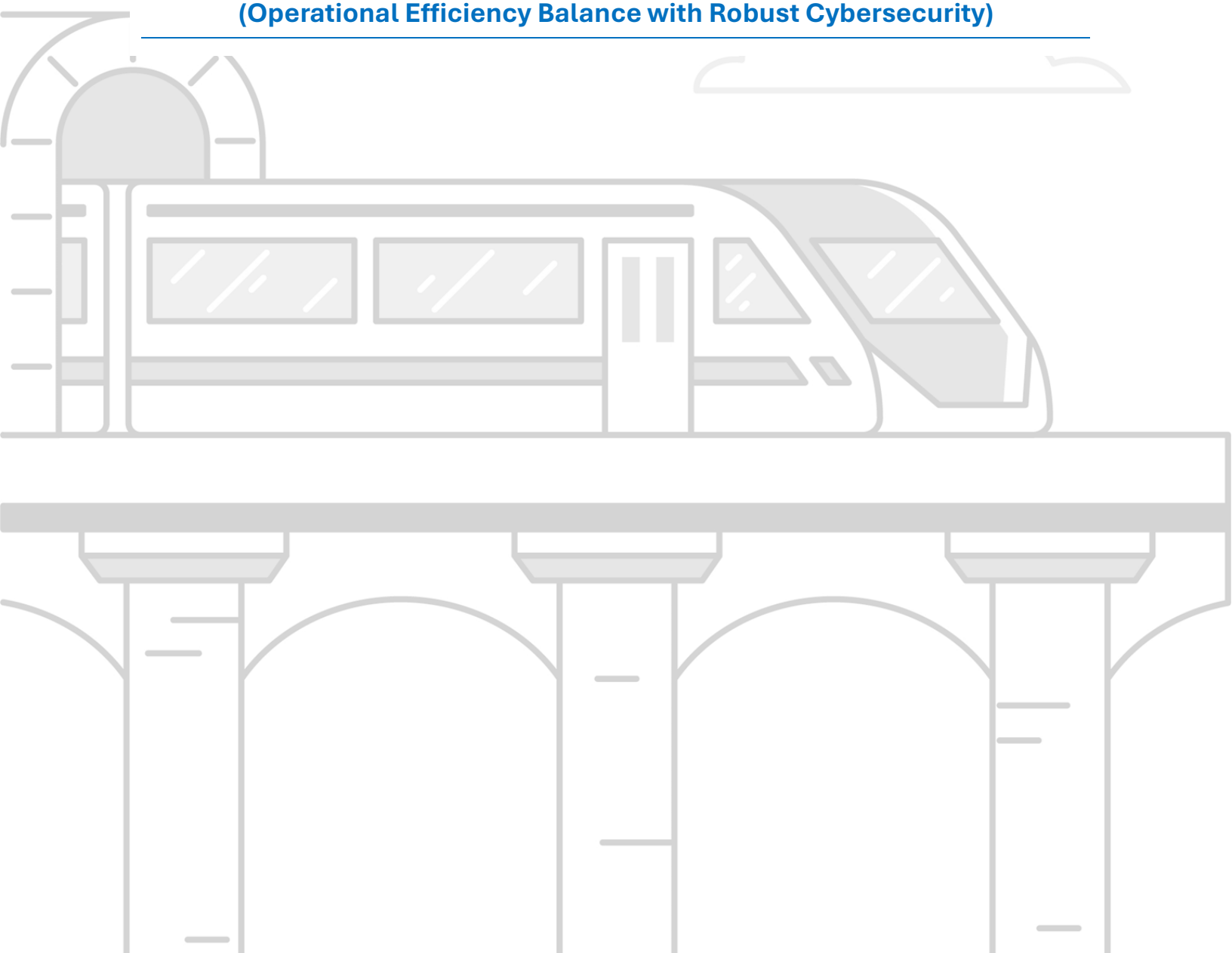
CYBERSECURITY IN RAILWAY DIGITAL TRANSFORMATION JOURNEY

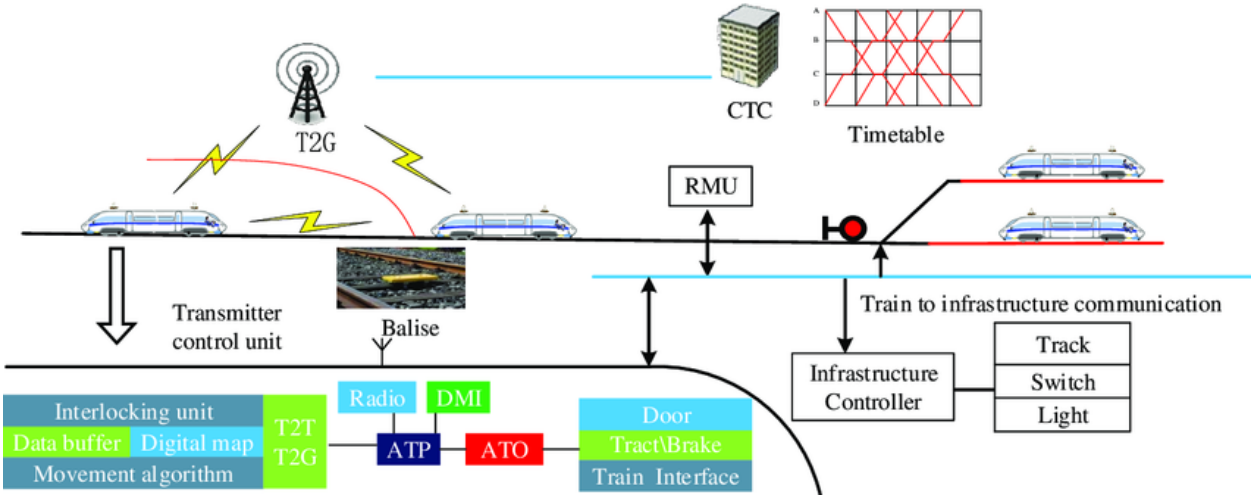
(Operational Efficiency Balance with Robust Cybersecurity)



Executive Summary

The railroad industry, integral to global transportation networks, is increasingly reliant on Operational Technology (OT) systems. These systems, critical for managing rail operations, are becoming prime targets for cyber threats. Ensuring robust cybersecurity measures is imperative to safeguard these infrastructures. This whitepaper explores the cybersecurity landscape for OT in the railroad industry, highlighting the importance of adhering to established standards and frameworks to mitigate risks and enhance security resilience.

In the railroad industry, OT systems are vital for operations such as signaling, control systems, and communication networks. With the convergence of IT and OT, cybersecurity threats targeting rail networks have escalated, necessitating stringent security measures.



Source: https://www.researchgate.net/publication/362174484_Train-centric_Communication_based_Autonomous_Train_Control_System

The Importance of OT Cybersecurity in Railroads

Railroads are critical infrastructure, essential for economic stability and public safety. Cyber threats targeting OT systems can result in severe consequences, including service disruptions, safety hazards, and financial losses. The complexity of railroad OT systems, coupled with their interconnectivity, presents unique challenges that require specialized cybersecurity strategies.

Cybersecurity Threats to Railroad OT Systems

