01. Global cyber security
02. The threat
03. ABB cyber security solutions
04. Process
05. FAQs
Global cyber security
Cyber security
An introduction

50% of large companies (10k+ employees) spent on average $1 M+ on security annually & another 43% spending $250k-$999k

97% Of businesses acknowledge security challenges because of the convergence of traditional information technology (IT) and operational technology (OT)

Exponential growth in the last 10 years has seen a 19% increase in the number of connected devices globally.

48% Of facilities say their team is inexperienced in Cybersecurity. While recruiting individuals with relevant expertise is an industry-wide challenge.
Industrial systems face elevated cyber security risks

Key risk factors
- Distributed systems
- Asset Complexity & Age
- Insufficient security visibility
- Insufficient Security awareness
- Process complexity
- Insufficient security expertise

Potential impacts
- Lucrative and attractive target
- Production losses
- Non-compliance costs
- Health and Safety
- Reputational Damage

Health and Safety
- Environmental
- Production losses
- Non-compliance costs
- Reputational Damage
The threat
Cyber security for operational technology
A short list of threats. Is this just a theory?

1. One field device gets manipulated or disturbed
2. Measurement data (traffic) spied
3. Measurement data (traffic) is manipulated
4. Automation network disturbed (control loops)

5. Device is used as part of botnet (compromising whole IT/OT infrastructure)
6. Cybersecurity is a moving target
Cyber security for analyzers
Some threat examples

1. The accepted safety limits on a device are changed so that emission limits are exceeded OR pressure warning not alerted risking serious damage

2. Data could be made public that could damage the company and impact share prices

3. Measurement data is manipulated to trick the company into thinking they are compliant

4. Performance of safety system compromised

5. Botnet attack stopping all site operations for indeterminate period

6. Cyber attacks are changing and becoming more intelligent – the future risk is unknown
Ideal system specification vs. threats

**Cyber security Requirements**
- Defined set of requirements conforming to best practices
- Incorporated in every step of device development
- Cybersecurity requirements and checking of supply chain (incl. software, engineering)

**Secure Boot**
- Public/private keypair for integrity protection of firmware
- Firmware on device is signed during development process
- Bootloader checks signature during start-up.

**Cyber security Testing**
- Extensive vulnerability testing in accordance with known standards
- Fault injection
- Flooding
- Fuzzy testing and more

**Password protection**
- Encrypted storage of password
- Password can (and shall) be changed by the user – described in instruction manual
- Dedicated password reset procedure

**Secure communication**
- Migration towards new protocols with integrated security protocols
  - OPC-UA as backbone of Industry 4.0
  - HTTPS to secure configuration of device?

**Customer care**
- Security alerts, notifications
- Incident management
- Trainings, webinars and workshops
- Continuous improvement of requirements and processes
- Patch management for software
What is your risk tolerance?

The cost of cyber security is more than just analyzer repair

$11k-175k/unit
Physical Cost of Repair
- Replacement parts per analyzer OR a new system + labor $7-150k
- Internal resource to investigate, recover & support $4-50k

$300k-1M
Unplanned Production Downtime
- Avg. 3-5 days of analyzer(s) associated production downtime
- Production loss$$$$
- Employee productivity cost $$$
- Retrospective network security strengthening cost $$
- Customer production contract breach penalties $

$10k-$33M
Regulatory & Customer Fines
- Depending on the kind of incident & whether there is a breach of critical infrastructure security regulations or environmental regulations, the resulting fines vary greatly
- $33M for failing to surrender sufficient allowances for under-reporting emissions
- $5.6 million failing to investigate original alerts, using outdated software systems & lack of staff training

$8-$90m
Reputational Damage & Ransomware payouts
- Environmental scandals cause major reputational damage regardless of fault
  - A UK Power Generation Company lost 20% of its customers the year following their emissions scandal
  - A global technology company had a 3.8% share price drop following their breach (2020) & a 6.7% drop across the week following their fine being issued (2023)

*Based on a $100-200k production loss cost per day."
Measurement & Analytics cyber security risk reduction
A tailored service solution to reduce risk

Identify areas in automation that may be vulnerable to cyber attacks

Protect assets by segmenting, hardening and implementing necessary controls

Review traffic logging to identify any unauthorized traffic in event of an incident

Support on-demand to a cyber attack that comprises analyzer systems

Recover faster from a cyber event with rapid asset repair

Part of Measurement Care Agreement
ABB Secure Network Service
Benefits

A simple, robust solution to increase your cyber security, giving you peace of mind.

**Improved Cyber Security**
- Ensuring the protection of data and system components
- Service identifies and mitigates potential cyber security risks
- Regulated network traffic

**Cost-effective**
- Reducing costs with a customized solution to fit your exact needs
- Risk assessment and remediation services are free of charge

**Customized and Easy-to-Maintain Network Segregation**
- Improving overall system resilience
- The service offers tailored network segregation solutions that are easy to maintain

**Robust Firewall Protection**
- Enhancing the system’s defense against cyber threats
- A secure firewall with long-term firmware support is available upon request
- Interactive GUI

**Minimal Disruption to Operations**
- Ensuring a seamless integration of the upgraded security measures
- Designed to reduce disruption
ABB Secure Network Service
Safeguard your investment with Secure Network Service

Product focus
ACF-NT Multi-component emission and process monitoring system (Obsolete System)

Protect your investment
The security of the ACF-NTs can be critical to operations, and we know that replacing them isn’t the first-choice solution. The outdated operating system can’t be upgraded due to certification, posing a potential security risk. At ABB, we have designed the Secure Network Services specifically tailored to safeguard your systems. We help minimize the risk and ensure your operations remain efficient in this transition period for your CEMS systems.

