EtherCAT Technology Group

Cyber Security Requirements on EtherCAT Systems

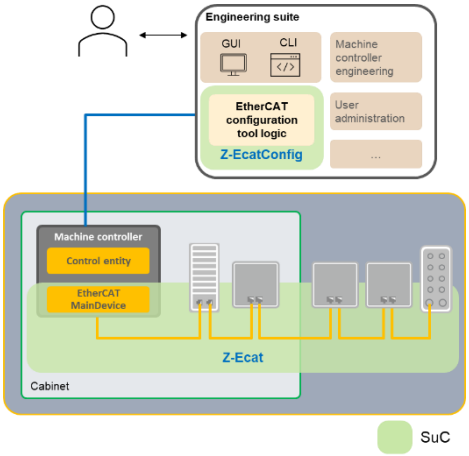
Explanatory Notes on the Certification of EtherCAT Cybersecurity Capabilities

EtherCAT® Technology Group

Cyber Security Requirements on EtherCAT Systems

The UL Solutions certificates [1] confirm the cybersecurity capabilities of EtherCAT technology in three different scenarios, each with a different risk profile. The built-in capabilities of EtherCAT were assessed based on the System Requirements defined in IEC 62443-3-3.

The System under Consideration (SuC) for the three scenarios is a typical representative of an EtherCAT-based automation system: a machine unit using the EtherCAT Device Protocol consisting of a machine controller and several SubDevices, like drives and decentralized input and output modules. Some devices are located inside a control cabinet, while others are located outside.



System under Consideration (SuC)

For the certificates provided by UL Solutions, all 103 system requirements (SR) from the IEC 62443-3-3 standard were evaluated and assessed to determine whether they apply to the SuC or not ("N/A"). For all applicable requirements, it is examined in detail whether and how the EtherCAT system meets them. For SRs classified as "N/A," further reasoning is provided and assessed if the SR must be met by the machine controller entity.

Three "Blueprint Scenarios" were used to evaluate different use cases of EtherCAT in industrial automation, to which different system requirements apply according to the risk-based approach of the standard. The assumed strength of the attacker is at the upper end of the range and may be rated differently in real-world applications.

Blueprint Scenario 1 represents a machine unit in a typical factory environment, such as a machine unit in a production hall. It assumes an attacker with the skills and motivation corresponding to Security Level SL 2 of IEC 62443-3-3. Without any modifications or extensions to the technology, EtherCAT meets all applicable requirements for this scenario.

Blueprint Scenario 2 depicts a similar plant with less restrictive access control and an attacker with a strength of up to SL 3. According to the assumed threat scenario, confidentiality of the data is not required. The built-in capabilities of EtherCAT, along with a few enhanced software features on the MainDevice, meet the applicable requirements, the SubDevices remain unchanged.

Blueprint Scenario 3 is an application with enhanced security requirements focused on the confidentiality of the system: cryptographic measures, including encryption, are required and attacks up to SL 3 strength are considered. In addition to the built-in capabilities of EtherCAT some extended features for the authentication and data encryption are used to fulfill all applicable requirements.

Manufacturers and users of EtherCAT systems can map their security requirements – determined through the respective Threat Analysis and Risk Assessment (TARA) for the use case in question – to the evaluated scenarios. Cybersecurity certification of the EtherCAT system according to the scenarios described does not require certification of the EtherCAT devices used.

Summarized assessment results

The following test case verdicts are used for the assessment:

- Pass: test object meets the requirement as the declared
- N/A: test case was evaluated and does not apply to the test object due to technical reasons, e.g. no wireless, or falls into one of the following sub-categories
  - Outside compensating countermeasures apply
  - n/i not implemented due to risk assessment
- N/E: test case outside the scope of submittal
- Fail: test object does not meet the requirement

The following tables (Table 1 to Table 8) summarize the results of the test report for the main zone **Z-Ecat**.

