OTORIO

HSB
A Munich Re company

Mitigating Cyber Risk for Operational Resilience

Uniting IT-OT Risk Management and Insurance for Business Success

White Paper

Table of Contents

OTORIO and HSB Joint Statement

Critical infrastructure and manufacturing have become increasingly reliant on OT connectivity. However, major gaps in risk preparedness, outdated risk mitigation approaches, and misaligned priorities by IT and OT teams prevent these industries from effectively addressing vulnerabilities. This increases risk, prevents the proactive power of advanced visibility of risk, and devalues good IT and OT current collaborations. All of this leads to more threat successes, more downtime, and more costs.

Operational resilience is crucial for cybersecurity risk management in OT environments. It is one of the most prevalent and least understood issues industrial organizations face, with potential consequences of disrupting business operations and causing financial loss.

Through its collaboration with OTORIO, HSB is applying 157 years of engineering and risk management experience to educate, manage, and ensure operational resilience against the imminent threats posed by connected industrial systems and ensure operational efficiency.

OTORIO delivers OT security and digital risk management solutions that ensure reliable, safe, and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial cybersecurity experts with cutting-edge digital risk management technology to provide the highest level of protection to critical infrastructure and manufacturing industries.

HSB is an A++ insurance company and fully-owned subsidiary of Munich Re Insurance, the largest reinsurer in the world. HSB is the leader in equipment breakdown insurance and has a deep background in understanding how physical assets and connected IoT systems perform, produce, and fail.

Introduction

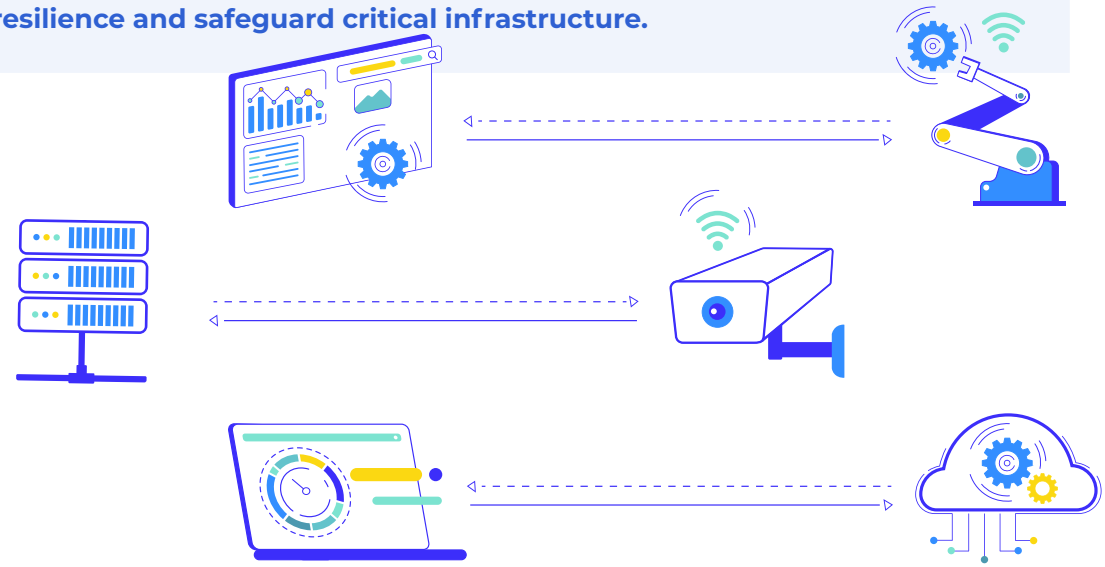
As today's IT and OT landscape continues to evolve, risk management approaches must progress to keep pace with the current challenges. The attack surface has expanded, and traditional security solutions cannot handle increasingly sophisticated threats. While the manufacturing, utilities, and energy industries are particularly sensitive to attack, all industries are susceptible. Any compromise of highly specialized systems can seriously affect safety and operations. Siloed OT environments have become dynamic risk environments that cannot be protected effectively by traditional IT security techniques.

Lack of integration between IT and OT systems challenges OT/IT risk management. Critical infrastructure was often designed without regard to IT and OT security, leaving these systems vulnerable in an attack. Organizations often need help to keep pace with the rapid changes and the ensuing risks created by rapid digital transformation.

