

Omni

4189341458-A

iE 250 | iE 250 Marine | iE 250 PLC | iE 350 | iE 350 Marine | iE 350 PLC | iE 650 PLC

Cybersecurity guidelines



1. About the Cybersecurity guidelines

1.1 Intended users of the Cybersecurity guidelines.....	4
1.2 About Cybersecurity.....	4
1.3 Applicable products and software.....	4
1.4 Legal information.....	4

2. Cybersecurity framework

2.1 DEIF Cybersecurity principles.....	6
2.2 Applicable standards.....	7
2.2.1 IEC 62443.....	7
2.2.2 IACS URE27.....	7
2.2.3 EU Cyber Resilience Act (CRA).....	8
2.3 Roles & responsibilities.....	8
2.3.1 About responsibilities.....	8
2.3.2 Product supplier (DEIF).....	8
2.3.3 System integrator.....	9
2.3.4 Asset owner (Operator).....	9

3. Security architecture and zones

3.1 Security zoning model.....	11
3.2 Typical security zones in an iE x50 system.....	11
3.3 Network architecture and topologies.....	13
3.3.1 Architecture principles.....	13
3.3.2 Diagrams for compliance and audits.....	13
3.3.3 IE 250.....	14
3.3.4 IE 350.....	14
3.3.5 IE 650.....	14

4. Hardening and configuration

4.1 Purpose of device hardening.....	15
4.2 Secure configuration baselines.....	15
4.3 Network exposure reduction.....	15
4.3.1 Network configuration.....	16
4.4 Physical protection measures.....	16
4.5 Logging and monitoring hardening.....	17
4.6 Hardening for Untrusted network scenarios.....	17

5. User and access management

5.1 About permissions.....	18
5.2 Roles and Users.....	18
5.2.1 Role settings.....	18
5.2.2 User settings.....	19
5.2.3 Default user.....	20
5.3 Password strength verification.....	20

6. Vulnerability management

6.1 Monitoring and on-going security.....	21
6.1.1 About activity logs.....	21
6.1.1.1 Event log.....	21
6.1.1.2 System log.....	21
6.1.2 Backup procedures.....	22
6.2 Security advisories.....	23

6.3 Incident response & recovery plan.....23

6.3.1 Report vulnerability..... 23

6.3.2 System recovery and restore..... 24

PRELIMINARY

1. About the Cybersecurity guidelines

1.1 Intended users of the Cybersecurity guidelines

The Cybersecurity guidelines are intended for **System integrators** and **Asset owners (Operators)** who want to secure their DEIF controllers in accordance with the cybersecurity standard.

1.2 About Cybersecurity

This document defines cybersecurity requirements based on IEC 62443 and IACS UR E27, covering secure development, system hardening, access control, network segmentation, and vulnerability management.

These requirements also support alignment with the **EU Cyber Resilience Act (CRA)**, which establishes mandatory cybersecurity obligations for products with digital elements placed on the European market.

While IEC 62443 and UR E27 provide the technical and process foundations for secure system design and operation, the CRA introduces additional regulatory obligations, including lifecycle accountability, vulnerability reporting, and user-facing security information.

1.3 Applicable products and software

The information in this document relates to these products and software versions:

Software	Version			
	IE 250	IE 250 Marine	IE 350	IE 350 Marine
Software bundle	2.0.17.x or later	2.0.17.x or later	2.0.17.x or later	2.0.17.x or later
PICUS	2.0.26.x or later	2.0.26.x or later	2.0.26.x or later	2.0.26.x or later
	IE 250 PLC	IE 350 PLC	IE 650 PLC	
Software bundle	2.0.16.x or later	2.0.16.x or later	2.0.16.x or later	
CODESYS IDE	3.5.20.40 or later	3.5.20.40 or later	3.5.20.40 or later	
IE x50 CODESYS TSP	1.3.8.0 or later	1.3.8.0 or later	1.3.8.0 or later	



More information

See www.deif.com for the latest approved certifications on your product.

1.4 Legal information

Third party equipment

DEIF takes no responsibility for installation or operation of any third party equipment. In no event shall DEIF be liable for any loss of profits, revenues, indirect, special, incidental, consequential, or other similar damages arising out of or in connection with any incorrect installation or operation of any third party equipment.

Use of Non-cybersecurity certified software (Developer edition firmware)

The Developer/Engineering Edition Firmware (identified as *IE x50 UPE vX* software bundle) is intended solely for advanced development purposes.

