



“
A single hour of
downtime in critical OT
systems can cost millions

Cyber Security in OT (Operational Technology) Resilience Services

The increasing interconnectedness of industrial control systems and the rise of sophisticated cyber threats pose significant risks to industries.

We address these challenges by providing comprehensive solutions to identify vulnerabilities, mitigate risks, and protect industrial control systems from cyber threats.

Your Challenges



Rise of cyber attacks

Breaches in Operational Technology (OT) can lead to disruptions in operations, financial losses (such as business interruptions or investigation costs), potential safety risks, and even physical harm.



Increased attack surface

The growing connectivity of industrial control systems (ICS), SCADA and information technology (IT) creates new entry points for cyber threats.



New regulatory requirements for Operational Technology

With the NIS2 directive, more businesses and sectors using OT and industrial control systems must demonstrate that cyber security measures are taken to enhance cyber resilience on the long run.

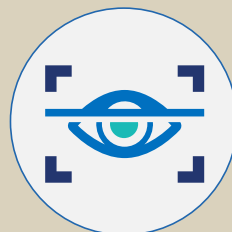
Your Benefits



**Strengthen NIS2
Technical
Compliance**



**Identify and
Mitigate Threats
and Vulnerabilities**



**Monitor, Detect and
Response to Cyber
Threats**



**Evaluate Incident
Readiness**



OT Security journey



OT Security is much more than deploying sensors to monitor for network anomalies



Risk Assessment and Technical Compliance

- Identify OT environment threats
- Assess security maturity against IEC 62443 and our in-house industry benchmark
- Develop a non-disruptive security strategy
- Prioritize Health, Safety, and Environmental (HSE) considerations
- Receive actionable recommendations and a roadmap for implementation
- Ensure high availability / system resilience
- Achieve compliance with NIS2 directive or CRA (Cyber Resilience Act) for equipment

OT Security Testing



- Simulate real-world attacks to test your resilience and existing controls
- Identify technical vulnerabilities
- Obtain tailored remediation strategy
- Improve awareness through security trainings and simulations



OT Monitoring & Incident Response

- Monitor operational processes and systems 24/7
- Detect and analyse potential threats in real-time
- Implement advanced detection and response with Claroty or Nozomi
- Integrate with existing IT and OT infrastructure

Incident Plan & Crises exercises



- Develop a robust Incident Response Plan
- Simulate incidents on OT Systems
- Test readiness to detect, mitigate and restore operations quickly
- Identify gaps, improve response strategy
- Minimize downtime and operational impact





Cyber x Industry Experts

We combine Cyber and Industry Engineers to secure critical infrastructure, optimize operations, and ensure compliance.

Cyber Experts



Vivien Bilquez

Global Head Cyber Resilience
vivien.bilquez@zurich.ch



Sylvain Luiset

Head of Cyber Resilience CH
sylvain.luiset@zurich.ch



Jean-Hermann Ly

Cyber Risk Engineer
jeanhermann.ly@zurich.ch



120 Cyber Engineers worldwide

ZRS Industry Experts



Manufacturing



Energy & Utilities



Oil & Gas



Transportation & Logistics



Water & Waste Management



Construction



Chemicals



Pharma & Healthcare



1000 Risk Engineers worldwide in Manufacturing, Energy & Utilities, Oil & Gas, Transport & Logistics, Pharma, Healthcare, Food & Beverage, Chemicals, Mining & Metals, Water, Agriculture and Construction.



Contact us

cyber.resilience@zurich.com

Why Zurich Cyber Resilience Solutions?



Support to improve insurability



Combining claims data and industry benchmarking



Service packages tailored for every business size and their needs.



Team of Cyber Specialists combined with Industry Risk Experts



Global presence for remote and on-site solutions



This is a general description of (insurance) services such as risk engineering or risk management services by Zurich Resilience Solutions which is part of the Commercial Insurance business of Zurich Insurance Group, and does not represent or alter any insurance policy or service agreement. Such (insurance) services are provided to qualified customers by affiliated companies of Zurich Insurance Company Ltd (Zurich Insurance Group). The prices stated are exclusive of VAT and are subject to change at any time.

The opinions expressed herein are those of Zurich Resilience Solutions as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any members of Zurich Insurance Group as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group.

Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy.

This document may not be distributed or reproduced either in whole, or in part, without prior written permission of Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.

Zurich Resilience Solutions

Release date: January 2025