Table 1: CCSSC – Common control system security constraints, Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
CCSSC 4.2	Support of essential functions	Pass	Pass	Pass
CCSSC 4.3	Compensating countermeasures	N/A	N/A	N/A
CCSSC 4.4	Least privilege	N/A	N/A	N/A

Table 2: FR 1 – Identification and authentication control (IAC), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 1.1	Human user identification and authentication	N/A	N/A	N/A
SR 1.1 RE1	Unique identification and authentication	N/A	N/A	N/A
SR 1.1 RE2	Multifactor authentication for untrusted networks	N/A	N/A	N/A
SR 1.1 RE3	Multifactor authentication for all networks	N/A	N/A	N/A
SR 1.2	Software process and device identification and authentication	Pass	Pass	Pass
SR 1.2 RE1	Unique identification and authentication	Pass	Pass	Pass
SR 1.3	Account management	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 1.3 RE1	Unified account management	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 1.4	Identifier management	N/A	N/A	N/A
SR 1.5	Authenticator management	N/A (n/i)	N/A (n/i)	Pass
SR 1.5 RE1	Hardware security for software process identity credentials	N/A (n/i)	N/A (n/i)	Pass
SR 1.6	Wireless access management	N/A	N/A	N/A
SR 1.6 RE1	Unique identification and authentication	N/A	N/A	N/A
SR 1.7	Strength of password-based authentication	N/A	N/A	N/A
SR 1.7 RE1	Password generation and lifetime restrictions for human users	N/A	N/A	N/A
SR 1.7 RE2	Password lifetime restrictions for all users	N/A	N/A	N/A
SR 1.8	Public key infrastructure (PKI) certificates	N/A	N/A	N/A
SR 1.9	Strength of public key authentication	N/A	N/A	N/A
SR 1.9 RE1	Hardware security for public key authentication	N/A	N/A	N/A
SR 1.10	Authenticator feedback	N/A	N/A	N/A
SR 1.11	Unsuccessful login attempts	N/A (n/i)	N/A (n/i)	Pass
SR 1.12	System use notification	N/A	N/A	N/A

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 1.13	Access via untrusted networks	Pass	Pass	Pass
SR 1.13 RE1	Explicit access request approval	N/A	N/A	N/A

Table 3: FR 2 – Use control (UC), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 2.1	Authorization enforcement	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.1 RE1	Authorization enforcement for all users	Pass	Pass	Pass
SR 2.1 RE2	Permission mapping to roles	Pass	Pass	Pass
SR 2.1 RE3	Supervisor override	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.1 RE4	Dual approval	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.2	Wireless use control	N/A	N/A	N/A
SR 2.2 RE1	Identify and report unauthorized wireless devices	N/A	N/A	N/A
SR 2.3	Use control for portable and mobile devices	N/A	N/A	N/A
SR 2.3 RE1	Enforcement of security status of portable and mobile devices	N/A	N/A	N/A
SR 2.4	Mobile code	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.4 RE1	Mobile code integrity check	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.5	Session lock	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.6	Remote session termination	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.7	Concurrent session control	Pass	Pass	Pass
SR 2.8	Auditable events	Pass	Pass	Pass
SR 2.8 RE1	Centrally managed, system-wide audit trail	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.9	Audit storage capacity	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.9 RE1	Warn when audit record storage capacity threshold reached	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.10	Response to audit processing failures	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.11	Timestamps	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.11 RE1	Internal time synchronization	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.11 RE2	Protection of time source integrity	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.12	Non-repudiation	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 2.12 RE1	Non-repudiation for all users	Pass	Pass	Pass

Table 4: FR 3 – System Integrity (SI), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 3.1	Communication integrity	Pass	Pass	Pass
SR 3.1 RE1	Cryptographic integrity protection	N/A (n/i)	N/A (n/i)	Pass
SR 3.2	Malicious code protection	Pass	Pass	Pass
SR 3.2 RE1	Malicious code protection on entry and exit points	Pass	Pass	Pass
SR 3.2 RE2	Central management and reporting for malicious code protection	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 3.3	Security functionality verification	Pass	Pass	Pass
SR 3.3 RE1	Automated mechanisms for security functionality verification	Pass	Pass	Pass
SR 3.3 RE2	Security functionality verification during normal operation	Pass	Pass	Pass
SR 3.4	Software and information integrity	Pass	Pass	Pass
SR 3.4 RE1	Automated notification about integrity violations	N/A (Outside)	N/A (Outside)	N/A (Outside)

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 3.5	Input validation	Pass	Pass	Pass
SR 3.6	Deterministic output	Pass	Pass	Pass
SR 3.7	Error handling	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 3.8	Session integrity	Pass	Pass	Pass
SR 3.8 RE1	Invalidation of session IDs after session termination	N/A	N/A	N/A
SR 3.8 RE2	Unique session ID generation	N/A	N/A	N/A
SR 3.8 RE3	Randomness of session IDs	N/A	N/A	N/A
SR 3.9	Protection of audit information	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 3.9 RE1	Audit Records on write-once media	N/A (Outside)	N/A (Outside)	N/A (Outside)