It permits users to edit or remove embedded cybersecurity rules and policies, perform customisations, run own applications or integrate 3rd party software, that inhibits DEIF to take responsibility for the software to comply with product relevant cybersecurity standards.

To the extent that the customer modifies or disables such cybersecurity features, DEIF shall bear no responsibility or liability for any resulting security vulnerabilities, unauthorized external access, data breaches, or any other interference or damages affecting the project. The customer assumes full responsibility for the consequences of any such modifications and has the responsibility for relevant cybersecurity certifications.

Trademarks

DEIF and the DEIF logo are trademarks of DEIF A/S.

Bonjour® is a registered trademark of Apple Inc. in the United States and other countries.

Adobe®, *Acrobat*®, and *Reader*® are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

CANopen® is a registered community trademark of CAN in Automation e.V. (CiA).

SAE J1939® is a registered trademark of SAE International®.

CODESYS® is a trademark of CODESYS GmbH.

EtherCAT®, *EtherCAT P*®, *Safety over EtherCAT*®, are trademarks or registered trademarks, licensed by Beckhoff Automation GmbH, Germany.

VESA® and *DisplayPort*® are registered trademarks of Video Electronics Standards Association (VESA®) in the United States and other countries.

Google® and *Google Chrome*® are registered trademarks of Google LLC.

Linux® is a registered trademark of Linus Torvalds in the U.S. and other countries.

Modbus® is a registered trademark of Schneider Automation Inc.

Torx®, *Torx Plus*® are trademarks or registered trademarks of Acument Intellectual Properties, LLC in the United States or other countries.

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

All trademarks are the properties of their respective owners.

Disclaimer

DEIF A/S reserves the right to change any of the contents of this document without prior notice.

The English version of this document always contains the most recent and up-to-date information about the product. DEIF does not take responsibility for the accuracy of translations, and translations might not be updated at the same time as the English document. If there is a discrepancy, the English version prevails.

Copyright

© Copyright DEIF A/S. All rights reserved.

2. Cybersecurity framework

2.1 DEIF Cybersecurity principles

DEIF's cybersecurity is based on foundational principles to ensure resilient, trustworthy, and certifiable controller operation. In marine applications this is in trusted environments. In land applications this is in trusted and untrusted environments. These principles underpin all design decisions, documentation guidance, and recommended customer practices.

Security by design

DEIF embeds cybersecurity considerations throughout the product's lifecycle. This includes requirements, design, development, testing, and maintenance.

This includes secure boot mechanisms, code-signing of firmware, advanced roles-based access system, controlled configuration interfaces, and careful exposure of only necessary services and ports. Security is intrinsic to the platform's architecture.

Least privilege & minimal attack surface

Only essential services are enabled, and all user actions are constrained by role-based access control. Controllers prevent unauthorized configuration changes and reduce exposure by disabling optional interfaces when not actively needed. This also includes documentation-guided customer recommendations for segmentation, DMZ placement, and limiting externally reachable services.

Verified & trusted software

All firmware updates must originate from DEIF. DEIF cryptographically signs the firmware. All firmware must pass integrity checks prior to installation. The aim is to prevent tampering, guarantee authenticity, and ensure that only trusted software components run on the device.

Defense-in-Depth

DEIF promotes layered protection, this includes:

- Secure communication channels.
- Password and authentication enforcement.
- Auditing, logging, and timestamp integrity.
- Network segmentation and filtering.
- Hardware and software level input validation.

Each layer mitigates different types of threats, supporting resilience even if another layer is compromised.

Transparent responsibilities

The [cybersecurity responsibilities](#) between [Product supplier \(DEIF\)](#), [System integrator](#), and [Asset owner \(Operator\)](#) are clearly defined.

This ensures customers understand what the controller secures by itself and where external infrastructure (firewalls, VLANs, monitoring systems) must be applied.

Protection of data integrity

DEIF prioritises secure handling of data in transit and at rest. Communication channels are encrypted, sensitive authentication data is hashed, and administrative actions are logged. System behaviour ensures that only authenticated and authorised users can read or modify configuration or operational data.

Resilience, recovery & safe operation

The controllers are designed to continue safe operation even in the presence of partial failures or security anomalies. Backup and restore mechanisms, configuration export/import controls, event logging, and controlled recovery procedures ensure that systems can be restored securely without introducing new vulnerabilities.

