WHITE PAPER

ABB Ability™ Digital Powertrain enabled by Tampnet Networks and powered by Ericsson IoT Accelerator

IEC 62443 Compliance

- IEC 62443 is an internationally recognized standard for securing industrial automation and control systems (IACS).
- The standard comprises multiple documents addressing various perspectives of cyber security.

Table of contents

Executive Summary

IEC 62443 is an internationally recognized standard for securing industrial automation and control systems (IACS). The standard comprises multiple documents addressing various perspectives of cyber security. These include requirements for an organization's cyber security management system, requirements for developing secure products, and how to maintain security throughout the product life cycle. The cyber security management system (CSMS) is addressed in IEC 62443-2-4, while IEC 62443-4-1 focuses on secure product development and IEC 62443-4-2 provides requirements on securing products according to four security levels (SL1-SL4). An IACS product can be certified against IEC 62443-4-2. Such certification proves that the product exhibits capabilities to meet a specific security level, such as security level 2 (SL2). Certification against IEC 62443-4-2 specifies the security capabilities (SL-C) of the product.

This white paper presents the combined ABB, Tampnet and Ericsson offering: ABB Ability™ Digital Powertrain enabled by Tampnet Network and powered by Ericsson IoT Accelerator (IoTA) platform. At the core of this offering, which provides condition monitoring, is the ABB Drive Connectivity Panel, ACS-DCP-11. ACS-DCP-11 has been evaluated against IEC 62443-4-2 SL 2 (security level 2) requirements to provide assurance on how to securely use this device to collect and transmit data from within an operational technology (OT) environment. In addition to IEC 62443-4-2 compliance, it is essential to a secure product development process and life-cycle management to have an overall structured approach to cyber security. This is represented by a cyber security management system, such as that defined in IEC 62443-2-4. This white paper describes the CSMS for the three involved companies and how these together provide end-to-end cyber security for the joint offering.

This white paper was created in cooperation between ABB, Tampnet and Ericsson. The copyrights of the white paper are with ABB.

About ABB

ABB is a technology leader in electrification and automation, enabling a more sustainable and resource-efficient future. The company's solutions connect engineering know-how and software to optimize how things are manufactured, moved, powered and operated. Building on more than 130 years of excellence, ABB's ~105,000 employees are committed to driving innovations that accelerate industrial transformation.
More information at: www.abb.com.

About Tampnet AS

Founded in 2001, Tampnet owns and operates the largest offshore high-capacity communication network in the world and serves more than 350 oil and gas platforms, FPSOs, exploration rigs and vessels in the Gulf of Mexico and the North Sea. Tampnet's infrastructure includes over 4,500 km of subsea fiber optic cable which is complemented by numerous high capacity, carrier grade radio links, and an extensive 4G LTE network with a coverage area of over 500,000 sq. km. Recently expanding the network, Tampnet is now providing connectivity to offshore wind farms and has added Trinidad and Tobago and Canada to its portfolio of serviced regions.
More information at: www.tampnet.com.

About Ericsson

Ericsson enables communications service providers and enterprises to capture the full value of connectivity. The company's portfolio spans the following business areas: Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses.
This portfolio is designed to help Ericsson's customers go digital, increase efficiency, and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.
More information at: www.ericsson.com.

Introduction and background

ABB, Tampnet and Ericsson collaborate to offer end-to-end security of condition monitoring solutions and services for ABB customers. ABB provides security for the Digital Powertrain devices, Tampnet provides secure mobile network solutions and services, and Ericsson secures the underlying network infrastructure. The ABB Ability™ solution running in Microsoft Azure is secured by Microsoft, with additional security configurations provided by ABB. Together, this ensures end-to-end security and provides the essential trust needed for condition monitoring of ABB assets within operational technology (OT) environments.

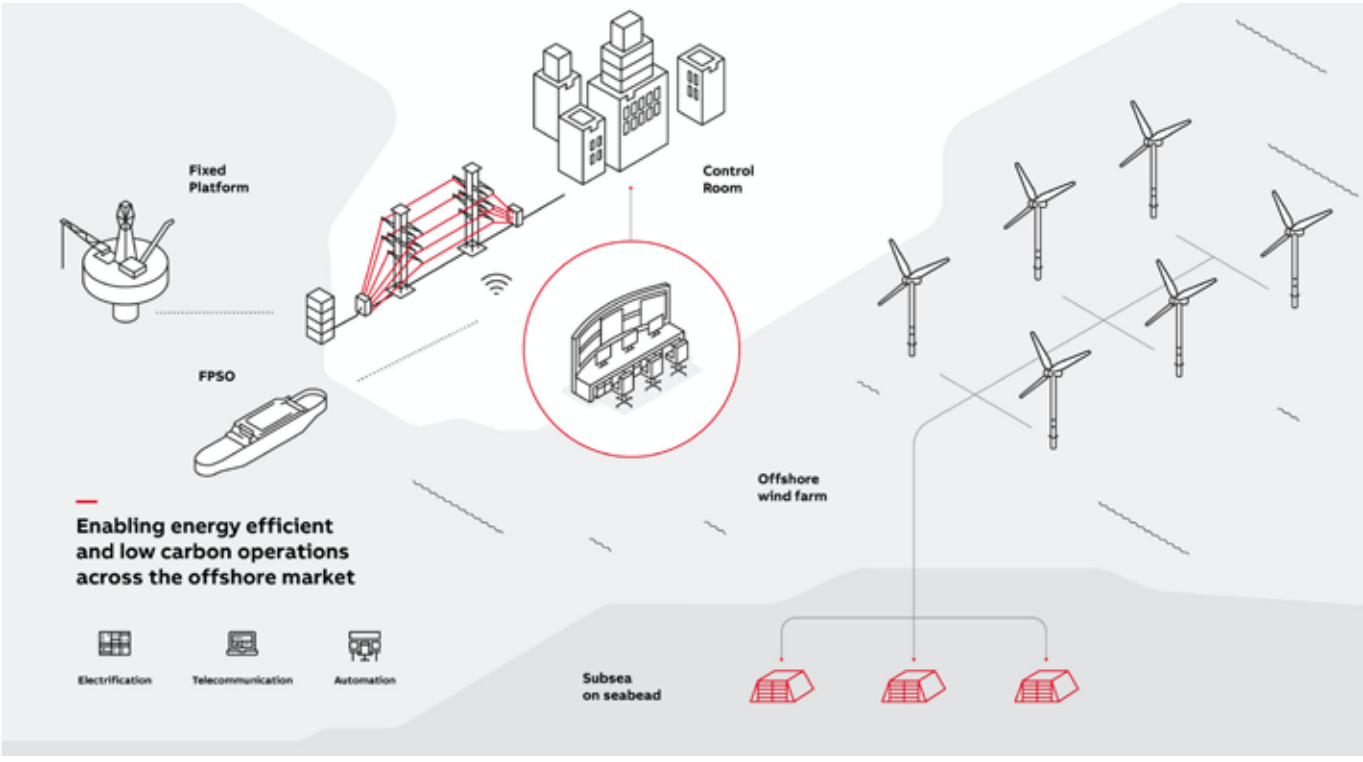
ABB's integrated electrical, automation and telecommunication approach, backed by its extensive service and digital capabilities, allows customers to execute projects and run efficient operations, sometimes in very remote locations. ABB can optimize production and costs throughout the asset's life. From floating production units to subsea, ABB provides innovative, next-generation solutions to help improve uptime and operational efficiency.

