PAC

Whitepaper

OT/ICS Security:

Project and Managed Services are key success factors

Lead-Analyst:

Wolfgang Schwab

PAC, July 2024

In cooperation with

Infosys®

Navigate your next

TABLE OF CONTENT

Hybrid Multi Cloud – Copyright PAC GmbH 2024

INTRODUCTION

ABSTRACT

In this whitepaper, PAC discusses the challenges of OT security, the approach needed to succeed, the services an OT security provider should offer, and why a service provider can be a good choice for project and managed services.

Cybersecurity is a crucial aspect of modern life, as it protects individuals and organizations from the threat of cyberattacks, data breaches, and other forms of digital compromise. In recent years, the importance of cybersecurity has only grown, as the internet of things (IoT) has expanded to include operational technology (OT) systems in industries such as manufacturing, energy, transportation, and healthcare. OT security is a critical subset of cybersecurity that specifically focuses on protecting these critical infrastructure systems from cyber threats. As OT systems increasingly rely on internet connectivity, they become vulnerable to hacking, malware, and other forms of cyber attacks, which can have devastating consequences for industrial processes, equipment, and even human life. Effective OT security is essential to prevent these risks, ensuring the reliable operation of critical infrastructure and safeguarding the physical world from cyber-based threats.

Infosys and PAC believe that OT security should not be considered separately from IT security. At the same time, a foundation must be created on the OT side to enable security operations in the first place. Topics such as network segmentation, zero trust, or endpoint protection are usually not implemented on the OT side but are essential before IT-OT integration is considered. Unfortunately, many companies implement their digitalization strategies without giving them sufficient thought. Therefore, the subsequent implementation of reliable OT security is important. Very few companies are able to accomplish this internally, as there is usually a need for additional human resources. Service providers can offer short-term support here and successfully implement projects and, if necessary, also take over operations.

INDUSTRY SCENARIO

The industry continues to be strongly impacted by the emergence of innovative technologies, such as IoT, virtual reality/augmented reality, robotics/cobots, and (generative) artificial intelligence, which in theory have a double impact: increased efficiency of internal processes (e.g., product development, production, logistics) and enlargement of product offerings (e.g., smart products). Therefore, for the industry, there are two major areas of investment to increase efficiency further and to transform into a smart factory to respond to changing customer and market demand in an agile and flexible manner: Factory Automation and IT/OT integration. Smart products and digital add-on services are essential, but most companies are not yet ready.

> "An integrated IT and OT security strategy and architecture is necessary today."
>
> *Wolfgang Schwab, Head of Cyber Security, PAC*

- Factory Automation: In the short term, manufacturers will continue to automate selected shop floor processes. Examples include autonomous vehicles on the shop floor or in the warehouse and automated digital quality control systems. This will drive investments in robotics and AI solutions in particular. In the longer term, next-generation production concepts, such as modular production cells, will be applied to

enable the autonomous production of highly customized or individual products. This will drive investments in robotics, AI solutions, edge computing, and IoT.

- IT/OT Integration: Increasing transparency on the shop floor is a prerequisite for identifying the potential for process optimization. Therefore, integrating the various data silos – resulting from a vast variety of applications on the shop and top floors (enterprise level) – will be essential. This will drive investments in the shorter term, for e.g., capturing data from production machines and connecting this data with the enterprise's back-end systems, including investments in data platforms and analytics. In the medium to longer term, this will drive investments in the end-to-end integration of processes, from product development and production to logistics. To run such environments safely, the OT side must be secured to the same extent as the IT side to prevent safety issues, downtime, and, consequently, revenue loss.