Compliance-aligned design

Where relevant, DEIF aligns product capabilities and documentation with marine and industrial cybersecurity standards, ensuring that system integrators and vessel owners can demonstrate compliance.

This includes mapping platform features to specific requirement areas (authentication, audit logging, cryptography, backup, recovery, and so on).

Continuous improvement & vulnerability handling

DEIF actively maintains product security through:

- Vulnerability management processes.
- Security advisories for customers published through controlled channels.
- Design iteration driven by internal assessments, security testing, and customer feedback.

This ensures that the provided cybersecurity is strengthened with reviewed threats and regulatory expectations.

Secure operational practices

Principles are backed by practical recommendations for everyday use:

- Strong password policies.
- Performing firmware updates securely.
- Monitoring logs for anomalies.
- Applying network segmentation.
- Reducing physical access risks.

These operational principles ensure the secure features built into the product are actually effective in real deployments.

2.2 Applicable standards

2.2.1 IEC 62443

Under IEC 62443, cybersecurity requirements are applied across the product lifecycle, with emphasis on secure design, development processes, component-level security, and lifecycle maintenance.

2.2.2 IACS URE27

Under IACS URE27, cybersecurity compliance applies to the product, its integration into maritime vessel systems, and its operation and maintenance within the onboard environment.

Product supplier (DEIF), as the product manufacturer, is responsible for implementing the applicable component-level security requirements. DEIF is also responsible for providing documentation describing the product's security capabilities and limitations (this document + others on request).

The **System integrator** is responsible for implementing compliant configurations and security controls as part of the system integration. The system integrator also produces configuration and commissioning artefacts that support compliance at the time of delivery.

The **Asset owner (Operator)** is responsible for ensuring that the deployed system remains compliant within its operational environment. The Asset owner (Operator) also maintains and presents the evidence required to demonstrate compliance over the system's lifecycle.

2.2.3 EU Cyber Resilience Act (CRA)

Under the EU Cyber Resilience Act (CRA), cybersecurity requirements apply across the product lifecycle, including design, development, market placement, and ongoing maintenance, with defined obligations for vulnerability management, reporting, and lifecycle support.

2.3 Roles & responsibilities

2.3.1 About responsibilities

This document specifies roles with associated responsibilities as defined by the cybersecurity standards.

Product supplier (DEIF)

- Secures the controller in compliance to cybersecurity requirements.
- Actions and resolves any detected cybersecurity issues.
- Provides information on any detected vulnerabilities and their mitigation or resolution.

System integrator

- Defines the system design and architecture in compliance to cybersecurity.
- Ensures the system is implemented in compliance to cybersecurity.

Asset owner (Operator)

- Ensures that the compliance requirements are properly met and demonstrable.
- Ensures that the operating environment remains secure over time (Operator).
- Ensures on-going monitoring for cybersecurity risks, including detection, tracing, diagnosing, and remediated efficiently.

2.3.2 Product supplier (DEIF)

DEIF's responsibilities focus on the security of the controller itself, the embedded software, and the mechanisms required to maintain a trustworthy operational platform.

Secure platform design & development

- Provide a controller platform designed according to security-by-design principles.
- Integrate cryptographic protections (secure boot, signed firmware, TLS).
- Minimize attack surface through restricted services and hardened defaults.

Firmware integrity & update security

- Ensure all firmware packages are digitally signed.
- Provide a validated update path that rejects tampered or untrusted firmware.
- Maintain secure distribution channels for firmware and documentation.

Authentication, Access control & User management mechanisms

- Implement secure password storage (hashing), login enforcement, and access control logic.
- Ensure system-enforced role-based permissions behave predictably and securely.
- Provide configuration mechanisms for disabling unused accounts and restricting access.

Logging, event auditing & system visibility

- Provide system logs (audit trails, I/O logs, user access logs) supporting traceability.
- Ensure timestamps, audit retention, and event classification follow IEC 62443 principles.

Security documentation & guidance

- Deliver accurate documentation about:
 - Product capabilities

- Network/protocol behaviour
- Supported security configurations
- Security advisories
- Provide customer-consumable guidance on secure configuration and best practices.

Vulnerability management

- Operate internal processes for vulnerability intake, triage, correction, and disclosure.
- Publish known issues through controlled channels.

2.3.3 System integrator

Integrators assemble complete solutions around the controller. Their security responsibility focuses on system architecture, networking, physical access, and correct application of DEIF's controls.