ABB Ability solutions combine ABB's deep domain expertise with connectivity and software innovation. This combination empowers real-time, data-driven decisions for safer, smarter operations that maximize resource efficiency and contribute to a low-carbon future. ABB's extensive portfolio of digital solutions helps organizations automate, optimize and future-proof their business to achieve new heights of performance and drive sustainable progress.

ABB and Ericsson have been collaborating on various research activities on industrial connectivity since 2015. Together, ABB and Ericsson are driving the digital transformation of industries, seizing the full potential of 5G connectivity for collaborative automation and digitalization with greater simplicity, flexibility and productivity for manufacturing customers globally.

Tampnet operates the world's largest offshore LTE network (> 500 000 km² combined in NSEA[1)] and GoM[2)]). Together with Ericsson, Tampnet provides telecommunications infrastructure and solutions to support ABB's existing and future deployments of machine-to-machine communication and digitization initiatives in maritime industries and offshore markets.

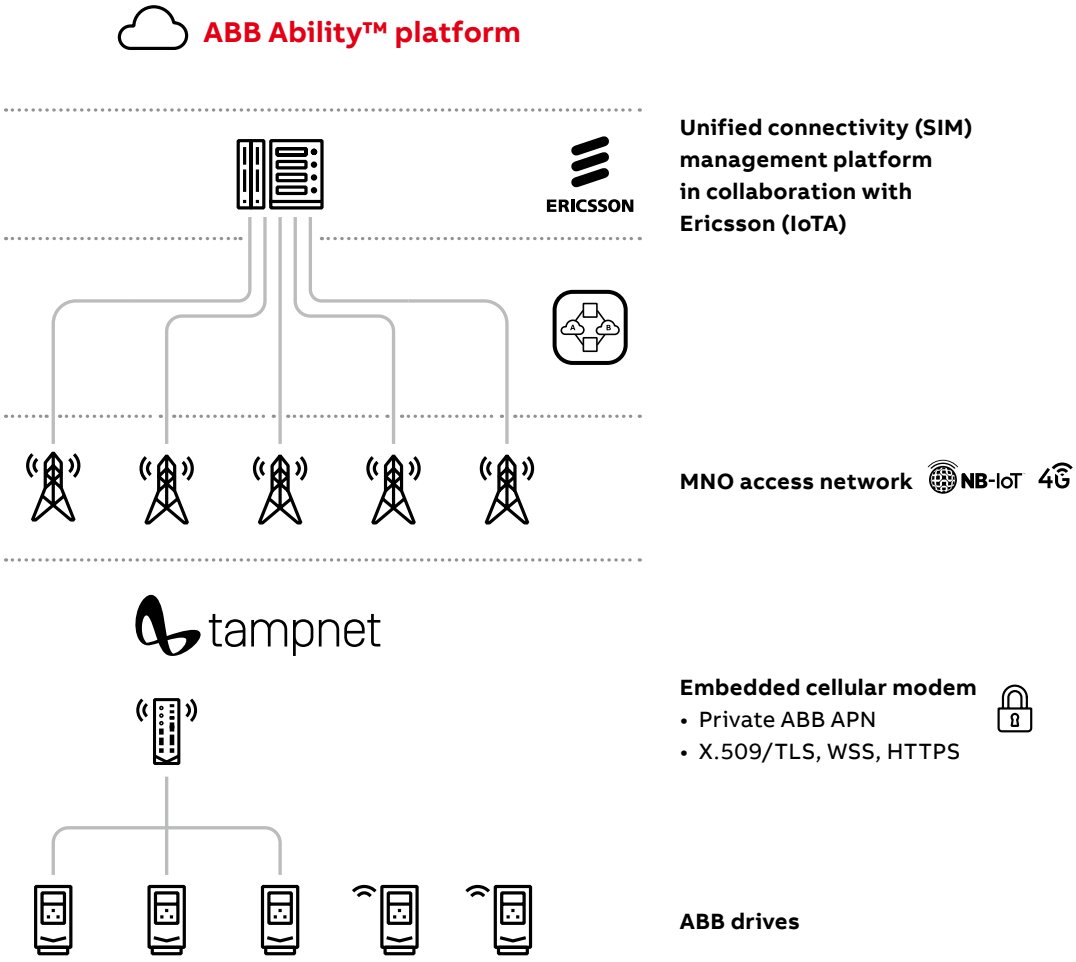
[1)] North Sea
[2)] Gulf of Mexico



Solution overview

The ABB Ability™ Digital Powertrain enables data collection and secure transfer of data from within an operational technology (OT) environment to the ABB Ability™ platform. The solution offers end-to-end security supported by Tampnet Network solutions and the Ericsson Internet of Things Accelerator (IoTA) platform. These are combined with ABB's products and services to offer a secure and holistic condition monitoring solution.

The figure below outlines the wireless data flow from ABB's Digital Powertrain over the Tampnet radio network and the Ericsson IoTA platform to the ABB Ability™ Digital Powertrain portal.



Self-service condition monitoring

The ABB Ability Digital Powertrain is a suite of digital technologies to improve the performance, reliability and efficiency of all components within the powertrain: from drives and motors to pumps, fans and other applications. The purpose is to help customers make better decisions and to keep processes running smoothly, with lower downtime and increased energy efficiency.

This white paper focuses on ABB Ability™ Condition Monitoring for drives which is part of the ABB Digital Powertrain offering. The services provide information about drive events and changes in behavior, ensuring that equipment is always available, reliable, and well-maintained.