Malware Attacks: Malicious software designed to disrupt, damage, or gain unauthorized access to railroad OT systems.	**Denial of Service (DoS) Attacks**: Overloading systems to disrupt operations.	**Insider Threats**: Employees or contractors with access to OT systems might intentionally or unintentionally compromise security.	**Advanced Persistent Threats (APTs)**: Prolonged and targeted cyber intrusions aimed at stealing information or disrupting operations.

Cyber Attacks Timeline

2015

Ukraine, DoS attack. An advanced persistent threat (APT) actor carried out a large-scale coordinated attack to destabilize the Ukrainian government by targeting power stations, mining and railway infrastructure. The aim of these attacks was to paralyse public and critical infrastructure by disabling industrial control systems (ICS).

2016

United Kingdom, Intrusion. Between July 2015 and July 2016, four cyberattacks were discovered on the UK railway network. After analysis, these attacks were considered as part of a reconnaissance operation before an APT (Advanced Persistent Threat) attack, probably led by a national state threat actor. No disruption or modification of data was detected.

2017

Germany, Ransomware. Deutsche Bahn was a victim of the WannaCry ransomware. Some devices were corrupted and due to this could show no information to the passengers anymore. Train operation was not disrupted.

2018

Denmark, DDoS. A DDoS attack impacted the ticketing systems of DSB. The Danish travellers could not purchase tickets from ticket machines, the online application, website and certain station kiosks. DSB estimated that approximately 15,000 customers were affected.