Secure system architecture

- Design network layouts (segmentation, VLANs, firewalls, DMZs) that respect DEIF's recommended trust boundaries.
- Ensure controllers are placed inside appropriate zones (that is, control zone, restricted access areas).
- Avoid exposing controller interfaces directly to untrusted networks.

Correct configuration of security features

- Configure TLS, certificates (if applicable), port rules, and user access as recommended.
- Disable unused interfaces (USB, Ethernet ports, services) following the hardening guidelines.

Secure deployment & commissioning

- Perform secure installation activities such as:
 - Changing default passwords
 - Restricting physical access to HMIs and controllers
 - Ensuring installation follows E27-aligned checklists
- Verify backups and recovery procedures are functional after commissioning.

Integration with external systems

- Secure SCADA, PLC, and external subsystem connections (protocols, firewall rules, access control).
- Ensure 3rd-party components do not weaken the security posture of the DEIF controller.
- Validate that data flows comply with the system-level security design.

Incident handling & maintenance

- Monitor logs and alerts from the controller as part of the system's security monitoring strategy.
- Apply firmware updates responsibly and promptly when DEIF releases security patches.
- Maintain disaster recovery processes aligned with DEIF's guidance.

2.3.4 Asset owner (Operator)

End users are ultimately responsible for the operational security environment in which the controller runs.

Protecting access to the system

- Enforce strong password policies and ensure only authorised personnel have access.
- Manage user accounts according to organisational policies.

Operating in a secure environment

- Maintain physical security of controller cabinets, rooms, HMIs, and connected equipment.
- Ensure network firewalls, monitoring tools, and intrusion detection systems (if used) remain active and configured properly.

Compliance with regulatory & certification requirements

- Ensure that the **overall vessel or plant installation** meets the cybersecurity requirements applicable (E27).
- Provide DEIF with necessary information if additional documentation is required for regulatory audits.

Lifecycle & change management

- Ensure updates, configuration changes, and maintenance activities follow secure operational practices.
- Periodically review access rights, logs, and system behaviour.

Incident handling & maintenance

- Monitor logs and alerts from the controller as part of the system's security monitoring strategy.
- Apply firmware updates responsibly and promptly when DEIF releases security patches.
- Maintain disaster recovery processes aligned with DEIF's guidance.

3. Security architecture and zones

3.1 Security zoning model

Security zoning defines how different parts of a system are separated based on trust, criticality, and exposure.

By segmenting the installation into well-defined zones, cybersecurity risks can be contained and mitigated, even if one part of the system is compromised.

The zoning model ensures that:

- Only essential traffic crosses boundaries.
- Interfaces exposed to external parties are tightly controlled.
- Critical control functions remain isolated and safeguarded.
- System integrators have a clear blueprint for secure network design.

Purpose of zones

The main objectives of zoning in deployments are to:

- Limit the affected area of a cybersecurity incident.
- Separate trusted and untrusted networks clearly.
- Control data flow pathways between subsystems.
- Apply differentiated security controls based on risk and operational needs.
- Support compliance with standards such as IACS E27, which prescribes explicit separation between control and non-control domains.

3.2 Typical security zones in an iE x50 system

A secure installation commonly includes the following zones. These may be adapted depending on vessel, plant layout, or integrator design choices.

Control zone (Highly trusted)

This is the most critical zone, containing safety-relevant and operationally essential components. This is the core zone that must remain operational even if outer layers experience disruptions.

Characteristics

- Contains the iE x50 controllers, I/O modules, local HMI, and internal control network.
- Physically protected and access-restricted.
- Minimal and tightly controlled external connectivity.
- Only essential traffic allowed (for example, SCADA read-only data, time sync, monitoring)

Security Controls

- Role-based access (local or remote).
- Non-routable internal addressing.
- Inbound firewall filtering with default-deny posture.
- Strict password policies and configuration lockdown.

Service or maintenance zone (Restricted access)

Used for local engineering laptops, setup tools, or on-site maintenance activities. This zone balances usability with the need to protect sensitive configuration functions.

Characteristics

- Temporary access only (commissioning, updates, diagnostics).
- Often physically local and supervised.
- Must never be permanently bridged to external or corporate networks.

Security Controls

- One-time passwords or controlled maintenance accounts.
- USB port limitations (where applicable).
- TLS-secured connections for configuration tools.
- Logging of configuration changes and administrative actions.