Approach
IDENTIFY: We provide a comprehensive survey and evaluate the status of the network configuration
PROTECT: We implement a robust preconfigured firewall to manage network traffic securely. With yearly subscription service including beneficial firmware upgrades and security patches available. Operational training required is provided as necessary.
DETECT: Optional service in the event of an incident, review logging as part of investigation
RESPOND: Optional service support to respond and assess the results of a compromised system
RECOVER: Optional stocking of required parts in the event of an incident and resulting repair
ABB Secure Network Service

The process

- Users may be unaware of potential risks in their network configuration
- Vulnerable parts are usually not well protected

Configuration & Demand survey
- Online surveys are available for on-site service engineers to complete to understand the current network setup to determine correct product solution
- Risk assessment
- Meetings will be held to identify potential risks and the demand for protection

Customized quotation
- Complimentary assessment
- Customized quotation will be provided based on specific use case
- Additional security measures are available upon request

Approval
- Finalizing agreements
- Finalizing subscription

Commission
- Designed to reduce disruption
- Easy-to-Maintain solution

- Provide a temporary plan for minimizing risks, without any additional cost
ABB Secure Network Service

A typical multi-ACF-NT configuration example

Risks:
1. Unprotected connection – Vulnerable components may be exposed during maintenance.
2. Serial connection – When targeted all ACF-NT systems and other 3rd party ethernet enabled systems could be infected.
3. Unregulated connection – The firmware of these devices could be outdated, posing a risk to the internal network. It is also common for the Micro-Edge to permit external connections, potentially exposing devices within the internal network.
ABB Secure Network Service
Solution example

Benefits:

- Segregate ACF-NT systems from the customer network to reduce risk of malware propagation
- Installing a firewall blocking unnecessary communications from the ACF-NT systems
- Enable logs within the Firewall to monitor traffic flows
- Install network switch box to enable remote troubleshooting in emergencies
- Provision port on firewall to connect to ACF-NT systems during routine service
ABB Secure Network Service
Summary

1. **NO SUCH THING AS 100% SECURE**
   - Cyber security is a risk management process where the focus should be on reducing the risks of a cyber security incident and additionally reducing the impact if an incident occurs. It is not a 100% guarantee.

2. **SECURE NETWORK DESIGN IS KEY**
   - By segregating networks like ABB Secure Network Service does, the risks of attack and potential impacts such as proliferation through your network can be minimized.

3. **A CHAIN IS ONLY AS STRONG AS ITS WEAKEST LINK**
   - An assessment of devices within a network can help to identify weaknesses that could compromise the security of your plant, these weaknesses can be reduced.

4. **RISKS OF ATTACK ONLY INCREASE**
   - There are countless well publicized examples of cyber security attacks which have damaged property, created production outages, ransom requests, fines by governments & often irreparable brand damage.
Identify Risk Assessment FAQ

What is it?
A survey to categorize the type of installation of the ACF-NT at customer sites & identify any potential cyber security risks based on this configuration.

What problem do we address?
The survey provides a quick way to find out if there are any obvious weaknesses in the network setup based on the ACF-NT.

What do I (customer) have to do?
Work with ABB team members (sales & service) to complete the survey including understanding the current network setup.

Is there any risk to my production?
The survey is mostly offline & inspection based. It does not require any interference with the network or analyzers risking production. Just checking of IP addresses.

Why should I care?
The majority of cyber incidents can be avoided by applying basic cyber security. The risk assessment survey will help detect areas where the defenses are weak.

Benefits
- Better understanding of network setup
- Quickly see any major cybersecurity risks based on the use of obsolete ACF-NT technology
- Designed for ABB analyzer systems

What can/will happen if I don’t?
The system may be at risk from an unknown cyber weakness that could have been easily corrected.

How much work is involved?
The survey will take about 1 hour onsite, then there will be another few hours of behind-the-scenes work preparing your consult results.

What is the deliverable?
An assessment of the network with complimentary consultation addressing high-risk steps and a quote for overall system improvements.

Which systems does it work on?
The service is currently designed for ACF-NT systems with the roadmap to expand to other ABB analyzers soon.

How is it deployed?
Your ABB sales will talk to you about this new product opportunity. An ABB service member will support site survey and later the installation.
Identify Consultation FAQ

What is it?
Based on the survey results, ABB will make a series of recommendations to improve your network security.

What problem do we address?
Learning about any potential weaknesses in your current network setup and getting a solutions to remedy them.

What do I (customer) have to do?
Meet with you ABB contact to go through the results of your survey. You will then need to make the decision on what suggestions you action and whether to enter into an ABB Secure Network Service Agreement to improve your cyber security.