2020

United Kingdom, Data breach. The email addresses and travel details of about 10.000 people who used the free Wi-Fi provided UK railway stations have been exposed online. Network Rail and the service provider C3UK confirmed the incident. The database contained 146 million records, including personal contact details and dates of birth. A breach involved the app 'Indian Rail' which is a top app on the Apple App Store. It was due to an exposed Firebase database. The breach contained 2.357.684 rows of emails, usernames and plain-text passwords.

2020

Switzerland, Malware. Swiss rail vehicle manufacturer Stadler was hit by a malware attack that impacted all of its locations and may have allowed attackers to steal sensitive company data. After compromising Stadler systems, attackers reportedly infected its systems with malware that was then used to exfiltrate sensitive corporate data from breached systems.

2021

The Swiss train manufacturer, Stadler Rail, experienced a cyber attack that resulted in the theft of sensitive data. The attackers threatened to publish the stolen data if a ransom was not paid.

Railway Cybersecurity Challenges

Cybersecurity challenges in the railroad industry are multifaceted due to the complexity, scale, and critical nature of rail systems. Here are the primary cybersecurity challenges faced by the railroad industry:

1.Real-Time Requirements
Challenge: Rail operations require real-time monitoring and control, which demands cybersecurity solutions that do not introduce significant latency or disruptions.

Impact: Implementing robust cybersecurity measures without impacting operational performance is a delicate balance.

2. Legacy Systems
Challenge: Many rail systems rely on outdated technology and legacy systems that were not designed with cybersecurity in mind.

Impact: These systems can have vulnerabilities that are difficult to patch or secure, making them attractive targets for cyber attackers.

3. Interconnectivity and Integration
Challenge: Modern rail operations integrate IT (Information Technology) and OT (Operational Technology) systems, which increases the attack surface.

Impact: The convergence of IT and OT systems can lead to vulnerabilities where traditional IT threats can impact OT systems, disrupting critical rail operations.

4. Network Complexity
Challenge: Rail networks are vast and complex, with numerous interconnected subsystems, including signaling, control, communication, and passenger information systems.

Impact: The complexity makes it challenging to monitor and secure all components effectively, and a breach in one subsystem can have cascading effects.

5. Physical and Cybersecurity Integration
Challenge: Rail systems require strong integration of physical and cybersecurity measures to protect both digital and physical assets.

Impact: Ensuring that physical security measures (e.g., securing access to control rooms) are complemented by cybersecurity measures is essential but often challenging to implement comprehensively.

6. Regulatory Compliance
Challenge: Ensuring compliance with various national and international cybersecurity standards and regulations can be complex and resource intensive.

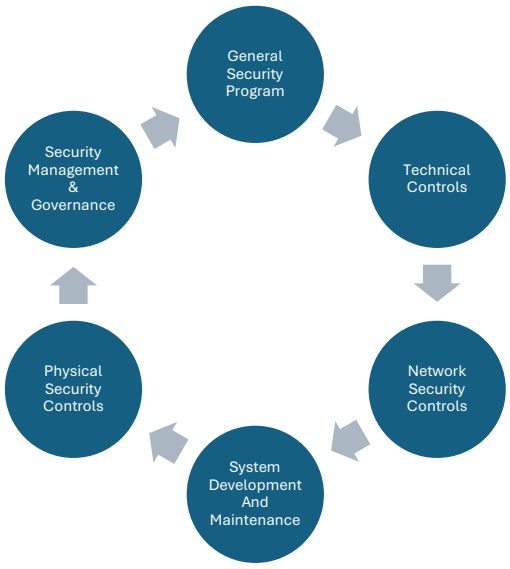
Impact: Non-compliance can result in legal penalties, but more importantly, it can leave rail systems exposed to cyber threats.

Applicable Standards and Frameworks

1. IEC 62443

International Electrotechnical Commission (IEC) 62443 is a series of standards focused on the cybersecurity of industrial automation and control systems. It provides a structured approach for securing OT systems, emphasizing risk assessment, security policies, and technical controls.