Operational or monitoring zone (Moderately trusted)

This zone hosts systems that need controlled access to operational data, such as:

- SCADA systems
- Vessel monitoring systems
- Historian servers
- Alarm and event collectors

This zone should not be able to modify core controller parameters unless explicitly designed and approved.

Characteristics

- Read-mostly access to the Controller.
- Typically isolated from both corporate IT and the Control Zone.
- May exchange data via proxies or one-directional communication paths.

Security Controls

- Strictly defined firewall rules.
- TLS for telemetry transmission.
- Rate-limiting and protocol whitelisting.
- Event and audit log forwarding.

Corporate or administrative zone (Low trust)

This network is usually part of the vessel owner's or plant operator's IT infrastructure. This zone may access cybersecurity documents, logs, or SBOM files, but never the control system directly.

Characteristics

- Contains office PCs, email systems, internal servers.
- Higher user diversity and risk of malware exposure.
- Not suitable for direct communication with the controller.

Security Controls

- No direct access to the Control Zone.
- Access routed through jump hosts, secured proxies, or DMZ.
- Segmentation from operational systems (OT/IT separation).
- System integrator-managed firewall boundaries.

External or Untrusted zone (No trust)

All networks outside the vessel or plant are considered *untrusted*:

- Internet or satellite links.
- Remote vendor access.
- Supplier-provided cloud services.

Controls

- No direct access to any internal zone.
- Remote access only via VPN or secure tunnel under tight supervision.
- Authentication, MFA (if supported), and session logging required.

3.3 Network architecture and topologies

3.3.1 Architecture principles

Network architecture and topology diagrams provide the bridge between security principles and real-world implementations. When combined with zoning, device hardening, and operational discipline, they help ensure that DEIF controllers are deployed securely, maintainably, and in a way that supports certification and long-term operation.

These principles align with the security zoning model described earlier and provide the baseline for all examples.

- Controllers are placed in a protected control zone.
- Direct access from untrusted networks is not permitted.
- All cross-zone communication is explicitly defined and restricted.
- Configuration and maintenance access is separated from operational data access.
- Network segmentation (firewalls, VLANs, routing rules) enforces zone separation.

NOTICE



Example topologies

All diagrams are examples and must be adapted to the specific vessel, plant, or project requirements. They do not replace detailed network engineering diagrams or account for possible project constraints.

Segmented control architecture

- Control Zone isolated behind firewall.
- Monitoring systems receiving data through restricted rules.
- No inbound connections from lower-trust zones.

DMZ-based architecture

- DMZ acting as buffer between control and corporate networks.
- Data replication or proxy services in DMZ.
- No direct routing between corporate IT and control systems.

One-way or restricted data flow architecture

- Read-only data export paths.
- Physical or logical enforcement of unidirectional flow where applicable.

3.3.2 Diagrams for compliance and audits

The topology diagrams can be used to:

- Demonstrate compliance with E27 zoning and segregation expectations.
- Support vessel or system inspections.
- Validate that architecture aligns with documented security principles.
- Identify gaps between recommended and implemented designs.

Customers and integrators should annotate diagrams with:

- Actual IP ranges

- Firewall rules
- Device identifiers
- Physical locations

3.3.3 iE 250

Key Characteristics

- iE 250 located within the **Control Zone**
- Local HMI and I/O connected via internal control network
- SCADA or monitoring systems connected through a controlled interface
- Maintenance access via a dedicated service network or temporary connection

Illustrated Elements

- Control Zone (iE 250, I/O, local HMI)
- Operational / Monitoring Zone (SCADA, historian)
- Service / Maintenance Zone (engineering laptop)
- Firewall or gateway enforcing access rules

Security Highlights

- No direct connection between iE 250 and corporate or external networks
- Read-only access paths clearly differentiated from write/configuration paths
- TLS-secured communication where applicable

3.3.4 iE 350

3.3.5 iE 650

4. Hardening and configuration

4.1 Purpose of device hardening

Device hardening increases robustness even when outer network zones or operator practices are imperfect.

It protects the system and operation and aims to:

- Reduce the available attack surface.
- Enforce secure defaults and disable unnecessary features.
- Ensure predictable and resilient system behaviour.
- Support E27 requirements related to least functionality, secure configuration settings, auditability, and resilience.
- Provide a foundation upon which integrators and customers build secure installations.