Is there any risk to my production?
Our recommendations will not stop production, but they might require access to the analyzers.

Why should I care?
The majority of cyber incidents can be avoided by applying basic cyber security. ABB Secure Network Service helps align your network with IEC protocols.

Benefits
- Complementary course of actions for high-risk concerns to action ASAP
- Designed for your system solution to upgrade your cyber security
- Designed for ABB analyzer systems

What can/will happen if I don’t?
The system will be at risk from known cyber weaknesses that could have been easily corrected. In the event of an incident linked to ACF-NT’s your company would be liable.

How much work is involved?
This will depend on the results of the assessment and how your network is set up. The installation portion of the ABB Secure Network Service is a quick process.

What is the deliverable?
An action plan for immediately addressable risks and a quote for an ABB Secure Network Service solution.

Which systems does it work on?
The service is currently designed for ACF-NT systems with the roadmap to expand to other ABB analyzers soon.

How is it deployed?
The immediately addressable actions can be discussed and we can support you in their completion if needed. The quote will be provided with all the details you need for the SNS & any additional ABB products & services you might be considering.
Protect
Firewall Security Updates FAQ

What is it?
Annual update to the firewall ensuring ongoing network security

What problem do we address?
Keeping the network up to date with the latest software and firmware versions

What do I (customer) have to do?
Arrange with Service Contact for annual update to system. This can be coordinated with other service needs of your system.

Is there any risk to my production?
The update to the firewall does not interfere with the operation of the analyzer.

Why should I care?
Keeping the system up to date is important for ensuring your ongoing cyber security. Cyber threats are changing constantly, by updating the system, new threats can be better accounted for. Most reported cyber attacks happen because systems are out of date.

Benefits
• Up to date system to reduce threat of new developments in cyber threats
• Continued cyber security safety

What can/will happen if I don’t?
Whilst the segregation of network with the current firewall will still provide enhanced security compared to having nothing, the risk of will be higher from newer forms of threat.

How much work is involved?
Prepare the firmware image in advance. The estimated time for commissioning or performing the annual update of the firewall is about one day.

Which systems does it work on?
The service is currently designed for ACF-NT systems with the roadmap to expand to other ABB analyzers soon.

How is it deployed?
Your service team, or ABB engineer, will arrange annual visits with you. They will need access to the firewall setup.
**Protect Training FAQ**

**What is it?**
A catalog of cyber security training focused on industrial systems created by skilled educators with a background in industrial cyber security.

**What problem do we address?**
Educate industrial customers as to the importance of cyber security.

**What do I (customer) have to do?**
Determine what level of training, if any, is required and schedule time for cyber security training for all relevant employees.

**Is there any risk to my production?**
There is a considerable risk if the personnel doesn't understand how cyber security affects all of the production and how all must work together.

**Why should I care?**
General cyber security awareness has the potential to reduce the risk considerably by stopping malicious activity before it starts.

**Benefits**
- Better understanding of the importance of cyber security safety
- Smarter employees making more secure cyber security decisions

**What can/will happen if I don’t?**
Example: an employee may not understand that plugging in an unknown USB device may jeopardize the whole system.

**How much work is involved?**
The online webinar for customers is 1h and can be viewed in your own time.

**What is the deliverable?**
Increased understanding what cyber security is, how it affects all of us, and how we can all help.

**Which systems does it work on?**
Our cyber security classes may be targeted for industrial use, but the knowledge and skill is applicable to all in many situations.

**How is it deployed?**
Online webinar that the team can give you access to.
**Detect, Respond, Recover**

**Incident response as part of MCA**

**What is it?**
Measurement Care is a service agreement tailored to you and your business needs. For ABB Secure Network Service, we can offer access to our Cyber Security Experts for reviewing traffic logging & investigating your incident, stocking of relevant spare parts based on your system, and engineer hours for completing the repair.

**What problem do we address?**
Ensure the resources will always be on hand to help you in the event of an incident limiting cost and consequences.

**What do I (customer) have to do?**
Speak to your ABB contact about starting or amending your My Measurement Care service agreement. An agreement can cover as little or as much support for your analyzers as needed.

**Is there any risk to my production?**
Yes – there is considerable risk to your production in the event of an incident. Having a My Measurement Care agreement can reduce your downtime by 1-3 days depending on location and service availability.

**Why should I care?**
Your response to an incident can help limit repercussions, get your operation back online sooner and limit the costs.

**Benefits**
- Reduced downtime in the event of an incident getting operations back online sooner
- Assistance with your incident investigation by product experts

**What can/will happen if I don’t?**
There may be delays in getting your system repaired and operational again in the event of an incident.

**How much work is involved?**
My Measurement Care agreements are flexible and designed to supplement the work required that you don’t have internal resources to do such as routine maintenance and technical support. So the work involved is up to you and your business needs.

**Which systems does it work on?**
Our cyber security classes may be targeted for industrial use, but the knowledge and skill is applicable to all in many situations.

**How is it deployed?**
A My Measurement Care agreement is managed by your local ABB Service agent.