1 Select your drives

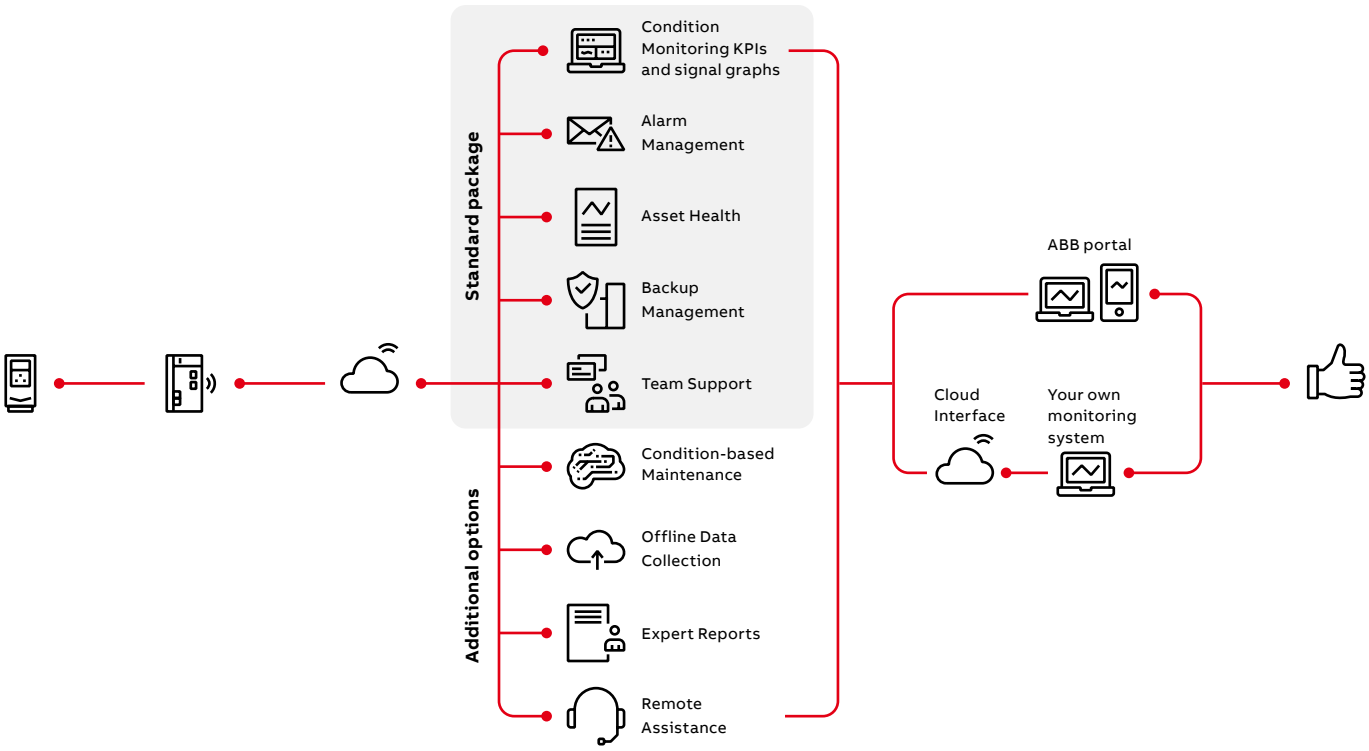
2 Install the connectivity device

3 Get acces to the Condition Monitoring standard options and choose your additional options

4 Access directly to the ABB portal or activate data transfer via Cloud Interface

5 Start monitoring

6 Make proactive decisions – built on real-time information



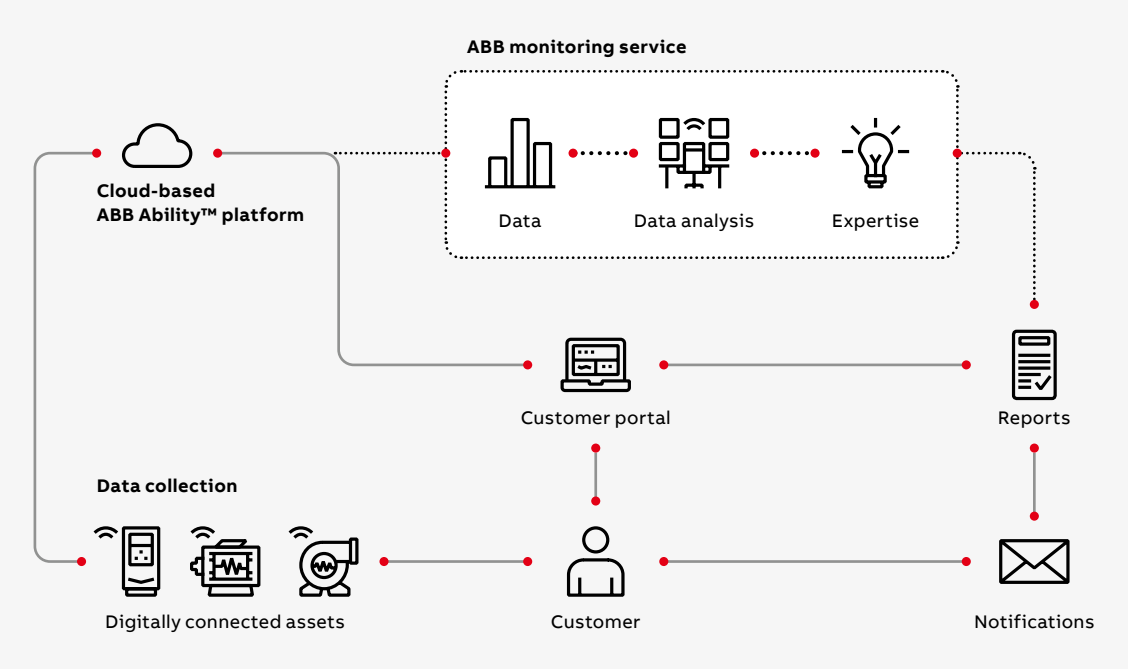
The standard package provides industry-leading capabilities to fit any monitoring needs. It supports drive status monitoring through ABB's internet portal and the integration into existing customer-managed monitoring systems.

Optional services include digitally enabled remote assistance, advanced analytics and reporting, and other features to make maintenance operations more effective.

Monitoring service

ABB's monitoring service gives users of motors, variable speed drives and their driven equipment access to a network of remotely located ABB technical experts. These engineers proactively track the performance of assets, provide regular reports, trigger early warnings, and highlight areas for improvement.

Keeping a watchful eye on all motor-driven applications can be time and resource-demanding. Furthermore, handing over the performance tracking of assets not only offers peace of mind but frees valuable maintenance teams to be deployed on other critical tasks.



The monitoring service engages a network of ABB engineers to track the performance of a facility's motors, drives and applications, such as pumps and fans. It can be applied to an asset if it gathers data using one of ABB's connectivity devices, such as the 2nd generation Smart Sensors [3], NETA-21, or ABB Drive Connectivity Panel. Alongside remote monitoring, ABB provides regular updates with informed comments about the status of the assets included in the monitoring contract. If a motor or drive is under-performing, an extended report can be provided, offering a greater insight, highlighting critical issues that require attention and provide recommendations on maintenance priorities.