The standard includes a range of cybersecurity controls designed to address various aspects of system security. Here are some key controls outlined in IEC 62443:



General Security Program	• **Security Policy and Procedures**: ○ Establish and maintain security policies, procedures, and practices. • **Risk Assessment and Management**: ○ Conduct regular risk assessments to identify and mitigate risks to IACS. • **Personnel Security**: ○ Ensure that personnel are screened, trained, and aware of cybersecurity policies and procedures.
Technical Security Controls	• **Access Control**: ○ Implement access control measures to ensure that only authorized individuals can access IACS components and data. ○ Use role-based access control (RBAC) to assign access based on job functions. • **User Authentication and Authorization**: ○ Require strong authentication mechanisms for users and devices. ○ Use multi-factor authentication (MFA) where appropriate. • **System Integrity**: ○ Ensure the integrity of systems and data through measures like cryptographic checksums and digital signatures. • **Data Confidentiality**: ○ Protect sensitive data at rest and in transit using encryption and other confidentiality measures. • **Restricted Data Flow**: ○ Limit and control the flow of data between different segments of the IACS network. • **Timely Response to Events**: ○ Implement monitoring and logging mechanisms to detect and respond to security incidents promptly.

Network Security Controls	• **Network Segmentation**: ○ Use network segmentation to isolate critical systems and limit the impact of potential security breaches. • **Firewalls and Intrusion Detection/Prevention Systems**: ○ Deploy firewalls and intrusion detection/prevention systems to protect IACS networks. • **Secure Remote Access**: ○ Ensure that remote access to IACS networks is secure and monitored.
System Development and Maintenance	• **Security by Design**: ○ Incorporate security considerations into the design and development of IACS components and systems. • **Patch Management**: ○ Establish a patch management process to ensure that security updates are applied promptly. • **Vulnerability Management**: ○ Regularly identify, assess, and mitigate vulnerabilities in IACS components and systems. *[REPLIL INDUSTRIAL PATCH MANAGER] provides centralized visibility of OEM patches and tools to manage, deploy and report the missing, installed and vulnerable systems.*
Physical Security Controls	• **Physical Access Control**: ○ Implement measures to control physical access to IACS components and facilities. • **Environmental Controls**: ○ Ensure that environmental controls (e.g., temperature, humidity) are in place to protect IACS components.
Security Management and Governance	• **Security Leadership and Governance**: ○ Establish leadership and governance structures to oversee the cybersecurity program. • **Security Metrics and Reporting**: ○ Develop metrics and reporting mechanisms to measure and communicate the effectiveness of the cybersecurity program. • **Continuous Improvement**: ○ Implement a continuous improvement process to enhance the cybersecurity posture of the IACS over time.

2. NIST SP 800-82

National Institute of Standards and Technology (NIST) Special Publication 800-82 provides guidance on securing Industrial Control Systems (ICS), including those used in railroads. It offers a comprehensive framework for identifying vulnerabilities and implementing protective measures.

3. CENELEC EN 50159

CENELEC EN 50159 pertains specifically to the safety-related communication in railway signaling. It addresses the security aspects of communication channels to ensure the safe operation of railroad signaling systems.

Various Controls highlighted are

1. **Risk Assessment**:
Perform thorough risk assessments to identify potential threats and vulnerabilities in the communication systems.

2. **Security Requirements**:
Define and implement security requirements tailored to the specific needs and risks of the railway communication environment.

3. **System Integrity**:
Ensure the integrity of data transmitted over communication networks to prevent unauthorized alterations.

4. **Authentication**:
Implement robust authentication mechanisms to verify the identities of devices and users accessing the communication network.

5. **Confidentiality**:
Protect the confidentiality of sensitive data through encryption and other security measures to prevent unauthorized access.

6. **Access Control**:
Establish and enforce strict access control policies to limit access to the communication systems to authorized personnel only.

7. **Monitoring and Detection**:
Continuously monitor the communication systems for potential security breaches and employ detection mechanisms to identify and respond to threats in real-time.

8. **Incident Response**:
Develop and maintain incident response plans to effectively handle and mitigate the impact of security incidents.

9. **System Updates and Patching**:
Regularly update and patch communication systems to protect against known vulnerabilities and emerging threats.

[REPLIL INDUSTRIAL PATCH MANAGER] automatically test and validate the patches in "OT Patch Sandbox" to reduce operational downtimes.

10. **Security Testing**:
Conduct regular security testing, including penetration testing and vulnerability assessments, to evaluate the effectiveness of security measures.

11. **Supplier Management**:
Ensure that third-party suppliers comply with the same security standards and practices to protect the overall communication system.

12. Documentation and Reporting:
Maintain comprehensive documentation of security policies, procedures, and incidents, and report significant security events to relevant authorities as required.

4. TSA Rail Security Directives

The **Transportation Security Administration (TSA)** issues security directives for the rail sector, focusing on enhancing the cybersecurity posture of critical rail infrastructure through mandatory requirements and guidelines.

