2022-34765	A CWE-73: Exte… Communication … 80 advanced RTU
CVE-2022-34764	A CWE-119: Imp… (BMENOR2200H … U Communication Module
CVE-2022-34763	A CWE-345: Insu… Communication … ducts: X80 advanced RTU
CVE-2022-34762	A CWE-22: Impr… Affected Product … the firmware image path.
CVE-2022-34761	A CWE-476: NU… (V2.01 and later) … on Module (BMENOR2200H)
CVE-2022-34760	A CWE-835: Loo… Communication … 80 advanced RTU

CVE-ID

CVE-2022-37012 — Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation OPC UA C++ Demo Server 1.7.6-537. Authentication is not required to exploit this vulnerability. The specific flaw exists within the OpcUa_SecureListener_ProcessSessionCallRequest method. A crafted OPC UA message can force the server to incorrectly update a reference count. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-16927.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://documentation.unified-automation.com/uasdkcpp/1.7.7/CHANGELOG.txt
- URL:https://documentation.unified-automation.com/uasdkcpp/1.7.7/CHANGELOG.txt
- MISC:https://www.zerodayinitiative.com/advisories/ZDI-22-1030/
- URL:https://www.zerodayinitiative.com/advisories/ZDI-22-1030/

Assigning CNA

Zero Day Initiative

Date Record Created

20220728 — Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20220728)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=opc+UA

Hacking contests on OPC UA

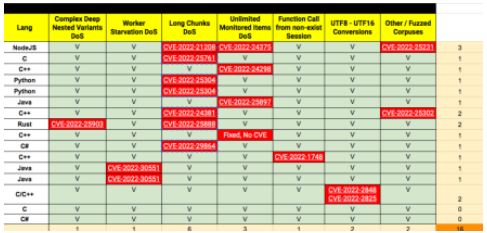
PWN2OWN ICS

- Specific OPC UA category
- 20 zero-day vulnerabilities disclosed every year

2023 PWN2OWN ICS Winner: Claroty Team 82 research Team (https://claroty.com/team82)

Active community around OPC UA Cybersecurity. Can be contacted using Slack

Lot of vulnerabilities found thanks to their Network Fuzzer. Available on GitHub (https://github.com/claroty/opcua_network_fuzzer).



Lang	Complex Deep Nested Variants DoS	Worker Starvation DoS	Long Chunks DoS	Unlimited Monitored Items DoS	Function Call from non-exist Session	UTF8 - UTF16 Conversions	Other / Fuzzed Corpuses	
NodeJS	V	V	CVE-2022-21208	CVE-2022-24375	V	V	CVE-2022-25231	3
C	V	V	CVE-2022-25761	V	V	V	V	1
C++	V	V	V	CVE-2022-24298	V	V	V	1
Python	V	V	CVE-2022-25304	V	V	V	V	1
Python	V	V	CVE-2022-25304	V	V	V	V	1
Java	V	V	V	CVE-2022-25897	V	V	V	1
C++	V	V	CVE-2022-24381	V	V	V	CVE-2022-25302	2
Rust	CVE-2022-25903	V	CVE-2022-25883	V	V	V	V	2
C++	V	V	V	Fixed, No CVE	V	V	V	1
C#	V	V	CVE-2022-25864	V	V	V	V	1
C++	V	V	V	V	CVE-2022-1748	V	V	1
Java	V	CVE-2022-30581	V	V	V	V	V	1
Java	V	CVE-2022-30581	V	V	V	V	V	1
C/C++	V	V	V	V	V	CVE-2022-2848 CVE-2022-2825	V	2
C	V	V	V	V	V	V	V	0
C#	V	V	V	V	V	V	V	0
	1	1	6	3	1	2	2	16

Source:
https://msrndcdn360.blob.core.windows.net/bluehat/bluehatil/2023/docs/DAY2/VeraSharon_BHIL2023.pdf
https://www.zerodayinitiative.com/blog/2023/2/16/pwn2own-miami-2023-day-three-results

Conclusion

Deployment of Cybersecurity mechanism is slow due to remaining myths

However, threat level is still high

OPC UA mechanisms allow to meet Cybersecurity requirements

Compliance to IEC 62443 standard for communication OK, not magic for application

Questions ?

Contacts

systerel
Solutions temps réel sécurisées

Jérémie BARJHOUX
Business Developer

+33 7 80 90 50 41
barjhoux@systerel.fr

systerel
Solutions temps réel sécurisées

Vincent LACROIX
S2OPC Product Owner

+33 4 42 90 41 21
lacroix@systerel.fr

GIMELEC

OPC FOUNDATION