Table 5: FR 4 – Data Confidentiality (DC), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR4.1	Information confidentiality	Pass	Pass	Pass
SR4.1 RE1	Protection of confidentiality at rest or in transit via untrusted networks	N/A	N/A	N/A
SR4.1 RE2	Protection of confidentiality across zone boundaries	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR4.2	Information persistence	Pass	Pass	Pass
SR4.2 RE1	Purging of shared memory resources	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR4.3	Use of cryptography	N/A (n/i)	N/A (n/i)	Pass

Table 6: FR 5 – Restricted data flow (RDF), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR5.1	Network segmentation	N/A	N/A	N/A
SR5.1 RE1	Physical network segmentation	N/A	N/A	N/A
SR5.1 RE2	Independence from non-control system networks	N/A	N/A	N/A
SR5.1 RE3	Logical and physical isolation of critical networks	N/A	N/A	N/A
SR5.2	Zone boundary protection	Pass	Pass	Pass
SR5.2 RE1	Deny by default, allow by exception	Pass	Pass	Pass
SR5.2 RE2	Island mode	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR5.2 RE3	Fail close	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR5.3	General purpose person-to-person communication restrictions	N/A	N/A	N/A
SR5.3 RE1	Prohibit all general purpose person-to-person communications	N/A	N/A	N/A
SR5.4	Application partitioning	Pass	Pass	Pass

Table 7: FR 6 – Timely response to events (TRE), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 6.1	Audit log accessibility	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 6.1 RE1	Programmatic access to audit logs	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 6.2	Continuous monitoring	Pass	Pass	Pass

Table 8: FR 7 – Resource availability (RA), Z-Ecat

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 7.1	Denial of service protection	Pass	Pass	Pass
SR 7.1 RE1	Manage communication loads	Pass	Pass	Pass
SR 7.1 RE2	Limit DoS effects to other systems or networks	Pass	Pass	Pass
SR 7.2	Resource management	Pass	Pass	Pass
SR 7.3	Control system backup	Pass	Pass	Pass
SR 7.3 RE1	Backup verification	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 7.3 RE2	Backup automation	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 7.4	Control system recovery and reconstitution	Pass	Pass	Pass
SR 7.5	Emergency power	Pass	Pass	Pass
SR 7.6	Network and security configuration settings	Pass	Pass	Pass
SR 7.6 RE1	Machine-readable reporting of current security settings	N/A (Outside)	N/A (Outside)	N/A (Outside)
SR 7.7	Least Functionality	Pass	Pass	Pass
SR 7.8	Control System Component Inventory	Pass	Pass	Pass

The applicable requirements for **Z-EcatConfig** are listed in Table 9. All other SRs are not applicable for this zone.

*Table 9: Summary of applicable requirements for **Z-EcatConfig***

ID	Requirement	Scenario 1	Scenario 2	Scenario 3
SR 1.8	Public key infrastructure (PKI) certificates	N/A (n/i)	Pass	Pass
SR 1.9	Strength of public key authentication	N/A (n/i)	Pass	Pass
SR 3.2	Malicious code protection	N/A (Outside)	Pass	Pass
SR 3.2 RE1	Malicious code protection on entry and exit points	N/A (Outside)	Pass	Pass
SR 3.3	Security functionality verification	Pass	Pass	Pass
SR 3.3 RE1	Automated mechanisms for security functionality verification	Pass	Pass	Pass
SR 3.3 RE2	Security functionality verification during normal operation	Pass	Pass	Pass
SR 3.5	Input validation	Pass	Pass	Pass
SR 3.6	Deterministic output	Pass	Pass	Pass
SR 7.3	Control system backup	Pass	Pass	Pass
SR 7.6	Network and security configuration settings	Pass	Pass	Pass
SR 7.8	Control System Component Inventory	Pass	Pass	Pass

List of EtherCAT features used for Cyber Security

The features shown in Table 10 are to be implemented or applied in accordance with the results of the respective TARA.

