



CYBERSECURITY AT THE CORE

GCP100 Gas Chromatograph
Secure by design

WHY CYBERSECURITY IN INDUSTRIAL ANALYZERS MATTERS

Gas chromatographs (GC) play a vital role across the hydrocarbon processing industry, from natural gas operations to oil refineries and petrochemical plants, delivering the data that plant operators rely on to drive performance, safety and compliance.

As digitalization increases across industries, cybersecurity has become instrumental in protecting industrial devices – especially gas chromatographs. Legacy field device security features lag behind more modern equipment, which leaves space for malicious actors to exploit.

While cyberattacks are on the rise worldwide, the oil and gas industry especially has seen a striking spike in ransomware attacks. According to the cybersecurity firm Zscaler, these types of cyberattacks

on the oil and gas industry increased dramatically between April 2024 and April 2025, with a staggering 935.3% rise in attacks.

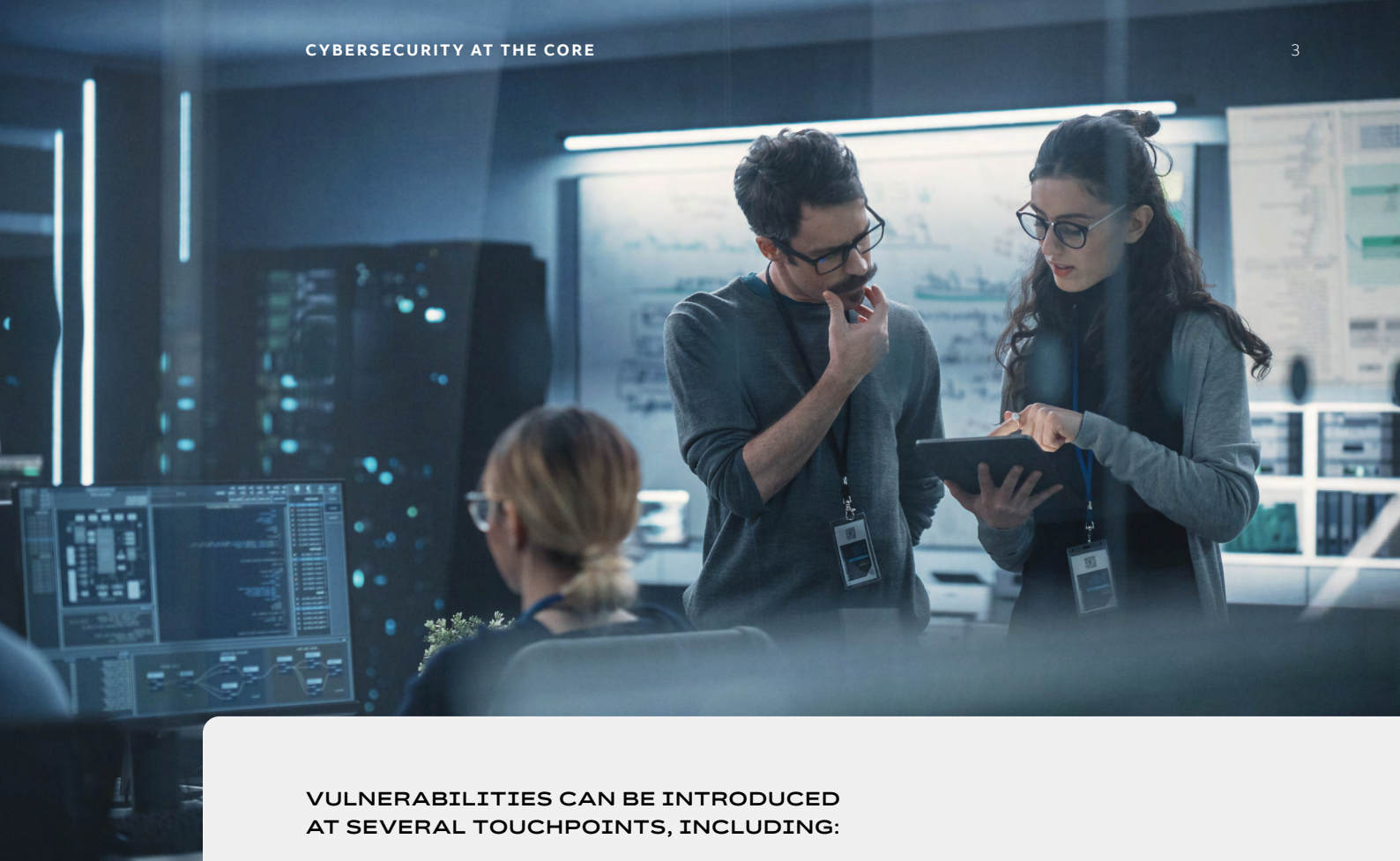
These vulnerabilities can put operations and intellectual property (IP) at risk in the race for data access and security. Cyberattacks targeting oil and gas operations can disrupt fuel supply chains, compromise public safety, and trigger cascading effects across utilities and customer services. The tight integration of operational and IT systems makes the sector especially vulnerable, turning each breach into a potential threat to national infrastructure.