Ensuring operational resilience leads to improved preparedness, response, and recovery from disruptive events, which is critical for a dynamic risk environment and to reduce insurance risk.

This unique risk-reduction approach to achieving operational resilience brings to the forefront the need to understand the operational context and business impact of risk consequences.

This whitepaper will address the key differences between IT and OT approaches to cyber risk and offer best practices to bridge these gaps for effective OT/IT risk management, emphasizing the importance of operational resilience for businesses. Through real-world examples, it will highlight the risk of business disruption resulting from an attack on the operational environment and provide recommendations for implementing and integrating industrial-native solutions to mitigate risk, ensure operational resilience and safeguard critical infrastructure.



Risk Management Challenges

In the past, Information Technology (IT) and Operations Technology (OT) were treated as separate domains within the larger field of Data Management. IT and OT were historically supported by separate organizations and matured independently.

However, with the rapid evolution of the industrial and informational landscape, the old model of distinct "chapters" has given way to a more interconnected approach. This evolution may be taking longer in the OT world because of the longer useful life of OT equipment and the large install base of older equipment.

The convergence of IT and OT also introduces new questions from an architectural point of view:

- Where do IT and OT intersect, and what new vulnerabilities does this create?
- Why is it important to manage the risks associated with this new paradigm?
- Who can serve as a trusted advisor to provide guidance on collaboration, interpretation, risk mitigation, and warranties?

At HSB/MRe and OTORIO, we've asked ourselves the same questions as our insurance customers: In response, we've created this paper to offer insights from the industrial perspective in general, and from the manufacturing, utilities, and renewable energy sectors specifically. After reading this paper, you should gain a better understanding of how to integrate IT and OT, as well as ideas on how to manage risks within your own operations. We also provide information on how to ensure your Process Control System (PCS) and Supervisory Control and Data Acquisition (SCADA) networks are secure against unauthorized access by scanning for vulnerabilities and offering guarantees against potential security breaches such as open doors, backdoors, loopholes, and other entry points for malicious actors.

Manufacturing

- If **Programmable Logic Controllers (PLCs)**, the equipment they sit on, hardwired or magnetic sensors, and other such hardware comprise the OT physical highway, then the configuration and variable data that runs on them is the IT turbo. There is no longer just Edge and Enterprise (behind the firewall) – there is also the space between them. This is also an area where the useful life of equipment can extend 40 to 50 years. The challenge is to integrate both newer and older equipment into a common security system.
- This is precisely where there must be oversight, understanding, monitoring, and clear play on where data is at any given time, much like trap doors that close shut behind each passage.
- Today's **complex control and ERP systems** require multiple vendors to service, patch, update, or replace them continuously. Because vendors come and go, this leads to uncertainty and poor visibility, which makes it challenging to ensure optimal performance and efficiency.

Utilities

- **Smart grids** are modern electrical grids that use IT systems to manage and distribute energy more efficiently. An attack can **lead to power outages, service disruptions**, and equipment damage.
- **SCADA systems** are used to monitor and control industrial processes in the utilities sector, such as water treatment plants and power generation facilities. A cyberattack can lead to **operational disruptions, safety hazards, and equipment damage**.
- **Microgrids** are connected to centralized national grids but are able to function independently. An attack can cause a disruption of power supply, data breaches, and equipment damage.

Renewable Energy

- **Wind turbines** have control systems that are used to optimize the efficiency and power output of the turbines. Cyberattacks could lead to operational disruptions, data privacy, safety hazards, and potential damage to the equipment.
- **Solar panels** have monitoring systems that are used to track the energy output and performance of the panels. Cyberattacks could lead to operational disruptions, data privacy, safety hazards, and potential damage to the equipment.
- **Hydrogen** production, transport, and distribution will each have unique vulnerabilities associated with their processes. Cyberattacks could lead to supply interruptions, safety and environmental hazards, and potential damage to equipment.
- **Hydro systems** monitor the efficiency and power output of the turbines, as well as the distribution of electrical power into the grid. Cyberattacks could lead to operational disruptions, data privacy, safety hazards, and physical damage to the generating and distribution equipment.
- **Energy storage systems** provide electrical power to equipment when the grid is not connected or is unavailable. Cyberattacks could lead to operational disruptions, safety hazards, and potential damage to the equipment.