INDUSTRY CHALLENGES

Currently, many companies are in the middle of their digitalization journey. They invest heavily in factory automation and IIoT but need more basic security measures for secure operations. The most common challenges currently are:

- **Asset visibility, inventory, and CMDB**: You can only protect what you know. Therefore, an up-to-date asset inventory list and CMDB are always important. Unfortunately, this "administrative work" is still carried out manually in many companies, which can lead to delays and errors.
- **Vulnerability remediations**: Identifying vulnerabilities is one thing; fixing them is another. This is a real challenge, especially in OT, as maintenance windows often do not exist or only exist infrequently. Accordingly, a planning process is necessary, and, on the other hand, the OT systems must be shielded so that weak points in individual systems cannot be exploited from the outside.
- **Network segmentation**: Network segmentation is an architectural approach that logically divides a network into several segments or subnets, each acting as its own small network. This allows data traffic between subnets to be controlled with detailed guidelines, protecting against the spread of threats. Unfortunately, many companies still shy away from the effort involved.
- **Security controls and policies**: While IT security controls and guidelines are common sense, OT is still weak. With increasing IT-OT integration, there is an acute need for action here.
- **Secure remote access**: Remote access is still essential for service providers and employees at various levels. However, appropriate protection and monitoring of activities is necessary and is often neglected.
- **Regulatory and compliance**: Regulation and compliance are top issues not only on the IT side but also on the OT side. By no means all companies are compliant with NIST, ISA 62443, GDPR, etc. compliant.
- **Endpoint protection and USB blocking**: Endpoint protection is a significant issue, especially on the store floor. End devices with outdated operating systems are often used here, and they have frequently been phased out of maintenance and, therefore, need to be protected differently from current operating systems. Endpoint protection and the most extensive encapsulation possible are just as necessary as strict control of USB interfaces to prevent data leakage or the introduction of malware.
- **Visibility coverage of OT env**: To operate security operations comprehensively and agilely, all OT protocol sources must be integrated, events prioritized according to risks and the probability of attacks, and integrated for correlation. It is also essential to ensure transparency across all locations. This is far from being the case for all companies today.

> "'Security First' is on everyone's lips in IT. It would be real progress in the OT environment if 'Security Last' was not standard."
>
> *Wolfgang Schwab, Head of Cyber Security, PAC*

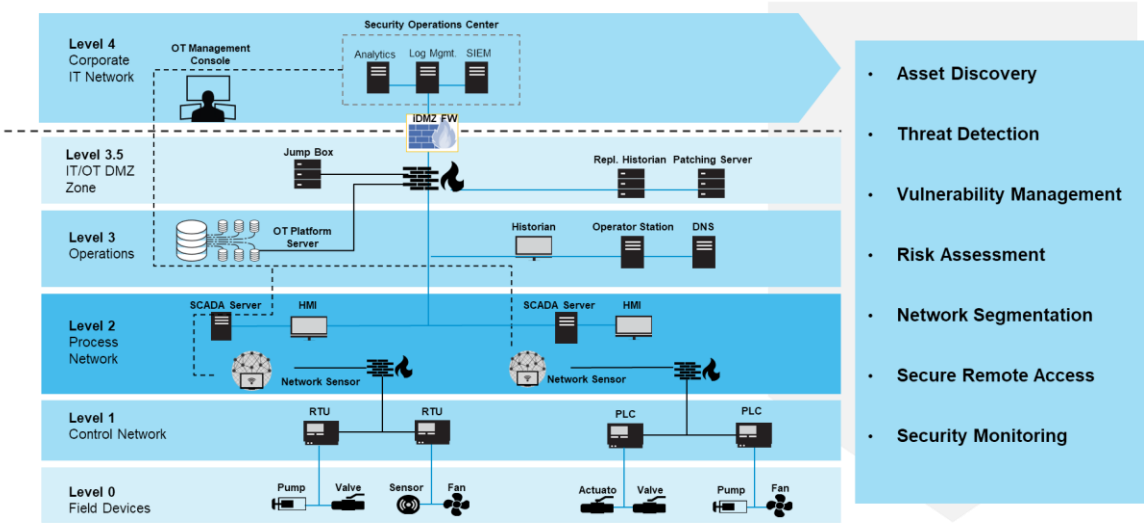
The bottom line: Many companies are working on implementing their digitalization strategies and integrating IT and OT to implement digitalization effectively. However, they often neglect the security aspect. Sooner or later, this will be their downfall. Security should be considered in parallel with digitalization and implemented in corresponding projects.