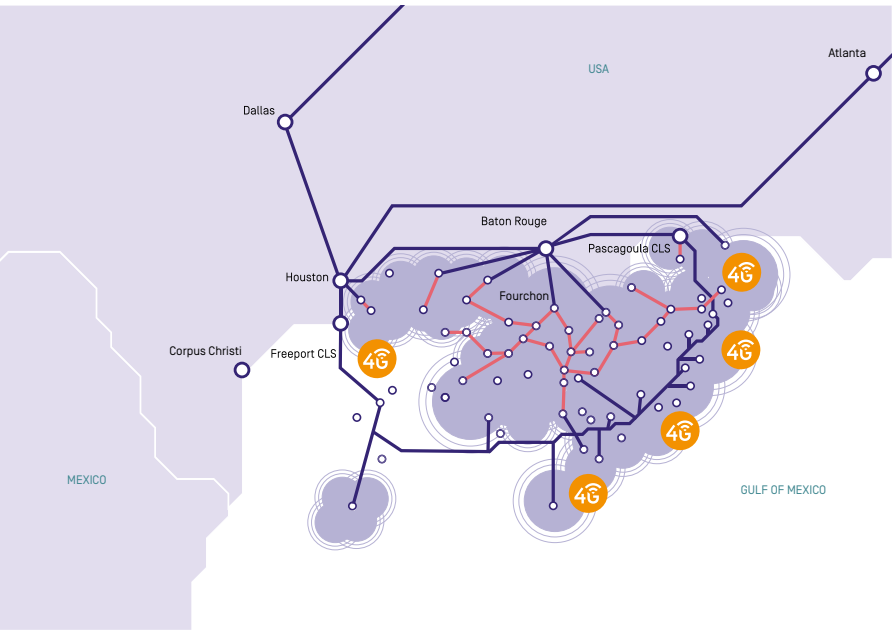
[3] Smart Sensors are not covered in this white paper.

ABB Drive Connectivity Panel: ACS-DCP-11

The ABB Drive Connectivity Panel enables an easy and secure Narrowband Internet of Things (NB-IoT) connection to drive support and digital services. The panel provides insights into the health and performance of drives and enables better operational decisions to keep processes running smoothly, with lower downtime and increased energy efficiency. Empowered by NB-IoT, the world's leading mobile communication technology for IoT, the ABB Drive Connectivity Panel can provide drive monitoring even if the drive is located underground or in a complete steel cabinet.

The NB-IoT modem connects to the ABB system within a private Access Point Names (APN).
It uses state-of-the-art transport layer security TLS1.2 certificates for secure communication and authorization towards the cloud system.
The panel is a further development of the existing control panel portfolio from ABB Motion, allowing the user to deploy the ACS-DCP-11 in their installed base without needing to train personnel on the products. Furthermore, it offers plug-and-play installation and easy commissioning without additional costs and supports all ABB Drives' all-compatible portfolio.

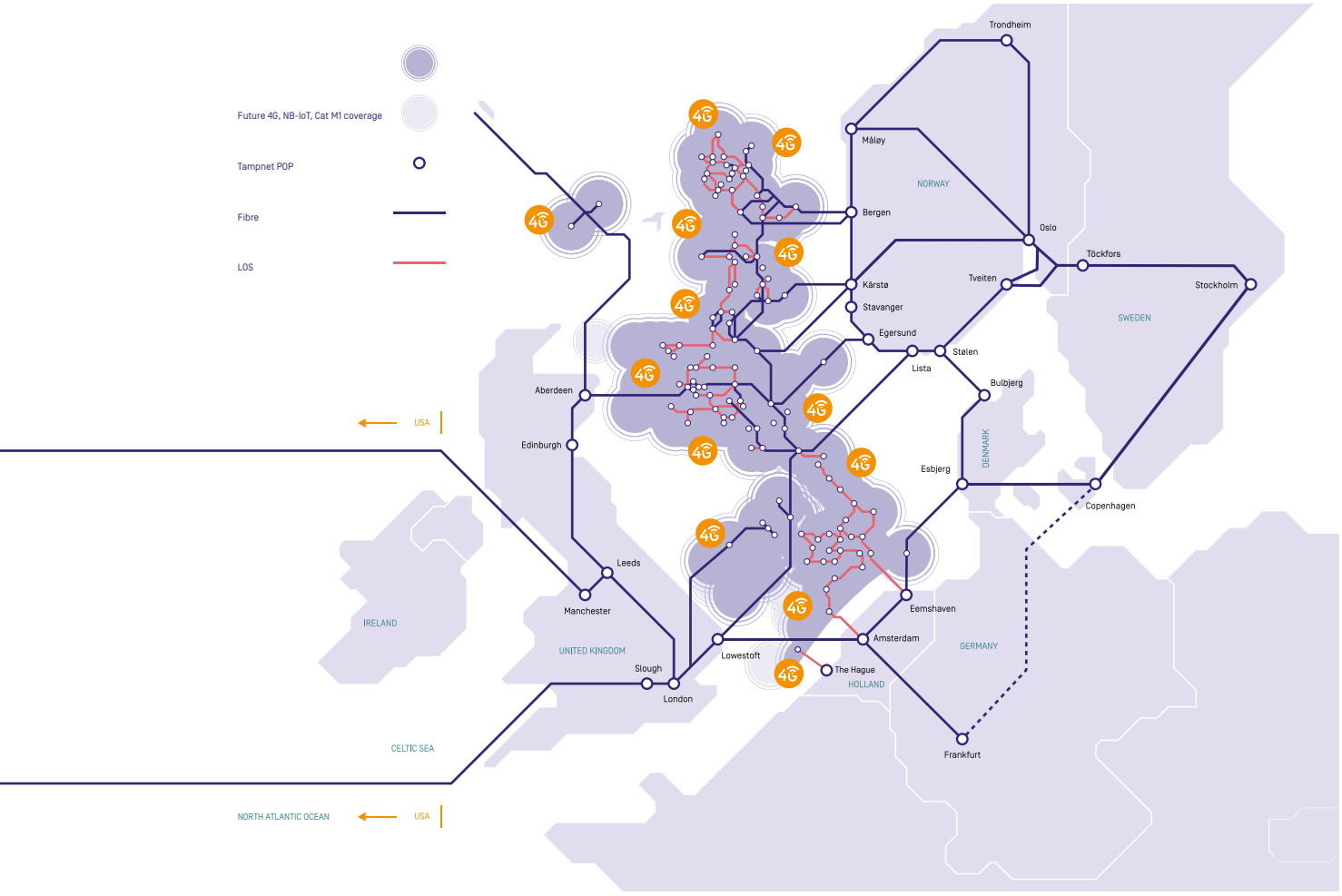
Tampnet Network and Services



Tampnet is a highly specialized and unique offshore communications and telecom operator. The Tampnet North Sea network consists of approximately 3300 kilometers (km) of subsea fiber cables owned and operated by Tampnet. The North Sea Infrastructure is complemented by 138 microwave hops and 50+ Long-Term Evolution (LTE) base stations providing 250,000 square kilometers of LTE coverage (including Narrowband Internet of Things (NB-IoT) and Category M1 (CAT-M1)). Tampnet provides premium connectivity to approximately 350 production platforms globally and for many drilling rigs and offshore vessels.