IT-based security systems may not work to protect OT-based systems for the following reasons:

- IT and OT systems have **different security priorities**. IT systems typically focus on confidentiality and data protection, while OT systems prioritize efficiency, availability, and reliability. This means that security measures that work well for IT systems may not be appropriate for OT systems.
- IT and OT systems have **different architectures and requirements**. OT systems typically involve specialized equipment and proprietary protocols that may not be used in IT systems.
- OT systems are often distributed and have a large number of endpoints, making it **difficult to gain full visibility into the system**. This can make it challenging to identify potential security threats and respond to them in a timely manner.
- OT systems are often older and have **limited resources**, which can make it difficult to implement modern security measures. For example, many OT systems do not have the processing power or memory to run antivirus or other security tools.
- OT systems are often **highly complex**, with multiple interdependent components, often from separate vendors, that must work together to ensure system availability and reliability.

Reducing Insurance Risk with an Industrial-Native Approach to OT Security

OTORIO and HSB provide an agnostic industry approach to assessing and managing OT security risks and ensuring operational resilience.

The OTORIO Industrial-native risk management platform is specifically built for discovering and protecting operational technology (OT) and understands the unique requirements of the OT environment. This includes OT systems in critical industries such as manufacturing, utilities, and energy. The platform differs significantly from traditional IT security systems that typically secure data centers and office networks.

HSB/MRe has a long history and deep understanding of a wide range of equipment, systems, and infrastructure optimal uptime guarantees and analysis of equipment breakdown failure. Combining this dual industry expertise empowers Industrial organizations with superior protection of OT assets. The collaboration presents a uniquely strong and unchallenged value chain in the OT industry security solution space that reduces insurance risk and offers unparalleled benefits to the insured.

To reduce cyber risk, security practitioners must have complete visibility and control over their OT systems. As the digital transformation of industrial organizations advances, Industrial organizations evolve further into multi-vendor OT environments with multi-generation industrial and security systems. In such complex industrial environments, it is challenging to maintain real-time visibility of asset inventory and the industry protocols used by each OT system.

Industrial-native platforms are designed to integrate with existing OT systems to monitor and secure the entire OT network. This seamless integration minimizes disruptions and downtime that could lead to safety risks, equipment damage, delays in production, and financial loss while ensuring that organizations comply with OT industry-specific regulatory requirements.

The Benefits of Industrial-Native Platforms for OT Security

As outlined above, OT systems require specialized security solutions to meet their needs. Industrial-native solutions can provide monitoring, threat detection, and incident response capabilities that are capable of effectively protecting OT systems. They can enable critical infrastructure to function undisrupted, even in the event of a security incident or system failure.

The benefits of industrial-native platforms include:

Security
Industrial-native platforms have advanced security measures, such as encryption, authentication, and access controls, to prevent unauthorized access and protect sensitive information.

Reliability
Industrial-native platforms are highly robust and reliable, allowing for continued operations even when there has been a breach and minimizing costly downtime.

Visibility
Industrial-native platforms have advanced analytics to enable data monitoring and analysis in real time. This makes for more informed decision-making and improves efficiency, thereby optimizing performance.

Integration
Industrial-native platforms are designed to integrate with existing control systems, sensors, and industrial equipment, streamlining operations and reducing manual processes.

Scalability
Industrial-native platforms can be scaled to manage large volumes of data and adapt to the evolving needs of industrial settings.

OTORIO Case Studies

Face emerging cyber threats with newfound confidence and an advanced, dynamic toolbox that protects uptime and safeguards business continuity.