If data is exposed, cyberattacks can reveal critical details about how a plant functions, turning gas chromatographs into attractive targets.



Ransomware cyberattacks in the oil & gas industry **increased 935% between April 2024–2025**





VULNERABILITIES CAN BE INTRODUCED AT SEVERAL TOUCHPOINTS, INCLUDING:



User missteps or negligence



Unreliable third-party connections

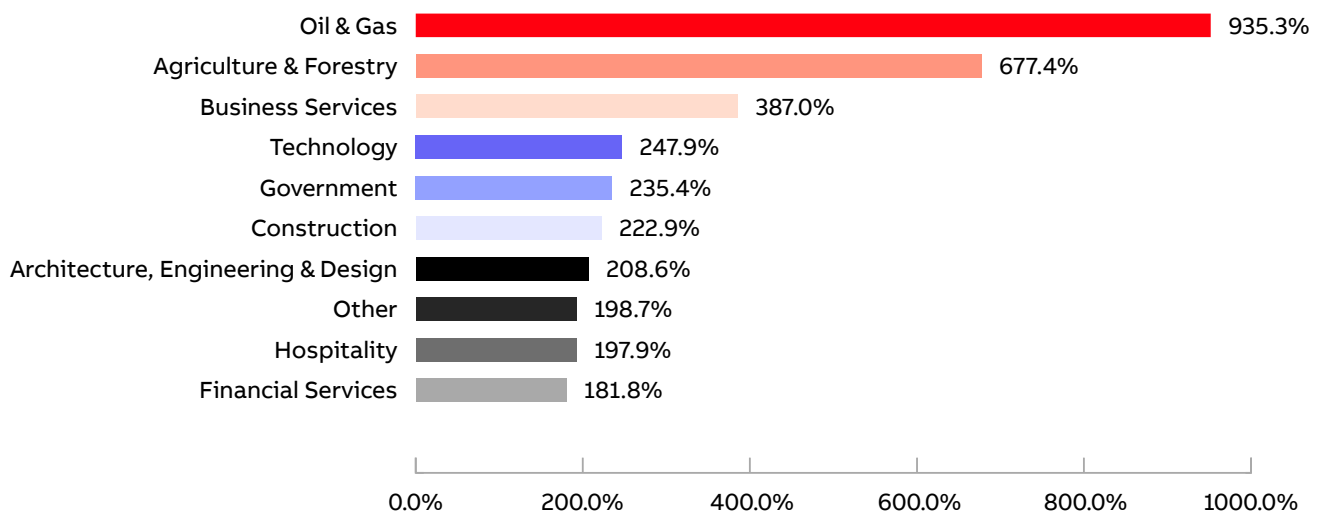


Software vulnerabilities including back-doors into a device/network



Weak points in network security

CYBERATTACK INCREASES VIA RANSOMWARE



01 Year-over-year percentage change in ransomware extortion attacks by industry. Source: Zscaler

Cyberattacks pose enterprise risks capable of compromising company viability, according to the American Petroleum Institute.

“Natural gas and oil companies recognize that their assets are the targets of a growing number of increasingly sophisticated cyberattacks perpetrated by a variety of attackers including nation-states and organized international criminals,” the API states in its article titled *Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry*.

Protecting GC systems with built-in resilience is essential to safeguarding business continuity and maintaining trust in industrial performance.

This paper outlines how built-in cybersecurity addresses the growing demands of industrial environments, offering a secure, compliant and easy-to-deploy solution for analyzer specialists, plant managers and IT decision-makers.