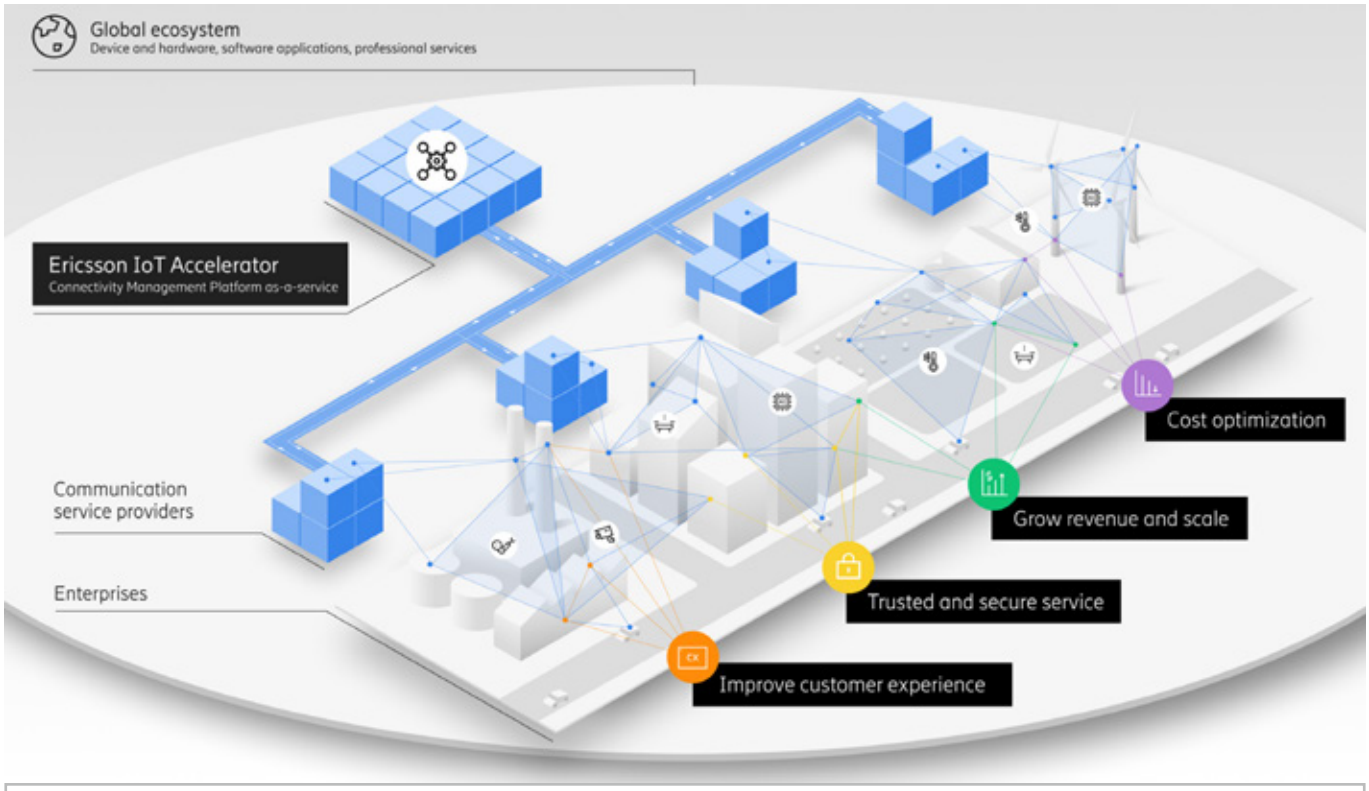
The Tampnet Gulf of Mexico (GoM) network resembles the North Sea infrastructure and consists of 1200 km of subsea fiber cables, approximately 100 microwave links and 250,000 km of offshore LTE coverage.

tampnet



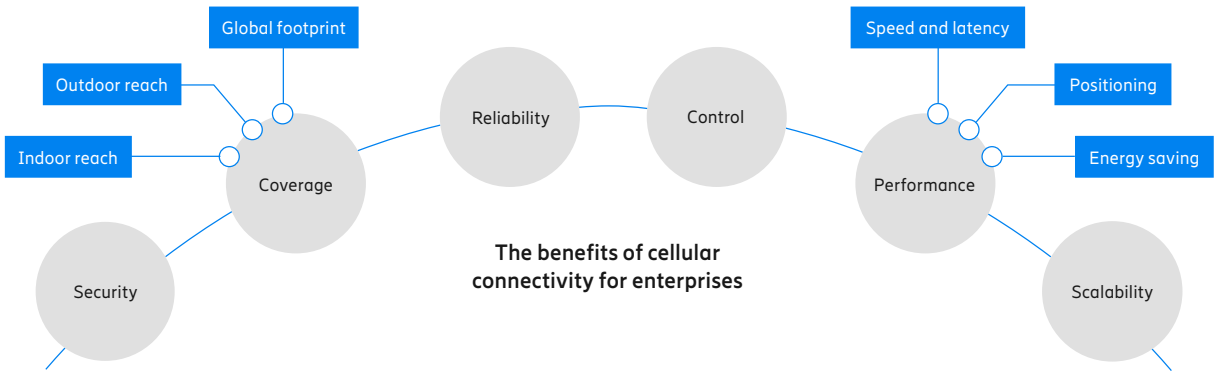
Ericsson IoT Accelerator

Ericsson IoT Accelerator (IoTA) enables enterprises to easily deploy, manage and scale their global IoT business from a single IoT platform. Delivered as a service through its global partner network, Ericsson's one core network provides complete visibility and control of all IoT devices throughout their entire life cycle, no matter where in the world they are located.



The cellular advantage – one network infrastructure to support all enterprises' needs
Cellular technology is built on global standards, future-proofing enterprises and connecting them to rich, diverse and versatile ecosystems.