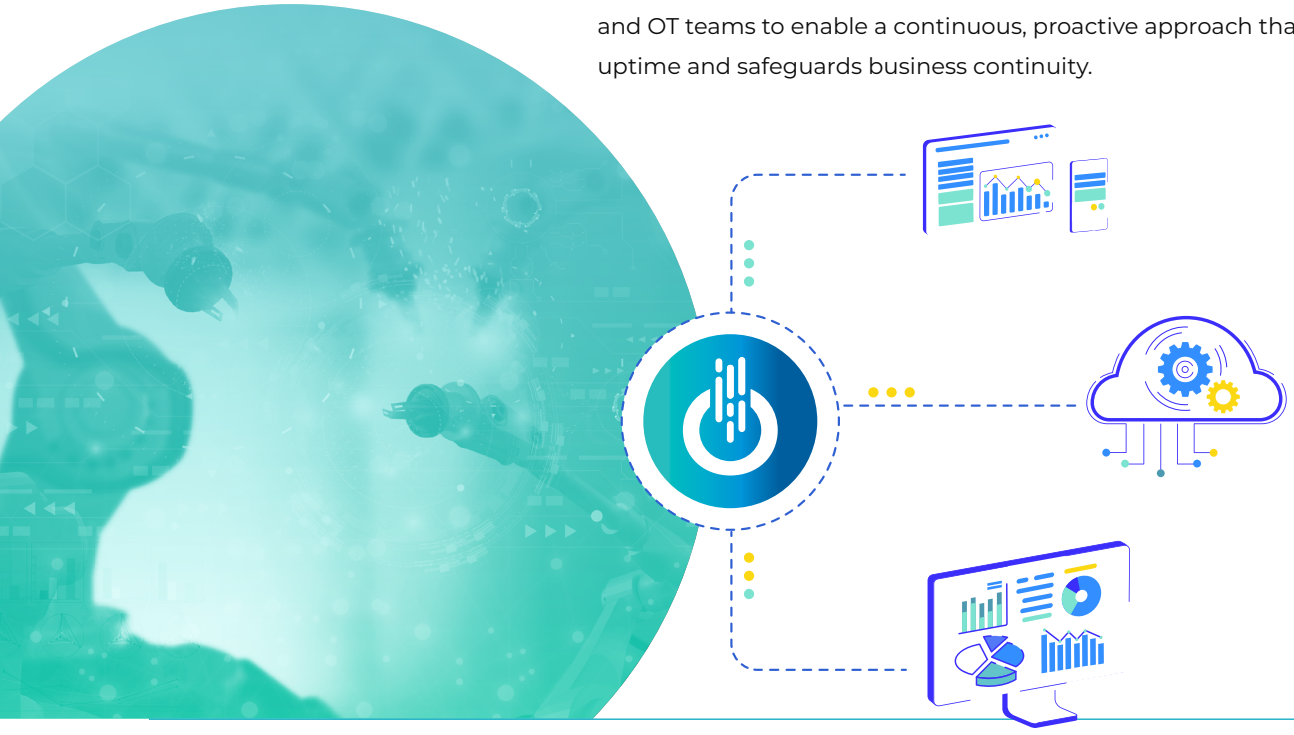
OTORIO has helped many organizations improve their risk management practices. In one example, OTORIO worked with a leading **pulp and paper manufacturer** to gain asset visibility of its OT, IT, and IIoT risks. OTORIO provided the company's security teams with operational context and impact analysis, as well as security posture assessments, to enable ongoing operations to continue undisturbed.

OTORIO's industrial-native RAM² solution integrated smoothly with the company's existing security controls and significantly improved the company's Mean Time to Detect and Mean Time to Respond. OTORIO's solution reduced alert noise and helped prioritize risks and vulnerabilities. Using OTORIO, the pulp and paper company gained the ability to deal effectively with suspicious events in a timely and appropriate manner.

In another instance, OTORIO worked with an **international energy company** to address risks without impacting ongoing operations. It improved the company's ROI by leveraging existing technology investments. OTORIO provided a thorough security assessment report that gave the energy company a complete picture of its OT cybersecurity posture.

OTORIO provided the energy company with an agile approach to risk mitigation. It allowed the company to harden site-specific OT network risks and vulnerabilities. With OTORIO's help, the company was able to proactively assess, mitigate, and manage risks and secure its OT environment.

OTORIO's solution facilitated collaboration between the company's IT and OT teams to enable a continuous, proactive approach that ensures uptime and safeguards business continuity.



Implementation and Integration Considerations

OTORIO's industrial-native OT security platform offers comprehensive security solutions for critical industrial assets, such as SCADA systems, OT networks, and industrial control systems. Organizations seeking to deploy such a security solution will want to take the following steps:

Assessment of the organization's existing security posture: This includes identifying potential risks and threats to critical assets, as well as gaining visibility of the organization's existing security procedures and policies.