STRATEGIC CONTEXT OF INDUSTRIAL CYBERSECURITY

in digitalization infrastructure and adoption

Overall, the oil and gas industries at-large benefit from adopting modern solutions early. In today's digital age, no device exists without digital aspects, no hardware without software. Developing a complementary cybersecurity and digital strategy helps industries thrive, maintain operations and protect their most valuable resources – people, data and IP.

Installing the most cybersecure devices possible with all aspects accounted for, from hardware to software, operations to the operators, is an essential part of a sound strategy in today's industrial and digital landscape.

When defining a plant or even organizational cybersecurity strategy, it's common to apply a risk-based approach. This approach assesses the criticality of each asset, threats, likelihood of an attack as well as the consequences if a malicious attack happens. While there are a number of steps that can be taken to reduce the risk of an attack, for example increasing network security, improving monitoring and surveillance of data traffic, an overall upgrade plan to install modern cybersecure devices that feature continuous patch management will form an essential part of a lasting, successful strategy.

Gartner found in their report *2026 CIO Agenda for Oil and Gas: Technology Priorities and IT Strategy*

Shifts that **“cybersecurity is a top strategic priority for oil and gas CIOs.”**

As cyber risk now influences shareholder value, leadership teams are embedding security into business strategy and aligning cybersecurity strategy with business objectives, according to Gartner.

In addition to helping protect valuable information and data, digitalization also helps address labor shortages, unlock stranded data, improve productivity and meet evolving sustainability and regulatory demands.

That's especially why technologically advanced, data-rich devices such as gas chromatographs need the tightest cybersecurity advantages possible along with digital tools to support today's workforce, and to safeguard information, ensure continuous operations and to deter any would-be malicious actors.

Accentuating the need for building a robust cybersecurity strategy is another recent finding from Accenture in their report, *State of Cybersecurity Resilience 2025*.

“Only 28% of organizations embed security into transformation initiatives from the outset, leaving critical infrastructure exposed during modernization,” the Accenture report states.



LEGACY RISKS AND REGULATORY PRESSURE

Legacy GCs, designed in a different era, often lack encryption, secure access or patch management. These GCs have not been fortified with embedded cybersecurity, exposing infrastructure during configuration, data transmission and maintenance. Many still rely on unencrypted protocols like Modbus and lack secure boot, firmware signing or user-level access control.

GCs, like other field devices left to run to failure, are ripe targets, especially for well-funded malicious actors with evolving digital advancements, strategies and legacy device understanding. Securing these devices is critical to protecting operations, device availability, data integrity and corporate reputation.

A single compromised device can jeopardize an entire network, especially if other links in the chain lack modern cybersecurity enhancements and defenses. The ransomware and cybersecurity report from Zscaler mentions outdated security practices and increased digital and automated processes that lack proper cybersecurity measures.

Ransomware attacks are likely driven by a combination of increased automation that is inflating the attack surface along with outdated security practices.

While those attacks rose more than 900%, the amount of data stolen from victims between that same April 2024 to April 2025 timeframe also represented a 92% increase over the amount stolen during the prior year – adding up to **238 terabytes**.



Data stolen from ransomware cyberattacks in oil & gas industry between April 2024–April 2025

238 Terabytes (238,000 GB)
92% increase from prior year

In May of 2025, the Cybersecurity and Infrastructure Security Agency (CISA) warned that even “unsophisticated” threat actors are exploiting vulnerabilities

in industrial control systems (ICS) and SCADA technology “within U.S. critical infrastructure sectors (Oil and Natural Gas).”

“The presence of poor cyber hygiene and exposed assets can escalate these threats, leading to significant consequences such as defacement, configuration changes, operational disruptions and, in severe cases, physical damage.”

– the Cybersecurity and Infrastructure Security Agency (CISA) states

Furthermore, most of these issues are not discovered quick enough to keep pace with advanced cyberattack techniques, making monitoring of device and data even more important and regular patch deployment a must.

Upcoming regulations, such as the Cyber Resilience Act (CRA), will mandate that all connected products

sold in the EU are “secure by design” and routinely updated. Additionally, manufacturers must provide clear information on potential cyber risks throughout the product lifecycle. The CRA will take effect by the end of 2027 in the EU, and this approach could extend to other soon-to-be-implemented regulations around the world as well.