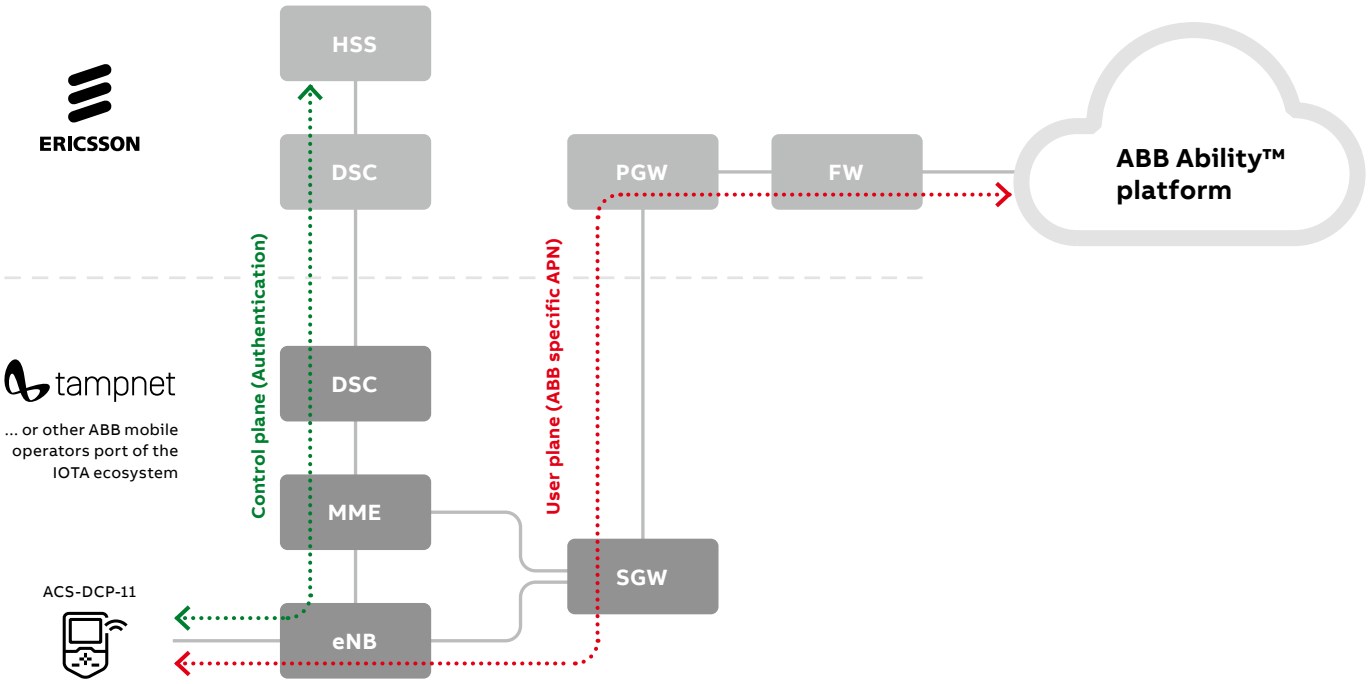
ERICSSON



The benefits of cellular connectivity for enterprises

End-to-end security

The ABB Ability Digital Powertrain provides end-to-end security by combining multiple security features, including identification, authentication, authorization, and secure data transfer using data encryption and transport layer security such as TLS1.2 and Virtual Private Network (VPN). The cloud part of the solution (ABB Ability platform) which provides the analysis involved in condition monitoring, whether self-service or monitoring service, runs on Microsoft Azure which provides extensive security features and international and regional security certifications. Certifications include SOC 1 Type 2, SOC 2 Type 2, SOC 3, ISO 27001, and relevant standards from the United States, Australia, New Zealand, EU countries, China, and others.



Core security features in the end-to-end security solution are identification and authentication of the ACS-DCP-11 Panel and establishing secure data sessions.

The elements involved in authenticating and establishing secure data sessions are (as specified by the 3GPP):

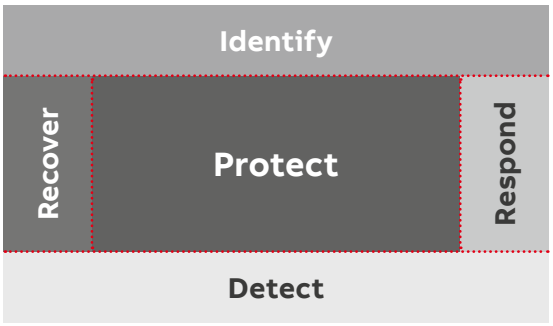
- Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network Node (eNB) covering functions including radio resource management, admission control, scheduling, enforcement of negotiated Quality of Service, cell information broadcast, ciphering/deciphering of user and control plane data, and compression/decompression of user plane packet headers.
- Mobility Management Entity (MME) that provides mobility session management for the Long-Term Evolution (LTE) network and supports subscriber authentication, roaming and handovers to other networks.
- Diameter Signaling Controllers (DSC) that ensure the routing of diameter signaling messages using DRA and DEA. The Diameter Routing Agent (DRA) role provides intra-network connectivity between elements, while the Diameter Edge Agent (DEA) role provides inter-network connectivity for roaming capabilities.
- Home Subscriber Server (HSS) which is the master user database. It contains subscription-related information and performs authentication and authorization of the user.
- Serving Gateway (SGW) which routes and forwards user data packets to the PGW.
- Packet Data Gateway (PGW) which is the connecting node between the ACS-DCP-11 and the firewall providing access to the ABB Ability platform.
- The firewall (FW) which terminates the data traffic and secures the traffic traversing the internet.

The components involved in the ABB Ability Digital Powertrain communicate between themselves on a dedicated ‘control plane’ and ‘user plane’ which provides the following services:

- The control plane authenticates ACS-DCP-11 in the mobile network. This is done at the user equipment level where a Subscriber Identity Module (SIM) card is authenticated with the SIM credentials and embedded security. User Equipment (UE) authorization to mobile network is managed from an advanced mobility management service to ensure that only authorized UE can access services and content. Furthermore, temporary identities are used to protect the user identity while communicating over a radio link.
- The user plane establishes a data session using a specific ABB APN between the user equipment (UE) (ACS-DCP-11) and the Packet Gateway (PGW) to send and receive data. The components communicate between themselves on this dedicated user plane network. The traffic is terminated in the ABB Ability platform.

The ABB Ability Digital Powertrain provides end-to-end authentication and encryption of all data from ACS-DCP-11 located within the OT environment and to the ABB Ability platform (cloud). In cases where a second layer of security is needed, Azure Express Route is an option that provides an end-to-end private connection to the ABB Ability platform (cloud). Azure Express Route is as an additional service on request.

IEC 62443 – Securing Industrial Automation and Control Systems (IACS)



IEC 62443 is the de facto industry standard for securing operational technology (OT) systems, referred to as industrial automation and control systems (IACS) by the standard. Cyber security is defined by five core functions: Identify, Protect, Detect, Respond, and Recover. Building a cyber resilient system, according to IEC 62443, covers all these five areas, but the emphasis is on 'security by design' and the selection of appropriate cyber security protection mechanisms. Protection mechanisms are defined through Security Levels (SL), with associated security requirements specifying required capabilities to identify, detect, respond, and recover from cyber security events and incidents such as cyber-attacks.