4.2 Secure configuration baselines

A secure configuration baseline defines the minimum required settings to operate the device safely. This baseline should be applied during commissioning and periodically re-verified.

User and access configuration

- Disable default or unused accounts.
- Assign minimal roles
 - Grant write/modify permissions only to authorised users.
- Ensure first-login password change is mandatory.

Service and interface configuration

- Disable or restrict unused network services (e.g., HTTP if only HTTPS is required).
- Turn off unused protocols and legacy functions not required by the application.
- Disable USB ports when not needed, or lock them physically (if supported).

4.3 Network exposure reduction

Hardening is closely tied to controlling which network interfaces are exposed and what they allow.

Port and service minimisation

- Close all non-essential inbound ports.
- Permit only documented application ports (refer to port/service matrix).
- Prevent external access to configuration services unless in maintenance mode.

IP filtering and access control

- Apply IP whitelisting where supported.
- Restrict access to only trusted IP ranges (that is, inside the control zone).
- For monitoring systems, consider one-directional write-protected paths where possible.

Protection against external interference

- Ensure the controller is not directly reachable from untrusted networks.
- For remote access, require authenticated tunnels (VPN, secure gateway) under controlled conditions.

4.3.1 Network configuration

The default is to use DHCP to obtain the IP address, subnet, netmask and DNS servers. If you use a manually configured (static) IP, be careful to make sure that the selected values match the network to which the controller is connected.

Service	Protocol	Port	Direction	Notes
Web configuration	HTTPS (TCP)	80	Inbound	Opened and re-directed to port 443.
Web configuration	HTTPS (TCP)	443	Inbound	Opened to allow communication with PICUS.
Modbus server	TCP	502	Inbound	Opened to allow Modbus TCP communication.

In addition, the controller may use the following ports for application and PLC communication:

Service	Protocol	Port	Direction	Notes
Network time synchronisation	UDP	123		NTP client
		503		
		1217		
		1740		
		1741		
		1742		
		1743		
		4321		
OPC UA	TCP	4840		If OPC UA is enabled.
Multicast DNS (mDNS)	UDP	5353		Used for device discovery.
		8000		
		8443		
		11740		
		12345		
		12346		
		12350		
		12351		

4.4 Physical protection measures

Security is not only digital as physical access can bypass many protective controls.

Physical isolation

- Install controllers in locked cabinets or control rooms with restricted access.
- Protect HMIs to prevent walk-up access by unauthorised personnel.

Port and interface controls

- Physically secure engineering ports, USB connectors, or unused wired interfaces.
- If applicable, use tamper-evident seals or locking mechanisms.

4.5 Logging and monitoring hardening

Hardening is incomplete without visibility into device behaviour.

Automatic logs

- All iE 250 or iE 350 controllers automatically create event and system logs.
- The controller stores up to 2000 event log entries and discards the oldest using First In, First Out when full.
- WebConfig provides further access to additional system logs which can also be exported.

Audit log retention

- Archive logs periodically, especially before and after commissioning.
- Use WebConfig to export the system logs and store these securely in your protected IT system.

Monitoring integrations

- Tie device logs into SCADA/historian systems if needed.
- Create alerts for repeated failed logins, unexpected port activations, or configuration changes.

4.6 Hardening for Untrusted network scenarios

In situations where controllers may be indirectly connected to untrusted networks (via gateway, shared infrastructure, vendor access):

- Use strict firewall isolation and deny all direct inbound connections.
- Require remote access to pass through a secure jump host or VPN with MFA.
- Limit available services to read-only interfaces wherever operationally acceptable.
- Increase log verbosity for these deployments to assist with monitoring.

5. User and access management

5.1 About permissions

The controllers' configuration and functionality is protected with permission access. Only users with the correct permission may access, configure, or update the configuration or controller settings.

Permission structure

The permissions consist of **Roles** and **Users** in each controller configuration. These are stored locally on each controller, or can be written to all connected and logged in controllers.

Each **user** is a member of a **role**. The **role** gives the **user** permissions to associated features or functions of the controller. You can also remove access from a user as required.

Permissions access enables you to easily control which user can access which function. This provides a layer of control for the operation of the controller.

NOTICE



Permissions access

You can only access the user permissions option if you are a member of a role that has access to that function.

5.2 Roles and Users

5.2.1 Role settings

Role settings include both **Role information** and **Role permissions**.

Role information

The **Role information** contains the name and automatically recorded changelog.