SECURING INDUSTRIAL OPERATIONS: A CALL FOR A NEW PARADIGM

The Purdue Reference Model is part of the PERA methodology (Purdue Enterprise Reference Architecture) developed in the 1990s. It is a reference model for automation and industrial networks. The reference model provides valuable assistance in protecting OT against cyber threats. The model can be used to structure complex automation and industrial networks. The model structures industrial and automation networks by dividing them into five areas (levels). Each device and system operated in the network is assigned to a level. This subdivision helps to protect OT against external and internal threats. The reference model was adopted in the ISA-99 and IEC 62443 series of standards. Although the model was developed in the 1990s and modern IIoT network architectures differ from the networks of that time, it is still relevant. It continues to be used for the protection of industrial and automation networks.

> "Even today, companies are well advised to follow the Purdue model."
>
> *Wolfgang Schwab, Head of Cyber Security, PAC*

OT Security Reference Architecture using align to Purdue Model



Note: This topology shows the use of OT Security components from one of the OT vendor. The exact network topology will be designed during the discovery and design phase with the respective OT security platform provider.

1- Courtesy Infosys

The reference model divides the networks into different areas (levels). The levels range from the lowest level, the physical components of the industrial manufacturing process, to the highest level, the office network. The lower the level, the higher the requirements for the availability and reliability of the systems. IT and OT levels are separated by a DMZ (demilitarized zone). The individual levels with their assigned systems are:

- **Level 0**: physical process with the components of the industrial manufacturing process, such as actuators and sensors.

Hybrid Multi Cloud – Copyright PAC GmbH 2024

- **Level 1**: intelligent control and monitoring systems such as programmable controllers or electronic control systems.
- **Level 2**: Process control systems for monitoring process control.
- **Level 3**: Operations management and production operating systems (operations management).
- **Level 3.5:** This is the IDMZ zone which segregates the OT to IT network. All the network traffic coming from IT is inspected and monitored by the Firewall placed in the iDMZ.
- **Level 4**: Corporate network with workstation, peripheral devices, analytics server, ERP software and other platforms.
- **Level 5**: This is the DMZ between Corporate Network and Internet. All the traffic from Cloud and internet are inspected by the Firewall.
- **Level 6**: Cloud platform, Internet and SaaS services. Here we have not depicted the level 5 in the architecture dgm.

In addition to a suitable security architecture, companies need to move from static OT security with manual tasks to dynamic approaches. Although the dynamics in the OT area are less dynamic today than in IT, further digitization efforts also increase dynamics here. Hence, there is a current need for action. The significant measures are:

- Automated Asset Discovery and Inventory. Tool-based accurate and in-depth security assessment.
- Integrated IT/OT Security, Monitoring from one console
- Secure Remote Access with Session management, workflow approvals, and MFA.
- Real-time and Advanced threat detection using AI/ML techniques.
- Automated policies, NAC, firewall rules recommendation for remediations.
- Software moving towards SaaS deployment.
- Proactive threat detection and response approach

The fundamental question is whether companies can and want to shoulder these challenges alone? Adaptations to modern OT security are currently necessary, but they are complex, and not all companies have the internal resources required to handle such projects. Subsequent operation is also not trivial, so managed services are a valid option.

OT/ICS SECURITY SOLUTIONS: KEY SERVICES FOR INDUSTRIAL ORGANIZATIONS

INDUSTRY BEST PRACTICES

Any suitable security service provider in this field must support the following best practices for OT security besides its own:

- **Place the OT security under the CISO's control**: OT systems have traditionally operated separately from IT departments, resulting in a siloed approach to cyber security. However, with the increasing convergence of OT, IT, IoT, and Industrial IoT (IIoT), a unified strategy to combat cyber threats is essential. Placing OT cybersecurity under the CISO helps to ensure the consistent application of security measures and optimize the company's overall security posture.
- **Identify and prioritize OT assets**: Before a company can defend its assets, it needs to know what is where. Organizations should maintain an up-to-date inventory of all OT systems, hardware, software, and related technologies. In some organizations, different business units still manage their OT assets separately. Ideally, however, the security team will have centralized, automated detection and management capabilities with complete visibility into the OT environment and attack surface. Once assets have been identified, they must be prioritized according to their importance to operations to focus investment on truly critical elements.
- **Conduct security awareness training**: Employees (internal or external) are often the weakest link in the cyber security chain, which also applies to OT environments. Regular security awareness training ensures that all employees - whether in IT, OT, or non-technical positions - understand the cyber risks and their role in mitigating them. Security awareness training should cover the specific challenges of OT systems, including the potential impact of attacks on critical infrastructure.
- **Control network access**: It is fundamental to control who and what can connect to an OT network, using security tools such as identity and access management and network access control. Follow the principle of least privilege and restrict access to OT systems to only those devices and users who need it to perform their tasks.
- **Consider a zero-trust framework**: The Zero-Trust model is based on “never trust, always verify.” It does not assume that everything in a company's network is secure but requires continuous authentication and authorization of all users and devices—both internally and externally.
- **Deploy micro-segmentation**: In an OT environment, this means implementing network segmentation so that devices from one zone cannot communicate directly with those from another zone without proper authorization. This limits the potential spread of threats and ensures that even if one segment is compromised, others are not.
- **Backup of Config files**: It’s very important to keep back up of the configuration files, policies list and firewall rules in a regular interval as any changes or deletion of these files can impact severely to the plant operations. Ensure the backup of these highly sensitive files, data need to be stored in a secure server so that it can be retrieved at the time of need.

Hybrid Multi Cloud – Copyright PAC GmbH 2024

OT/ICS SECURITY SERVICE PROVIDER REQUIREMENTS: KEY CAPABILITIES TO CONSIDER

A service provider who can bring real added value to a company's OT security operations should have the following capabilities:

- **Industry know-how**: In addition to technical expertise, which is essential, OT security service providers should have in-depth industry knowledge. This is the only way for the service provider to support customers at the process level.
- **Genuine deep partnerships with leading technology partners**: OT security service providers naturally also use standard software and, if necessary, appliances. To provide customers with the optimum solution, service providers must have a good overview of the market and maintain in-depth partnerships with the leading providers who can help them find solutions in the event of issues.
- **Own IP**: Customers need a service provider with experience in the OT security environment who has also developed its own intellectual property. This includes processes for using CVE information, blueprints for playbooks and automation, and OT security use cases and workflows.
- **Project and managed services**: The usual OT security journey starts with analyzing the status quo and developing a roadmap for improving it. After that initial step, integration projects are initiated, and the operations model needs to be discussed. The company runs operations afterward, or a service provider takes over as a managed service. The most crucial project steps a suitable OT security provider should offer are:
    - **OT security assessment & advisory**: OT security risk assessments should begin with a standardized comprehensive assessment of the current OT security strategy, policies, and infrastructure, as well as interfaces to IT and the outside world. A question-based assessment, according to NIST, ISA-62443, or other relevant standards, can help to get the right picture. Based on the assessment results, an OT security advisory can begin, providing recommendations, a strategy, and a roadmap for upcoming projects.
    - **Compliance and regulatory management**: This step is critical to ensure that industry regulations and compliance with NIS2, NERC-CIP, and other geographic regulations are met and certification can take place. A gap analysis between the current "as-is" status and the regulatory requirements is just as much a part of this as proposals for closing these gaps and the concrete implementation.
    - **OT-IT sec ops & governance**: In many cases, the OT sec ops and the associated governance must first be set up. OT mustn't be viewed in isolation but in harmony with IT. The resulting IT-OT SOC operation can then be carried out by a service provider in a managed service. The core elements here are:
        - 24*7 safety monitoring and triaging.
        - Continuous incident/alert management of SIEM/SOC.
        - Continuous security assessment and remediation measures.