IEC 62443 defines five Security Levels (SL), from SL0 to SL4, where SL0 means no security, while SL4 means resistance against nation-state attacks. SLs are essential in the standard and defined in detail in IEC 62443-3-3: System Security Requirements and Security Levels.

The following are the five security levels (SL) defined in IEC 62443-3-3:

- SL0: No security.
- SL1: Protection against accidental errors.
- SL2: Protection against intentional attacks with simple means and low resources and knowledge.
- SL3: Protection against intentional attacks with sophisticated means and moderate resources and knowledge.
- SL4: Protection against intentional attacks with sophisticated means and high resources and knowledge (nation-state attacks).

Furthermore, IEC 62443 comprises multiple documents across four categories: General, Policies and Procedures, System, and Component:

- General documents provide an overview of the industrial security process and introduce essential concepts for securing IACS.
- Policies and Procedures documents provide guidance on establishing policies and procedures to support an organization in securing IACS.
- System documents provide requirements to design and implement secure systems.
- Component documents provide requirements to design and implement secure industrial components.

General	**62443-1-1**	**62443-1-2**	**62443-1-3**	**62443-1-4**	
	Concepts and models	Master glossary of terms and abbreviations	System security conformance metrics	IACS security lifecycle and use-cases	
Policies & Procedures	**62443-2-1**	**62443-2-2**	**62443-2-3**	**62443-2-4**	**62443-2-5**
	Security program requirements for IACS asset owners	Security Protection Rating	Patch management in the IACS environment	Requirements for IACS service providers	Implementation guidance for IACS asset owners
System	**62443-3-1**	**62443-3-2**	**62443-3-3**		
	Security technologies for IACS	Security risk assessment and system design	System security requirements and security levels		
Component	**62443-4-1**	**62443-4-2**			
	Secure product development lifecycle requirements	Technical security requirements for IACS components			

The core general document is IEC 62443-1-1, which defines seven foundation requirements (FRs): FR1 – Identification and authentication control; FR2 – Use control; FR3 – System integrity; FR4 – Data confidentiality; FR5 – Restricted data flow; FR6 – Timely response to events; and FR7 – Resource availability. These seven FRs are the basis for defining security requirements in IEC 62443-3-3 for Industrial Automation and Control Systems (IACS) and in IEC 62443-4-2 for IACS components. IEC 62443-3-3 is a system document in IEC 62443, while IEC 62443-4-2 is a component document. IEC 62443-4-2 follows the same structure as IEC 62443-3-3, but rather than addressing the whole IACS system, it provides component requirements that specify security capabilities to enable an IACS component to mitigate threats for a given security level (SL).

The component requirements are split into four categories providing specific requirements to: software applications, embedded devices, host devices, and network devices:

- Software application requirements (SAR)
- Embedded device requirements (EDR)
- Host device requirements (HDR)
- Network device requirements (NDR)

Securing IACS components depends on fulfilling a set of security requirements but also requires that security is integrated into the development process. This integration provides security by design and ensures that security is addressed throughout the product life cycle. IEC 62443-4-1 defines Secure System Development Lifecycle (SSDLC) requirements for IACS components. Also, secure system development needs to be supported by a structured approach to security by the involved organizations, which is addressed in IEC 62443-2-4 as requirements to a Cyber Security Management System (CSMS).

Tampnet Cyber and Information Security Management System (CISMS)

Tampnet has implemented a Cyber and Information Security Management System (CISMS) with the purpose of facilitating a proactive, holistic, and systematic management of cyber and information security. The CISMS is the company's framework for establishing, implementing, maintaining, and continually improving cyber and information security.

The ISMS part of the framework is developed according to the ISO/IEC 27001:2017 standard and the principles of the NIST (National Institute of Standards and Technology) Cyber Security Framework (CSF) (version 1.1. April 2018).
The ISMS is technology neutral and supports a business risk-based approach. The CSMS part is developed based on IEC 62443-2-4 and focuses on operational technology (OT).

The following are some of the key governing documents relevant for Cyber and Information Security:

- Tampnet Cyber and Information Security Policy
- CISMS Scope
- Identification of Requirements
- Risk Management
- Classified Information
- Secure System Engineering
- Access Control
- Password
- Remote Access
- Physical Security
- Supplier Security
- Disposal and Destruction
- Acceptable Use of Assets
- Operations Security
- Incident Management
- Major Security Incident Procedure
- Backup and Restoration
- CISMS Performance Evaluation

The policies are regularly reviewed and updated.

Security controls related to General Data Protection Regulation (GDPR) privacy regulations are also covered and fully integrated with Tampnet’s CISMS.

ABB Motion ISO 27001 Information Security Management System (ISMS)

ABB Motion applies ABB corporate information security policies, standards, and guidelines using the ABB ISO 27001 certified information security management system (ISMS). ABB covers information security and cyber security within its governance framework. In the context of Motion, the main concern is the internet-facing solutions and cloud-connectable offerings. The secure software development lifecycle (SSDLC) is handled as part of the governance framework.

ABB cyber security requirements for building secure products and services

Cyber security for automation and control systems, specifically for critical infrastructure, has gained much attention in the last few years and is becoming increasingly important. Cyber security is a strategic topic in ABB.

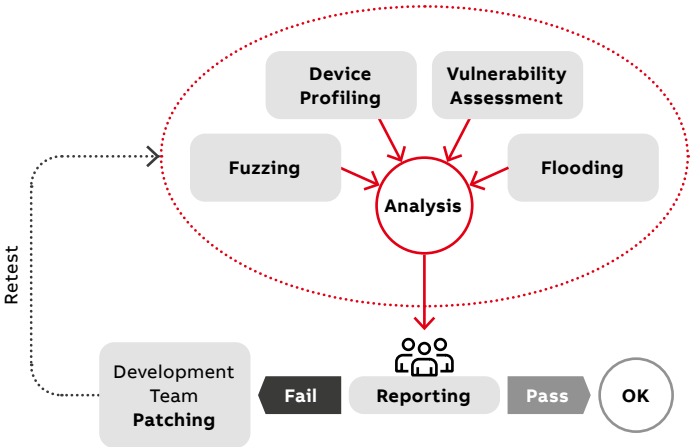
By understanding market conditions, customer needs, and the cyber environment, ABB strives to achieve the required levels of cyber security without compromising operational performance.

ABB solutions reduce business risk, providing comfort and confidence and enabling compliance with standards and legal requirements.

ABB's cyber security efforts aim to ensure compliance with relevant requirements within information security and cyber security. This work starts from the design table and continues to the operative phase of the product life cycle.

ABB Device Security Assurance Center (DSAC)

ABB has established a dedicated, independent security test center where its products are subject to security and robustness tests. A detailed test report and analysis are shared with the development teams to help them rectify detected vulnerabilities.