Setting	Type	Format	Notes
Name	Manual	Text	The Role name.
Created	Automatic	Date	Date the role was created.
Changed	Automatic	Date	Date the role was changed.
Editor	Automatic	Text	The user who created or changed the role.

Role permissions

The **Role permissions** allow or remove access to features in the software.

Parent permissions are required for any child permissions. For example, to allow access to the feature **Emulation** (a child), the role must also have access to **Application** (the Parent). If you remove a parent permission, all child permissions are automatically removed.

Some features can be configured for **Read** and/or **Write** access. With **Read** only access the user cannot write or update any information. **Read** access is mandatory if you allow **Write** access.

Feature permissions	
Live Data	Live Data
Application	Plant configuration Emulation Supervision
Alarms	Alarms Alarm acknowledge Alarm reset latch Alarm out of service Alarm shelve
Log	Event log Engine interface J1939 DM2 Engine interface J1939 DM2 clear
I/O status	I/O status
Tools	Print setup Backup restore Backup Restore Restore configuration Trending Regulator status Alarm test Firmware User management Role management
Configure	Date and time Communication Input/output configuration Parameters Counters CustomLogic Modbus Fieldbus configuration Fieldbus supervision Dashboard configuration Header configuration
Not assigned a category	Feature toggle Notification configuration

5.2.2 User settings

Setting	Type	Notes
User name	Required	Minimum 2 characters.
Organisation	Optional	
Roles	Required	Selectable from list.
Mobile number	Optional	
Direct number	Optional	
Email (primary)	Optional	

Setting	Type	Notes
Email (secondary)	Optional	
Password	Required	Minimum 8 characters and must comply with password verification .

5.2.3 Default user

The default administration user is **admin**. Only **admin** can access WebConfig.

User	Password	Role
admin	admin	Administrator for the system.

NOTICE



Secure your system

Ensure that all default passwords are changed to reduce the security risk to your system. Additionally, it is recommended to adjust or edit the role and user permissions according to your own operational needs.

NOTICE



Lost passwords

Lost passwords cannot be recovered. If you have lost your password you can not configure your controller or system.

If you have lost your password, then you must use the Factory reset and reconfigure your controller by using your recovery backup.

5.3 Password strength verification

All created and modified passwords are subject to password strength verification.

Entered passwords must:

- Have a minimum length of 8 characters or more.
- Not include repeated words or substrings (for example "abcabcabc").
- Not be listed on known vulnerable passwords (for example "12345678", "password").

6. Vulnerability management

6.1 Monitoring and on-going security

Vulnerability management is not limited to firmware updates or published security advisories. Continuous monitoring of system behaviour, access, and events is a critical part of maintaining a secure and resilient installation during the operational lifetime of the system.

The DEIF controllers provide built-in security mechanisms and logging capabilities. End-customers are responsible for maintaining the security of the system throughout its operational lifetime. This includes actively monitoring, reviewing, and responding to any security-relevant information generated by the system.

It is expected that Asset owner (Operator):

- Monitor the system behaviour and status to identify any anomalies or unexpected operations.
- Regularly review logs and access events for failed logins, configuration changes, or misuse.
- Manage user accounts and credentials, ensuring access is granted only when required.
- Control and audit maintenance or remote access, keeping it authorised and time-limited.
- Detect and respond to security indicators, even when no formal vulnerability notice exists.
- Maintain secure operation over time, including after system, network, or configuration changes.

6.1.1 About activity logs

Each controller records activity of both the system and operational events.

These are recorded in logs:

- Event log
- Live system log

6.1.1.1 Event log

This can be accessed with PICUS or the display.

All activities that require a user login are logged with the username. The user can also use the controller for some actions without logging in (for example, selecting breaker open). These actions are logged without a username.

The controller stores a maximum of 2000 event log entries. When the log is full, the controller discards the excess log entries using first in, first out.

If an ECU has been configured, you can also switch to see the DM2 logs.



More information

See the [PICUS manual](#) or [Operator's manual](#) for how to view the Event log.

6.1.1.2 System log

This can only be accessed with WebConfig and the **admin** user.

The *Live system log* records all different system-related events that occur. These logs can be useful for cybersecurity control, troubleshooting issues, and also for product support.

These logs include:

- System events and journal.

- Connected session access with WebConfig.
- CODESYS related information.

Download logs

You can select and download the system logs directly from the controller as text files.