Hybrid Multi Cloud – Copyright PAC GmbH 2024

- **Zero trust-aligned OT security services**: Zero trust is a proven model in IT that should also be used in the OT environment. Service providers should have experience in this area, as implementation is not trivial. The following steps are part of the optimal procedure:
  - Zero Trust assessment of the OT network
  - Zero Trust security controls and recommendations for OT networks for access control, network, data, etc.
  - Design and implementation geared towards zero trust, architecture & services
- **OT platform design, build, and management**: The largest single project is usually the concrete implementation of an OT security platform. The following tasks are essential:
  - Design of the system network topology and a blueprint of the deployment architecture.
  - Implementation of the OT security platform.
  - Tuning, alerting, and optimization of the platform.
  - Integration with third-party solutions such as NGFW, SIEM, AV, EDR, and ITSM tools.
- **Vulnerability and risk management**: OT security gaps often cannot be closed immediately due to a lack of maintenance windows. Therefore, encapsulating vulnerable systems without completely ignoring patching is critical. The most essential tasks in this area are:
  - Asset base configurations.
  - Identification of security vulnerabilities in connection with IT OT systems.
  - False positive analysis and reporting of vulnerabilities.
  - Risk analysis and risk prioritization.
  - Vulnerability management and governance.
  - Remediation plan and its implementation.
  - Reporting and dashboarding.
- **OT security training**: Security training is not only important for IT but also essential in the OT environment. The aim must be to bridge the skills gap between OT and IT resources, create awareness/training on OT security for plant engineers, and raise awareness of recommendations, best practices, standard operating procedures, and troubleshooting guidelines.
- **Managed services**: Most assessments should be repeated regularly, which often leads to adjustments to processes, specifications, and infrastructure. Accordingly, it can make sense to outsource both the operation and the continuous value development of OT security to a suitable service provider.

THE BENEFITS OF ENGAGING AN EXTERNAL OT SECURITY SERVICE PROVIDER

There are many reasons to choose a service provider for OT security projects and their operation. With advancing digitalization and increased IT-OT integration, the complexity of the IT/OT infrastructures used has increased significantly in recent years, as have the necessary cybersecurity measures. In addition, there has been a significant increase in increasingly professional attacks on companies. All of this has meant that many companies can no longer cope with further development and in-house operations.

COMPETENT STAFF

Qualified personnel are even more difficult to find in the OT security sector than in IT in general. The recruitment process and retaining employees are correspondingly expensive. Continuous training, essential in the security environment, is also cost-intensive. Medium-sized companies, in particular, quickly reach the limits of their financial resources here. In addition, staff turnover in the security sector is very high.

Service providers have decisive advantages here. Although they, too, can only find a few qualified employees on the open market, many work with colleges and universities to bind new employees to their own companies early and begin practical training. Staff turnover is also relatively high among service providers but lower than in other companies. This is partly due to the often more comprehensive range of further training opportunities and the fact that experts usually work for several clients, making the tasks more enjoyable.

COST EFFICIENCY, BETTER OPERATIONAL RELIABILITY, STEEPER LEARNING CURVE

Service providers have decisive advantages over companies in the security environment. In addition to the aforementioned advantage of recruiting specialists, the costs for training and further education are spread across several customers, and the service providers generally have an insight into companies of different sizes and sectors. They can derive best practices from this more easily. In addition, service providers can rely more heavily on complex automation, leading to faster response times and less damage. It can also be assumed that fewer errors occur due to the often higher level of training compared to other companies.

Hybrid Multi Cloud – Copyright PAC GmbH 2024

Especially when it comes to new technologies and attack vectors, service providers have the advantage of generally serving many customers, dealing with new technologies early, quickly recognizing new attack vectors, and gaining experience with suitable countermeasures. This leads to an earlier and significantly steeper learning curve than would be possible for other companies.

An additional advantage for service providers is that they can usually guarantee 24/7 operation without any problems, which is difficult for at least some other companies.

ADDITIONAL BENEFIT THROUGH A COMPREHENSIVE PARTNERSHIP OUTSIDE OF OT/ICS SERVICES

OT and IT security and IT are not only strategically linked but also in terms of operations. Accordingly, it can be advantageous to outsource IT and security projects and managed services to a single service provider, as this results in less coordination and moderation effort on the customer side. In addition, customers with a higher order volume are more important to the service provider, and the customer can expect a higher level of commitment.

> "OT security cannot be separated from other IT security and not completely from IT operations tasks. A single service provider therefore often significantly simplifies the coordination effort."
>
> *Wolfgang Schwab, Head of Cyber Security, PAC*

Therefore, given the potential desire to consolidate service providers, companies should bundle services and put them out to tender jointly.