The objective of the Device Security Assurance Center is to provide continuous protocol-stack robustness and vulnerability assessments of embedded devices, enabling ABB:

- to supply customers with products that meet the highest robustness standards
- products and devices to comply with existing and forthcoming governmental and industrial regulations.

A suite of state-of-the-art open-source and commercial solutions are used for testing, including device profiling, known vulnerabilities, denial of service, and protocol fuzzing tests.

For more information about ABB DSAC, please see the separate white paper: Whitepaper – Device Security Assurance Center (DSAC)

Ericsson Security Reliability Model (SRM)

The Ericsson Security Reliability Model (SRM) ensures that all products systematically incorporate security and privacy considerations into all relevant aspects and phases of the product value flow. The SRM specifies four areas of security and privacy controls: Functions, Assurance, Compliance & Documentation, and Deployment & Operations.

Functions refer to the features that are required for each product. Assurance is about how to implement and verify products and solutions. Compliance & Documentation focuses on providing guidance for security and privacy in use. Deployment & Operations provides practices to ensure that security and privacy are maintained.

One of the core purposes of the SRM is to ensure compliance with relevant laws, regulations, and standards, and to provide security and privacy by design that is supported throughout the whole life cycle of a product. The SRM is supported by Ericsson's ISO 27001-certified Information Security Management System (ISMS) which supports SRM activities with controls for information and IT security. Furthermore, the SRM uses risk management to decide the most efficient and fitted information and IT security controls for a specific product.

A core part of the SRM is security and privacy by design which includes, amongst other aspects, building assurance that the final product is secure when running in its target environment. Assurance activities involve:

- Risk assessment
- Privacy impact assessment
- Secure coding
- Vulnerability analysis
- Hardening

For more information on vulnerability management, please refer to Ericsson's Product Security Incident Response Team (PSIRT), https://www.ericsson.com/en/about-us/enterprise-security/psirt. Ericsson uses the Development, Security, and Operations (DevSecOps) approach and integrates security into a Continuous Integration/Continuous Deployment (CI/CD) pipeline to ensure all security tests are performed through the pipeline with minimum human interaction. The goal is to automate as much as possible and to introduce security as early in the process as possible to catch and mitigate vulnerabilities efficiently. Automation includes different types of security tests including static code analysis, software composition analysis, and dynamic application security testing.


Condition Monitoring

IEC 62443-4-2 Compliance for ACS-DCP-11

IEC 62443-1-1 defines seven (7) Foundational Requirements (FRs) which in IEC 62443-4-2 are split into sets of component requirements (CR). The CRs address required cyber security capabilities associated with the four security levels defined in the standard: SL1-SL4, for software applications, embedded devices, host devices, and network devices.

The seven FRs are:

- FR1 – Identification and Authentication Control (IAC)
- FR2 – Use Control (UC)
- FR3 – System Integrity (SI)
- FR4 – Data Confidentiality (DC)
- FR5 – Restricted Data Flow (RDF)
- FR6 – Timely Response to Events (TRE)
- FR7 – Resource Availability (RA)

The following sub-sections provide a summary of the capabilities involved for each of the seven FRs for the ABB Drive Connectivity Panel ACS-SCP-11.

ABB Drive Connectivity Panel ACS-DCP-11

The ABB Drive Connectivity Panel ASC-DCP-11 is defined as an embedded device according to IEC 62443-4-2 and is evaluated to offer capabilities addressing SL2 embedded device requirements (EDR).

FR1 – Identification and Authentication Control (IAC)
Identification and authentication are essential for establishing SL2 and cover security capabilities needed to uniquely identify and authenticate human users, software processes, and devices, including associated management systems.

ACS-DCP-11 supports identification and authentication locally on the device and through the cloud solution. The cloud interface provides capabilities for the unique identification and authentication of human users and devices. An 8-digit PIN, which can be changed regularly, protects the device. Device authentication to the cloud uses X.509 certificates over Transport Layer Security, TLS 1.2.

FR2 – Use Control (UC)
Use Control (UC) focuses on the enforcement of authorization, permission control, and control of mobile code, remote access, and sessions. Additionally, UC includes requirements for audit record logging and audit storage control.

ACS-DCP-11 does not have a user concept but is protected by an 8-digit PIN code on the local user interface. Audit logs are supported locally on the device and are pushed to the cloud in regular intervals. The cloud interface supports authorization, permission control, mobile code protection, secure remote access, and session control, and fulfils the audit logging requirements.

FR3 – System Integrity (SI)
System Integrity maintains a device's integrity, including firmware and associated software, to ensure that the device does not change its behavior or permit data to be manipulated.

ACS-DCP-11 provides a secure boot process and supports integrity checks and secure upgrades of firmware. Integrity failures are logged as an event locally on the device and pushed as part of audit logging to the cloud.

FR4 – Data Confidentiality (DC)
Data Confidentiality concerns the protection of data from unauthorized access.

ACS-DCP-11 provides capabilities to protect data using an 8-digit PIN code that is needed to access the device locally, in addition to the use of cryptographic mechanisms. All use of cryptographic mechanisms is according to NIST standards and includes RSA 2048, SHA 256, and AES 256.

FR5 – Restricted Data Flow (RDF)
Restricted Data Flow ensures that data is only made accessible on the networks that it should be accessible. ASC-DCP-11 operates on an isolated network and is protected by an 8-digit PIN code. The cloud interface is segregated from the drive interface locally on the device by means of separate and dedicated interfaces.

FR6 – Timely Response to Events (TRE)
Timely Response to Events concerns monitoring and recording of security events and includes access to audit logs and continuous monitoring.

ASC-DCP-11 supports audit logging and audit logs are regularly pushed to the cloud where they are made available through a dedicated read-only interface.

FR7 – Resource Availability (RA)
Resource Availability includes capabilities such as backup and restore, ability to run in degraded mode in cases of security events, denial of service protection, and management of network and security configuration settings.

ASC-DCP-11 provides capabilities for backup and restore, including verification of backup before the restore can be performed. The panel also has resource availability protection capabilities.

References

1. IEC 62443 Security of Industrial Automation and Control Systems (IACS).
2. IEC/TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts, and models.
3. IEC 62443-2-4 Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers.
4. IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.
5. IEC 62443-4-2 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.
6. IEC 62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.
7. 3GPP TS 23.002 version 17.0.0 Release 17 – Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture.
8. ISO 27001:2017 Information Technology – Security Techniques – Information Security Management Systems – Requirements.
9. NIST Cybersecurity Framework (CSF). Version 1.1. April 2018.

Additional information
We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

For more information, please contact
your local ABB representative or visit

new.abb.com/service/motion

4MWA000084 REV A EN 19.4.2023