Table 10: EtherCAT Features used for Cyber Security

General EtherCAT Features used to meet the requirements of Blueprint Scenario 1 without extensions to the technology
Functional Principle: Processing-on-the-fly
No IP traffic: only EtherType 0x88A4 is accepted by the EtherCAT SubDevice Controller (ESC)
EtherCAT frame allowed within UDP/IP frame – MainDevice blocks UDP port 0x88A4
ESC destroys all non-EtherCAT frames per default and by hardware
If Ethernet over EtherCAT (EoE) is supported, it is disabled in the MainDevice
A 32-bit Frame Check Sequence protects each EtherCAT frame
By hardware, ESC can only access data that is configured by the MainDevice
The MainDevice checks VPR(S) (Vendor ID, Product Code, Revision Number, Serial Number) of every SubDevice during start-up of the segment
The MainDevice checks the actual segment topology against the expected one during boot-up of the segment
The MainDevice checks the configured Explicit Identification Value
All unused EtherCAT ports are configured as “closed” by the MainDevice
For Hot-connect groups: the connection port(s) are opened manually, and the expected Explicit Device Identification-Value is checked before starting the hot-connect segment
Registers and startup-parameters are downloaded at every start-up and re-connect
The MainDevice checks the number of SubDevices in the segment with each cyclic frame
The MainDevice checks the AL-Status of the SubDevices
The EtherCAT MainDevice driver prevents unexpected injected frames
The MainDevice checks for lost frames
The MainDevice application checks the RX Error counters of SubDevices
The MainDevice application checks the Lost Link counters of SubDevices
The source of the ESI files that are used by the engineering tool are being checked
To protect the firmware file the SubDevice application checks its integrity before applying it
The SubDevice supports restoring the settings to default parameters
The MainDevice disables SubDevice-to-SubDevice mailbox communication
The MainDevice disables remote access via Mailbox Gateway, e.g., block UDP/TCP port 0x88A4
The MainDevice provides an interface to read the current security-related settings

Enhanced EtherCAT Features used to meet the requirements of Blueprint Scenario 2 with software extensions in the MainDevice only
The MainDevice reads the “Receive time”-register in the ESCs to detect intrusions by checking hardware propagation delay changes.
The MainDevice checks SubDevice parameter settings
The ESI file includes a certificate signed by the ETG Certificate Authority. The EtherCAT configuration tool verifies this certificate before the ESI file is used for configuration.
A unique identification information of the SubDevice is checked by the MainDevice (inventory check) during start-up of the segment
The firmware file includes a certificate that can be verified with information in the ESI file

Extended EtherCAT features used to meet the requirements of Blueprint Scenario 3 with software extensions only; no changes to the EtherCAT chips (ESC)
The MainDevice and SubDevice are paired with a symmetric key for authentication
Cryptographic integrity protection for data
Cryptographic confidentiality protection of data

List of System Requirements used in the Assessment

The EtherCAT features listed above, along with fundamental security features in the machine controller (such as access control, which is independent of the fieldbus in use), are used to meet the requirements of the use cases described in the three different scenarios. In the conformity statements, these are referred to as MDR (MainDevice Requirement) and SDR (SubDevice Requirement). They are detailed in Table 11 and Table 12:

Table 11: MainDevice Requirements [MDR]

MDR	MainDevice Requirement, depending on the use case	SL2	SL3	SR x.y
MDR01	To avoid UDP/IP-based EtherCAT traffic, the control application blocks UDP destination port 0x88A4	x	x	Multiple
MDR02	To avoid UDP/IP-based EtherCAT traffic, the IP forwarding to the EtherCAT segment port of the MainDevice remains disabled	x	x	Multiple
MDR03	If EoE-tunneled (IP) traffic shall be avoided the user does not enable EoE in the MainDevice or disables it after commissioning the system. The EoE feature in the MainDevice is disabled by default.	x	x	Multiple
MDR04	Configured Station Alias is not processed by FPxx commands. The MainDevice does not change the default configuration in the SubDevices “Ignore Station Alias”.	x	x	Multiple
MDR05	If cable swapping is considered an unacceptable risk (e.g., if the system is accessible and SubDevices of the same type (same VPR) are located next to each other in the topology), the MainDevice checks the Explicit Device ID of the SubDevices against the configured value. This is part of the user’s segment configuration. Note: The unnoticed swapping of sensor or motor cables is generally considered a higher risk.	x	x	Multiple
MDR06	EtherCAT ports of a SubDevice that are not used/have no link, i.e., are not connected to another SubDevice in the intended topology, shall be closed ("locked") by the MainDevice.	x	x	Multiple