Planning the process for implementing an industrial-native security solution: Considerations will include the project's timeline, scope, and budget, and will require extensive collaboration between IT and OT teams, along with other relevant stakeholders.

Deployment of the security platform: Whether on-premises or cloud-based, depending on the needs and preferences of the organization.

Integration with existing systems and security tools: This includes IDPS (intrusion detection and prevention systems) and firewalls. OTORIO integrates with organizations' existing systems by receiving and analyzing data from these systems and sharing threat intelligence with them.

Monitoring the OT network for potential threats: OTORIO analyzes system logs, network traffic, and other data sources to identify vulnerabilities and malicious activity.

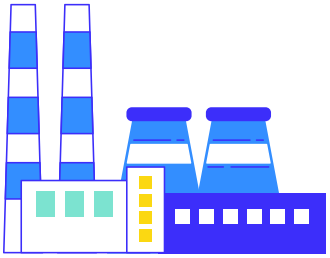
Response and mitigation: OTORIO provides organizations with real-time alerts prioritized by business priorities. Clear mitigation guidance and actionable playbooks accelerate response time and prevent business disruptions.

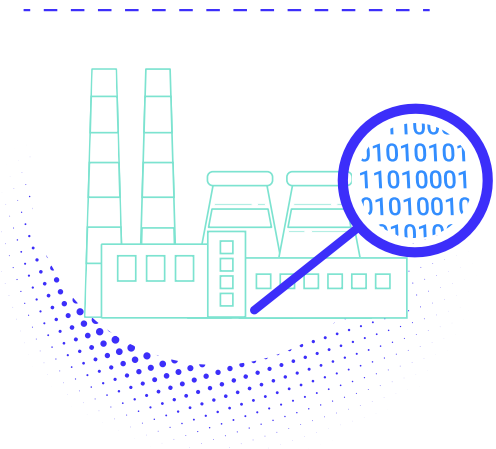
Ensuring Operational Resilience for Policyholders

Reducing cyber risk and ensuring operational efficiency is paramount to business success and insurability. Policyholders must proactively reduce cyber risk to avoid operational and business disruptions. Industrial organizations and HSB-insured businesses can benefit from OTORIO's OT security risk management platform to manage and mitigate operational risk in a more effective way and prevent disruption to business priorities.

Organizations aiming to adopt an industrial-native approach to risk assessment and risk management should follow these best practices:

- (UNDERSTAND OT ENVIRONMENT - VISIBILITY) Organizations must acknowledge that traditional IT security approaches will not be able to address the specialized requirements of OT systems successfully. Gaining broader visibility of their OT environment enables organizations to detect subtle anomalies which, if left unchecked, could lead to greater threats or unsafe conditions.
- (ASSESSMENT) Organizations should carry out a thorough review of their existing OT environment. This should include identifying assets, vulnerabilities, potential threats, and security gaps. Assessment lets organizations evaluate their risk level, ensure they meet compliance requirements, improve their incident response, and plan for future upgrades.
- (MONITORING) Organizations should seek to become more security literate and centralize their risk monitoring and asset visibility. They should seek to gain real-time visibility into network traffic and activity through continuous monitoring.
- (PRIORITIZATION) Organizations should properly prioritize risks based on their potential impact on operations. Prioritization allows critical infrastructure organizations to manage risk more effectively, make informed decisions, and improve their overall cybersecurity posture.
- (INCIDENT PLANNING) Organizations should develop a comprehensive and actionable plan with detailed instructions for the operational team once an attack is identified. The first steps taken are often the most critical, and can either improve the enterprise's response or make it considerably worse. The plan should focus on protecting the equipment from further damage, such as solidifying molten products, burning work in process, or dealing with out-of-synchronization situations.





On-Demand Assessment vs. Continuous OT Security Risk Monitoring

To support implementing the above best practices, organizations should integrate and leverage specialized OT security technology and protocols. OTORIO offers on-demand risk and compliance assessment, as well as continuous OT cyber risk monitoring and management.

spOT™ is an automated, out-of-the-box solution that provides compliance assessments of operational networks at the asset and site level, enabling organizations to demonstrate compliance with the necessary documentation, identify security gaps, and avoid penalties.