1. Select **Download** from **Logs**.
2. Select the **Duration** (period) you want to download.
 - This can be **Latest**, **Day**, **Week**, or **All**.
3. Select the **Type** of log to download.
 - This can be **SYSLOG**.
4. Select **Download** to create a ZIP archive with the log files included.
5. Locate your browser's download location to access the ZIP archive.

SYSLOG

The system log (SYSLOG) archive includes:

- Authentication journal.
 - *Connected sessions with WebConfig.*
- Reliability log.
 - *Operational values and performance information.*
- System journal.
 - *System operations.*

6.1.2 Backup procedures

Customers are **strongly recommended** to create and securely store backups of device configurations after commissioning and following significant configuration changes. Backups support recovery and operational resilience but may not include all system elements.

Purpose of backups

Backups are intended to:

- Enable recovery after device replacement, hardware failure, or unintended configuration changes.
- Reduce system downtime following incidents or maintenance activities.
- Support troubleshooting and system restoration activities.

Backup creation

Customers should:

- Create a backup after initial configuration and commissioning of the device.
- Create a new backup after any significant configuration changes.
- Ensure backups reflect the final operational configuration of the system.

Where multiple devices are deployed, backups should be created and maintained per device.

Backup content and limitations

Backups include device configuration data. They do not necessarily include application projects, external dependencies, or system-level data beyond the device configuration.

Customers are responsible for ensuring that all required system elements are backed up using appropriate tools and procedures.

Secure storage of backups

Backups should be:

- Stored in a **secure and controlled location**.

- Protected against unauthorised access, modification, or loss.
- Retained in accordance with the customer's internal policies and applicable regulations.

Where applicable, backups should be included in the customer's asset inventory and system documentation.

In maritime applications the backups should be stored as part of the ship inventory system.

Backup availability

Customers should ensure that:

- Backups are readily available when required for recovery.
- Backup files can be clearly associated with the relevant device, configuration, and system version.

It is recommended to verify backups periodically to ensure they remain usable.

The manufacturer provides guidance on supported backup mechanisms but does not manage customer backups.

Customer responsibility

The creation, storage, and management of backups is the **responsibility of the customer or system integrator**.

It is recommended to verify backups periodically to ensure they remain usable.

6.2 Security advisories

DEIF provides a list of known Cybersecurity related vulnerabilities on www.deif.com. Access is provided by a customer login.

Each vulnerability is listed:

- Identifier.
- Title.
- Detailed description.
- Recommended mitigation.

6.3 Incident response & recovery plan

6.3.1 Report vulnerability

You can report vulnerability or detected security issue by using the DEIF support ticket system.

<https://deifsupport.deif.com/support/tickets/new>

When providing a report, make sure to include as much additional information as possible.

Provide the following:		Notes
Requester	(Mandatory)	Your contact email.
Subject	(Mandatory)	
Type		Security vulnerability/incident
Product	(Mandatory)	
Software version	(Mandatory)	
Description	(Mandatory)	Textual description of the vulnerability or incident. Attach the following information: • System log files (Download from WebConfig).

Provide the following:		Notes
		Overall System configuration (Interface diagram).
Order number	(Optional)	
Product Serial Number	(Optional)	
Local office	(Mandatory)	

6.3.2 System recovery and restore

In the event of a suspected or confirmed cybersecurity incident, the customer is responsible for restoring the system to a known safe and trusted state.

Recovery actions should be performed in a controlled and documented way to prevent reinfection or configuration issues.

After identifying and containing the incident, customers should:

- Isolate the affected controller or system from networks and external access to prevent further impact.
- Preserve logs and configuration data where possible, to support analysis and reporting.
- Reset the controller to a trusted baseline, use the Factory reset if compromise cannot be ruled out.
- Restore the system from a known-good backup, created prior to the incident and verified as clean.
- Re-apply security hardening measures, including user access controls, passwords, and network restrictions.
- Verify correct operation and integrity before reconnecting the system to operational networks.

Any firmware updates or recovery images used must originate from trusted sources and follow documented procedures. Once restored, customers should review the incident to identify root causes and implement corrective measures to reduce the likelihood of recurrence.

Effective incident recovery depends on preparedness, including having up-to-date backups, clear internal procedures, and defined escalation paths.



More information

See the [PICUS manual](#) for how to create and restore backup files from your controller.



More information

See the **WebConfig** chapter in the Designer's handbook for how to *Factory reset* your controller.