MDR	MainDevice Requirement, depending on the use case	SL2	SL3	SR x.y
MDR07	To prevent a port in use from being used to connect (loop in) an unauthorized device to a running segment, all used ports in an EtherCAT segment are configured to 'Auto Close'. Then such an attempt first takes down the link on this port, which then leads to the port being closed. The port needs to be opened by the MainDevice.	x	x	Multiple
MDR08	The configuration of the MainDevice adds all relevant parameters to the startup command list to prevent parameters that were changed while the main device was powered off from taking effect.	x	x	Multiple
MDR09	The MainDevice ensures that a frame that was not sent by the MainDevice is not passed on to the operating system and that additional frames from the segment do not prevent the MainDevice from working as intended.	x	x	Multiple
MDR10	The MainDevice driver runs within a protected environment on the machine controller which ensures prevention, detection, reporting and mitigation of malicious code.	x	x	SR 3.2
MDR11	The EtherCAT MainDevice driver prevents other drivers (including other EtherCAT MainDevice drivers) from accessing the EtherCAT port through which it communicates with the EtherCAT segment.	x	x	Multiple
MDR12	The control system generates audit records relevant to security, which include alerts generated and provided by the EtherCAT segment, showing events such as the disconnection of segment parts, inconsistent data exchange, loss of OP state of one or more SubDevices. The interface to record these events includes a timestamp in the control application. The control application has or integrates into a centrally managed system-wide audit trail.	x	x	SR 2.8 SR 2.8 RE1
MDR13	The EtherCAT configuration tool supports the security settings, whereas the actual settings are a result of the risk analysis for the real application / machine unit.	x	x	SR 6.6
MDR14	The EtherCAT configuration tool or the MainDevice object dictionary provides an API or supports a file export of security-related settings.	x	x	SR 6.6
MDR15	The control system prohibits and/or restricts the use of unnecessary functions, ports, protocols and/or services.	x	x	SR 7.7
MDR16	The MainDevice verifies that the frame sent to the EtherCAT segment returns via the expected port within the expected time, whereas the minimum expected time is determined by the propagation delay in the segment, and the maximum expected time depends on the use case requirements.	x	x	Multiple
MDR17	The MainDevice increments a counter in the datagram header ("index" field), and checks this counter to detect - lost frames - duplicate frames - wrong frames, not matching the expected counter value	x	x	Multiple
MDR18	The control application checks the RX Error Counters of the SubDevices to determine irregularities.	x	x	Multiple
MDR19	The control application checks the Lost Link Counters of the SubDevices to determine irregularities.	x	x	Multiple
MDR20	The MainDevice driver does not forward mailbox requests with an unequal 0 address to prevent SubDevice-to-SubDevice mailbox communication.	x	x	Multiple
MDR21	If remote access via Mailbox Gateway is to be avoided the user does not enable the functionality in the MainDevice (with this feature being disabled by default).	x	x	Multiple
MDR22	The control application blocks TCP destination port 0x88A4 to prevent TCP/IP-based Mailbox Gateway communication.	x	x	Multiple

MDR	MainDevice Requirement, depending on the use case	SL2	SL3	SR x.y
MDR23	The control application blocks UDP destination port 0x88A4 to prevent UDP/IP-based EtherCAT traffic.	x	x	Multiple
MDR24	The MainDevice captures and compares the send/receive time of the frames to detect an intrusion between the MainDevice and the first SubDevice. Note: Ethernet controllers (NIC) can have hardware support for capturing a timestamp on the EtherCAT port.	-	x	Multiple
MDR25	The MainDevice cyclically reads the current parameter set and compares it with the expected values to detect any changes to the parameters in the SubDevices initiated from outside the system.	-	x	Multiple
MDR26	According to MDR25 the MainDevice supports user defined lists of parameters that need to be protected and checked against changes.	-	x	Multiple
MDR27	The EtherCAT configuration tool reports malicious code or provides an interface that supports this functionality.	-	x	SR 3.2
MDR28	The MainDevice and the SubDevice or their applications protect the relevant authenticators via hardware mechanisms.	-	x	SR 1.5 RE1

Table 12: SubDevice Requirements [SDR]

SDR	SubDevice Requirement	SL2	SL3	SR x.y
SDR01	SubDevices with an application based on EoE fulfill the security requirements for the system.	x	x	Multiple
SDR02	At least one of the Explicit Device Identification mechanisms is supported by the SubDevice.	x	x	Multiple
SDR03	The upload of the firmware is prevented by the SubDevice (vendor-specific).	x	x	Multiple
SDR04	The MainDevice and the SubDevice or their applications protect the relevant authenticators via hardware mechanisms.		x	SR 1.5 RE1

References:

[1] UL Solutions: 3 Certificates IEC 62443-3-3 and Technical Reports TRF:
Solution Application of Capabilities Assessment of EtherCAT Technology. issued by UL Solutions (Demko) Denmark, IECEE Certification Body: DK-177530-UL/DK-178394-UL/DK-178399-UL. IECEE CBTL (testing lab): UL Solutions Northbrook, IL, USA.