RAM² is a unified framework that provides continuous monitoring and threat detection for OT/ICS networks. It helps organizations proactively manage cybersecurity risks by collecting and analyzing network data on potential threats or suspicious activity, making operational environments more resilient.

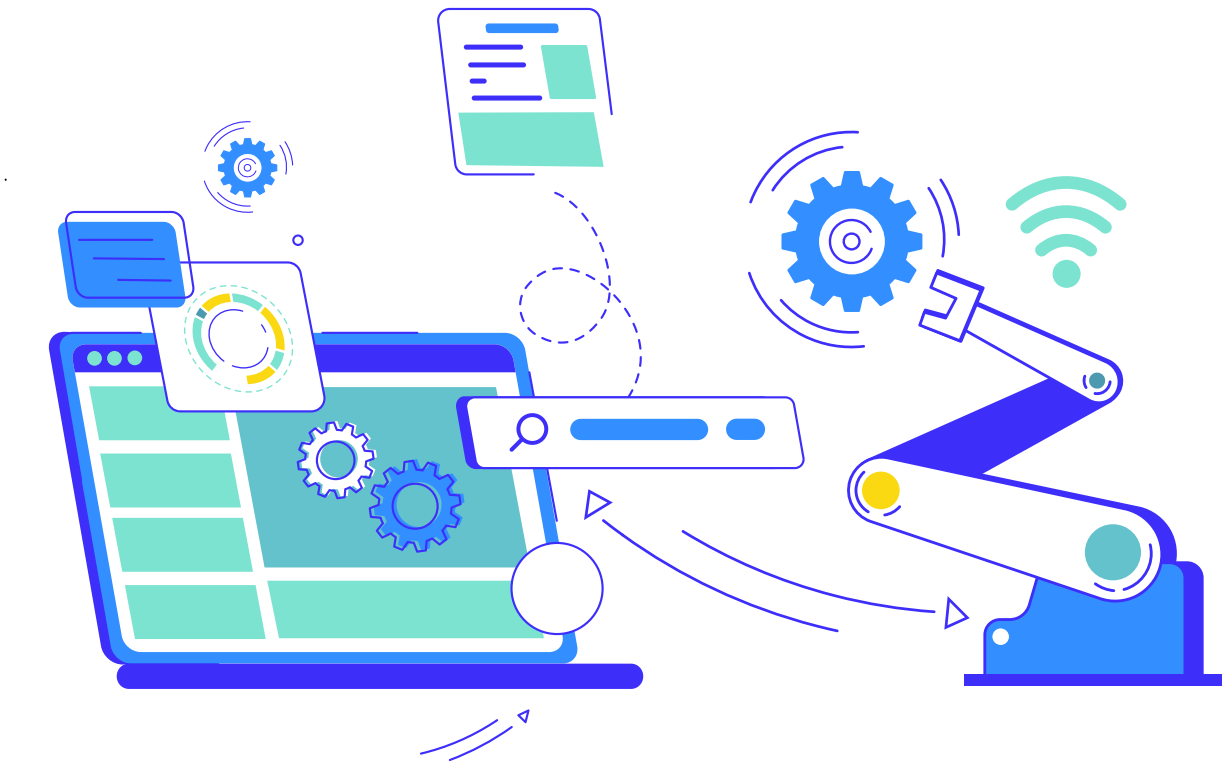
When choosing between the two, an organization should consider the following factors:

- What is the threat landscape in which the organization operates? If it is high risk, continuous monitoring may be needed to stay ahead of potential threats.
- What is the organization's risk tolerance level? If the organization can tolerate some downtime, an on-demand approach may suffice, whereas if it cannot afford any downtime, a proactive approach is recommended.
- What resources can the organization dedicate to the solution? Considerations such as staff, budget, and technology must be taken into account.
- What are the regulatory requirements to which the organization is subject? These may dictate the type of solution warranted.

Many critical infrastructure organizations are also still accustomed to traditional IT-led security protocols. Therefore, some concerns and objections may arise when considering an industrial-native risk management solution. Among them:

- What is the cost of implementing the platform within their existing risk management budget? Cost-benefit analysis can help organizations weigh this expense against the potential impact of a cybersecurity incident on their operations.
- How compatible is the platform with legacy systems and existing equipment? How easily can the new platform be integrated to coordinate with these systems?
- What is the operational impact of implementing the platform? Will it require updates to existing processes and procedures, possibly affecting the organization's ability to operate effectively?
- What type of training will be needed to implement and integrate the platform? Will new staff need to be brought on, or will additional training for existing staff be required?
- Will the platform meet the necessary regulatory compliance requirements demanded by authorities?