WHY INFOSYS

Infosys is a global leader in next generation digital services and consulting. With over four decades of experience managing global enterprises' systems and workings, we expertly steer clients in more than 56 countries as they navigate their digital transformation powered by cloud and AI. We enable them with an AI-first core, empower the business with agile digital at scale, and drive continuous improvement with always-on learning by transferring digital skills, expertise, and ideas from our innovation ecosystem. We are deeply committed to being a well-governed, environmentally sustainable organization where diverse talent thrives in an inclusive workplace.

Infosys CyberSecurity embodies the philosophy of driving digital trust through a focus on "Secure by Design", building resilient cybersecurity programs to scale, and embracing innovative technologies to secure the future.

The organization's approach is centered around a four-dimensional framework of Diagnose-Design-Deliver-Defend, which defines its commitment to digital trust. The company's competitive edge includes state-of-the-art Cyber Defense Centers located across the US, EMEA, and APAC, designed to prevent, detect, assess, and respond to cybersecurity threats and breaches. The organization's engineering and research labs provide clients with access to advanced threat hunting capabilities and the latest technological innovations in cybersecurity.

Additionally, Infosys CyberSecurity offers Platform Powered Services – Cyber Next, a single package combining pre-selected and pre-integrated ready-to-use security technologies that offer deep visibility, lifecycle management, automation, and risk-based prioritization. Strategic partnerships with industry-leading technology vendors and academic collaborations with universities like Purdue and NIIT enable the design of best-in-class security solutions and provide intensive cybersecurity training to upskill and reskill professionals.

Visit www.infosys.com to see how Infosys (NYSE:INFY) can help your enterprise navigate your next.

CONCLUSION

The demands on companies' OT security have increased enormously in recent years:

- Digitalization and, thus, the use of IIoT and the advancing IT-OT integration will amplified the requirements for security on the OT side as well.
- Security attacks have become more professional at all levels.
- The IT/OT infrastructure to be protected has become significantly more complex due to increased cloud usage and edge computing/IoT use.
- Compliance requirements have risen continuously in recent years and will continue to do so.
- New approaches such as automation and AI offer great potential for savings but are pretty complex to implement.

At the same time, the market for cybersecurity specialists is more than tight.

Project and managed security services that cover the entire IT/OT infrastructure and can be flexibly adapted to changing requirements are attractive.

Hybrid Multi Cloud – Copyright PAC GmbH 2024

DISCLAIMER, RIGHTS OF USE, INDEPENDENCE

Infosys commissioned this study.

Further information can be found at www.pacanalyst.com.

Disclaimer

The contents of this study have been compiled with the most excellent possible care, but no guarantee can be given for their accuracy. Estimates and assessments reflect our current knowledge in June 2024 and may change anytime. This applies in particular, but not exclusively, to forward-looking statements. Names and designations used in this study may be registered trademarks.

Rights of use

This study is protected by copyright. Any reproduction or forwarding to third parties, even in part, requires the client's prior explicit consent. The publication or dissemination of tables, graphics, etc., in other publications also requires prior approval.

Independence

This study was prepared solely by Pierre Audoin Consultants (PAC). The client did not influence the data's evaluation and the study's preparation.

ABOUT PAC

We are a content-based company with consulting DNA. PAC is the leading European market analysis and consulting company for the IT industry. We support software vendors and IT service providers worldwide. Since 1976, we have been helping our clients to interpret market dynamics, increase revenue, and raise their profile. With our unrivaled understanding of market developments in Europe and our in-depth analysis, we support leading market players in strategy development, go-to-market optimization, and gaining additional market share. With a team of over 100 experts in Europe, PAC offers consulting based on market analysis. Our market research covers over 30 countries worldwide and is based on the three portfolio pillars Guidance, Insights, and Visibility, as well as our renowned SITSI® research platform.

For more information, please visit www.pacanalyst.com.

Contact:

PAC
Holzstr. 26
80469 München

+49 89 719 62 65
info-germany@pacanalyst.com

www.pacanalyst.com
www.sitsi.com

Hybrid Multi Cloud – Copyright PAC GmbH 2024

© Copyright PAC GmbH 2024