Simplifying stakeholder support

In a nutshell, today’s industrial operations and threat landscape demand a fundamentally different approach.

Evidence shows that upwards of 90% of security incidents could have been avoided by following basic security practices, according to the World Economic

Forum. As cyberattacks on industrial systems are rising, taking that figure to as close to 100% as possible is dependent on advanced devices with enhanced cybersecurity protocols.

Stakeholders benefit from a GC that simplifies security, meets compliance and reduces cyber incident risk.



STAKEHOLDER BENEFITS OF A CYBERSECURE GC



Security specialists: Fewer manual security tasks



Analytical specialists: Analyzer can be networked, ensuring peak process operation



IT experts: Easier compliance and monitoring



Maintenance managers: Reducing risk of unplanned stoppages & increasing availability



Operations managers: Significantly reduced risk of downtime with risks mitigated

With the potential for multiple operators within a plant, this widens the scope and potential for a field device to become vulnerable and exploitable through various methods.

Arming today's industrial workforce with proper cybersecurity infrastructure and protected devices is a necessary step forward to safeguard against evolving cyberattacks in the digital age.

GCP100'S SECURE-BY-DESIGN APPROACH



First gas chromatograph with built-in cybersecurity & encrypted communication



Certified by Device Security Assurance Center (DSAC) for secure communication protocols



Cybersecurity tested and compliant to IEC 62443-4-1 standard



Introducing the modern GC solution to fortify critical industries

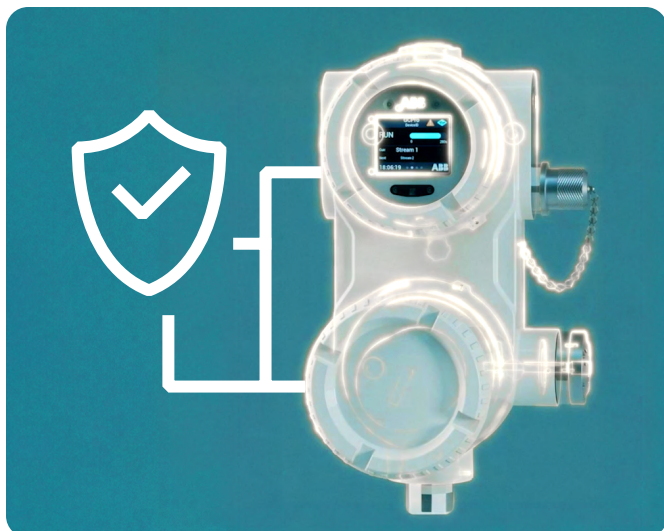


ABB worked to engineer a solution that both addresses legacy issues while also equipping industries with a future-proof solution.

The result is the new GCP100, the world's first gas chromatograph with built-in cybersecurity, designed to meet the most stringent industrial standards and regulatory requirements.

With a secure-by-design gas chromatograph, which builds on ABB's cybersecurity approach and architecture, the device provides built-in protection for information and users without external dependencies (such as total reliance on third-party firewalls).

Futureproofing the GCP100

When ABB developed the GCP100, the aim was to create a device that provided "built-in cybersecurity out of the box." This means that the device comes as standard with a number of secure-by-design features that help to protect the device itself, device data and the user from cyberthreats – all without requiring additional peripheral security solutions.

The legacy of ABB gas chromatograph engineering combined with a modern approach to cybersecurity and industry support means the GCP100 is built for the future. This approach is embedded into every industrial analyzer ABB engineers today.

As the first of its kind, the GCP100 features browser-based access and encrypted data transmission that meets standards, with architecture including:

GCP100 IS SECURE OUT OF THE BOX



Secure boot



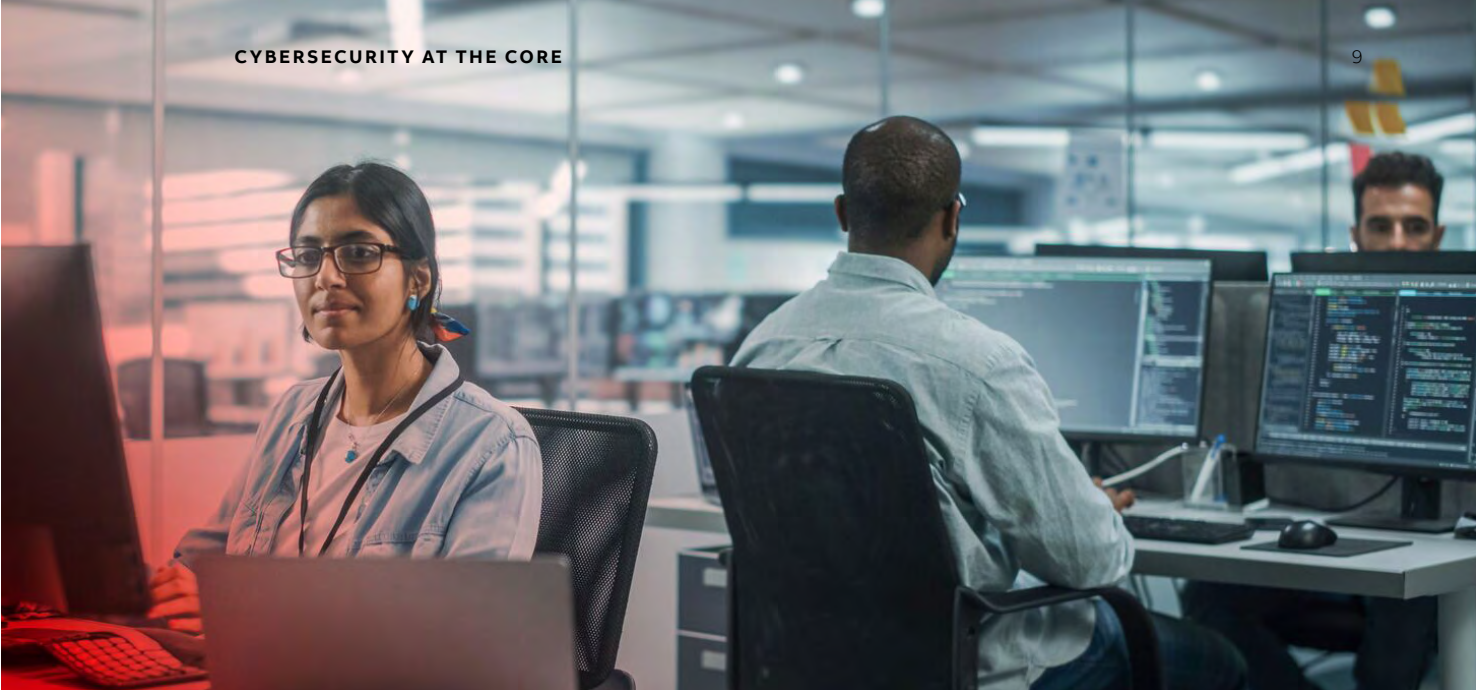
Signed firmware



Encrypted data channels and storage



Disabled-by-default communications



Engineered with a hardened architecture, GCP100 protects sensitive process data to prevent unauthorized code execution during startup. By encrypting data at the source and enforcing role-based access, it ensures that only the right people see the right information.

Integrating cybersecurity into every layer, from hardware to software, GCP100 eliminates common vulnerabilities and simplifies compliance with emerging regulations such as CRA, giving operators and IT teams confidence that their systems will remain protected, compliant and future-ready.

It is certified by ABB's Device Security Assurance Center (DSAC), which is certified to perform tests in accordance with IEC 62443-4-1. DSAC tests embedded devices, software and connectivity across platforms.

The American Petroleum Institute recommends aligning cybersecurity programs with ISA/IEC 62443 standards because they are built for oil and gas industrial environments. Certification helps ensure that devices such as gas chromatographs meet strict security requirements, protecting operations while supporting the industry's preference for collaboration over regulation.

Further strengthening its cybersecurity, the GCP100 is also equipped with a Dynamic QR code (DQR)

feature, which collects device data without a physical connection. This reduces the attack surface and supports secure diagnostics. Users can prompt the device to display a QR code that includes current diagnostic data and static details such as serial number, device type and software versions.

Scanning the code with a smartphone or tablet opens My Measurement Assistant+, where users can access documentation, lifecycle status, health reports and more. The QR code also supports cybersecurity audits by providing lifecycle and software version data. As regulations like the CRA evolve, My Measurement Assistant+ will offer deeper security insights to support IT and security teams for devices such as the GCP100.