Organizations can deploy and integrate OT security solutions thoughtfully and successfully by answering these questions and any others specific to the organization's needs.



Conclusion

Industrial-native security solutions enable organizations to overcome IT-OT risk management barriers because they are specifically designed to address the unique security challenges faced by IT and OT convergence from an operational standpoint. This forms the foundation for effective risk management, providing organizations with the control and visibility needed to protect their operations from cyber threats.

Implementing an effective risk management strategy reduces the likelihood of security breaches and their associated costs, and therefore reduces insurance risk. HSB and OTORIO are working in collaboration to bridge the gap between IT and OT for more effective OT risk management that reduces insurance risk in several ways:

- **Providing a unified framework for both IT and OT**, with a holistic view of the entire system that enables IT and OT teams to collaborate on risk management efforts.
- **Offering comprehensive visibility into both IT and OT systems**, facilitating the understanding of how these systems interact and identifying potential security risks at the intersection of these domains.
- **Detecting threats that target both IT and OT systems**, helping to prevent security breaches that can result in costly downtime, and mitigating potential safety risks.
- **Abiding by compliance requirements encompassing IT and OT**, supporting adherence to industry-specific regulations and standards with comprehensive and automated risk assessment.

As an HSB partner, OTORIO can provide organizations with additional SCADA network scanning capabilities to further bolster security and peace of mind. The advanced capabilities of OTORIO's OT security solutions offer invaluable support to companies seeking to safeguard their business continuity.

Organizations are therefore encouraged to leverage OTORIO's risk assessment and continuous monitoring toolbox along with HSB's insurance services to ensure they orchestrate the most comprehensive protection against potential threats.

End

Thank you for finding value in this paper. To gain deeper insights into the data behind the studies and IT-OT convergence trends, we invite you to explore the data and case study links provided below.

- **HSB ATS Division**
- **HSB and OTORIO Resources**
- OTORIO Case Study: **Energy Company Risk Assessment**
- OTORIO Case Study: **Manufacturing Asset Visibility**
- **spOT Risk Assessment Brochure**
- **RAM² Risk Monitoring Brochure**

By combining OTORIO's advanced toolbox with HSB's risk management services, organizations can confidently address emerging cyber threats, increase operational resilience, and safeguard business continuity.

To learn more, contact us at marketing@otorio.com.

About OTORIO

OTORIO is an innovative OT security risk management platform for advanced operational resilience. The platform provides organizations with a centralized and comprehensive view of cyber risk in alignment with business priorities and industry regulations to ensure safe, productive, and reliable operations. OTORIO discovers and protects multi-generational industrial and security systems, and multi-vendor OT environments, so organizations can confidently take the next step in digital transformation and OT security governance. OTORIO's unified risk management framework and actionable mitigation guidance enable security practitioners to proactively and efficiently reduce cyber risks, improve security posture and ensure business continuity..

Visit OTORIO.com

About HSB

HSB, part of Munich Re, is a multi-line specialty insurer and provider of inspection, risk management and IoT technology services. HSB insurance offerings include equipment breakdown, cyber risk, specialty liability and other coverages. HSB blends its engineering expertise, technology and data to craft inventive insurance and service solutions for existing and emerging risks posed by technological change. Throughout its 150-year history HSB's mission has been to help clients prevent loss, advance sustainable use of energy, and build deeper relationships that benefit business, public institutions and consumers. HSB holds A.M. Best Company's highest financial rating, A++ (Superior).

Visit munichre.com

This white paper highlights how industrial organizations can enhance the ROI of their first-generation IDS and empower their teams using OTORIO's comprehensive, industrial-native RAM² OT security solution as an overlay. Alternatively, companies that have not yet implemented OT security into their existing security stack can utilize RAM² as a comprehensive OT-IT-IIoT solution to lay a solid foundation to proactively manage digital risks and build resilient operations. In each scenario, RAM² empowers IT and OT teams to be truly connected and streamlined for security collaboration.