Cybersecurity threats continue to evolve, and manufacturers and operators must treat device security as a core responsibility, not a feature. Applying this approach to the GCP100 is not unique, the same secure-by-design principles are applied in all ABB product developments. This shift means users, security experts and IT professionals can think of managing industrial devices like they do laptops, by monitoring risks, applying patches and keeping systems current.

It's a shared approach to resilience, built for today's threats and tomorrow's standards.

As part of its own cybersecurity and digitalization strategy, ABB deploys regular patch updates to address evolving threats and monitors systems for potential attacks as additional support to industrial partners.

ABOUT THE AUTHOR



David Lincoln, Global Digital Lead

ABB Measurement & Analytics

David Lincoln is the Global Digital Lead at ABB Measurement & Analytics. In this role, he is responsible for driving the digital transformation within the business. Amongst other things, he works on integrating Gen AI capabilities into ABB products for industrial applications.

A British native, David holds a Master of Engineering degree (MEng, Mechanical Engineering) from the University of Manchester and a PhD from Cardiff University / Prifysgol Caerdydd focused on flow measurement of electricity insulated liquids using electromagnetic fields.

More information

To find out more about ABB's next-generation gas chromatograph, the GCP100 with built-in cybersecurity, visit our [portal page](#).

And to go deeper on ABB's cybersecurity approach and implementation, visit our [cybersecurity page](#).

References

1. [2025 Ransomware Trends & Insights: Zscaler ThreatLabz Report](#)
2. [Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry](#)
3. [Unsophisticated Cyber Actor\(s\) Targeting Operational Technology](#)
4. [The Cyber Resilience Act, Explained](#)
5. [Ransomware attacks against oil and gas firms surge | Cybersecurity Dive](#)
6. [2026 CIO Agenda for Oil and Gas: Technology Priorities and IT Strategy Shifts](#)
7. [State of Cybersecurity Resilience 2025](#)
8. [World Economic Forum's The Global Risks Report 2022](#)

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 AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB AG.

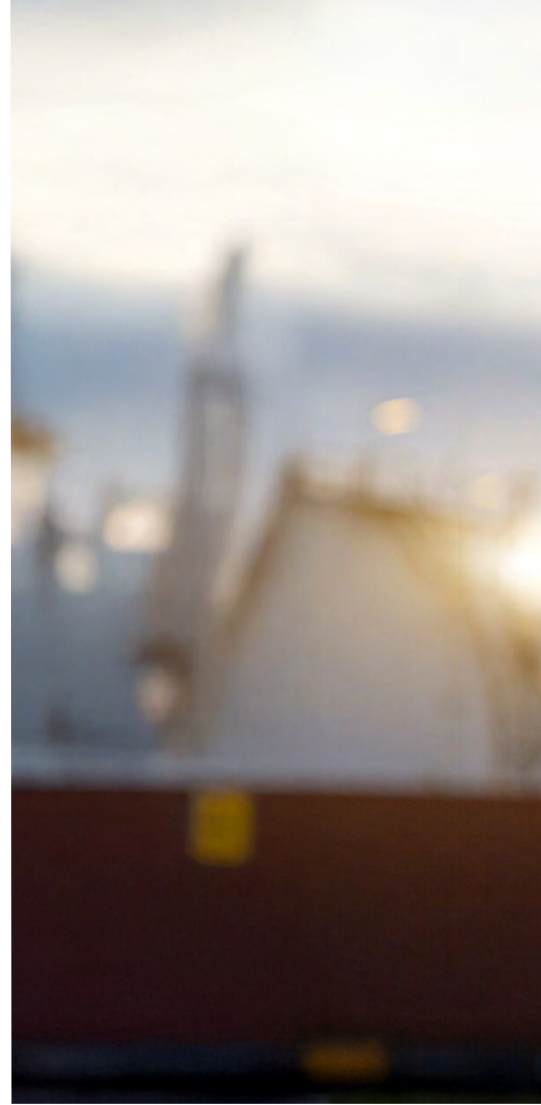


ABB Inc.
Measurement & Analytics

[solutions.abb/analytical](https://solutions.abb.com/analytical)

© Copyright 2025 ABB. All rights reserved.
Specifications subject to change without notice.