Risk based Approach provided by TSA

Reference: https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/regulations-and-guidance/safety/66201/rail-security-what-you-need-know-tsa.pdf

Important Standards to be implemented to develop complete ISMS program and cover end to end systems.

- **NIST Cybersecurity Framework (CSF)**: Provides guidelines to manage and reduce cybersecurity risks.
- **ISO/IEC 27001**: Specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
- **Federal Information Security Management Act (FISMA)**: U.S. law requiring federal agencies and their contractors to develop, document, and implement an information security program.

Essential Cybersecurity Controls for Railroad

Cyber threat protection is usually based on the principle of layered defenses, diversity in those defenses and the ability to “retreat, regroup and recover.” A successful defense-in-depth (DiD) approach requires segmenting the rail systems into clearly differentiated zones based on specific security requirements. Cybersecurity derived from informational technology (IT) system practices are capable of being applied to rail system architectures such as ERTMS, communications-based train control (CBTC), and IP-based and/or cloud-based emerging signaling designs.

Below are the recommended Essential Cybersecurity Controls for Railroads

Next Generation Firewalls for Zone Isolation & Protection as per IEC 62443

Implementing next generation firewalls provides robust zone isolation and protection, aligning with IEC 62443-3-3 SR 3.1 and SR 3.2 for network segmentation and control of data flow.

Endpoint Protection (Application Whitelisting etc.)

Endpoint protection, including application whitelisting, complies with IEC 62443-3-3 SR 7.2 by ensuring only authorized applications run on critical systems, reducing attack vectors.

Identity, Authentication, Authorization Management

Strong identity, authentication, and authorization management are essential as per IEC 62443-3-3 SR 1.2 and SR 1.3, enforcing access controls and user accountability.

Industrial Patch Management

Industrial patch management, guided by IEC 62443-2-3, ensures that all software and firmware in OT environments are up-to-date with the latest security patches, mitigating vulnerabilities and enhancing system resilience against cyber threats. This process includes identifying, acquiring, testing, and applying patches systematically to maintain the integrity and security of industrial control systems.

[REPLIL INDUSTRIAL PATCH MANAGER] follows IEC62443-2-3 Strategy with unmatched visibility into critical infrastructure vulnerable assets.

Detection of Threats using IDS Engine

Intrusion Detection Systems (IDS) are critical for detecting threats, supporting IEC 62443-3-3 SR 3.3 by providing timely identification and response to unauthorized activities.

Monitoring of Distributed Assets

Continuous monitoring of distributed assets aligns with IEC 62443-3-3 SR 4.2, ensuring real-time awareness and management of security-related events across the network.

Business Continuity & Disaster Recovery

Business continuity and disaster recovery plans, per IEC 62443-2-1, are vital for maintaining operations and ensuring rapid recovery from cyber incidents.

Digital Forensics & Incident Management

Digital forensics and incident management processes, in accordance with IEC 62443-4-2, enable thorough investigation and effective resolution of security breaches.

Physical Protection

Physical protection measures, guided by IEC 62443-3-3 SR 1.1, safeguard critical infrastructure against unauthorized physical access and tampering.

WHY REPLIL

REPLIL provides comprehensive product lines for industrial assets, using a risk-based approach to cover the entire patch management flow in alignment with DHS and IEC62443 strategies. Our offerings include:

- ***IEC62443-4-1 / IEC62443-4-2 Compliant Products***
- ***Agentless Patch Management****: Robust tools designed specifically for critical OEM systems.*
- ***Customized Reporting & Dashboards****: Tailored to meet all compliance requirements.*
- ***Centralized Management Console (CMC)****: Centralized visibility and control across distributed sites.*

REPLIL STRATEGY TO SECURE CRITICAL INFRASTRUCTURE USING IEC62443 "SL3" PRODUCTS

To ensure the security and effective management of critical infrastructure, developing a robust strategy for patch management is essential. Below is a comprehensive strategy for using REPLIL Industrial Patch Manager and REPLIL OT Patch Manager for securing critical infrastructure, along with an explanation of the importance of visibility for critical patches.

Importance:

1. Threat Mitigation

- **Timely Response**: Visibility into critical patches enables timely identification and mitigation of vulnerabilities, reducing the risk of exploitation by threat actors.
- **Prioritization**: Clear visibility helps prioritize patches based on the threat landscape and the criticality of vulnerabilities, ensuring that the most severe risks are addressed first.

2. Compliance and Auditing

- **Regulatory Compliance**: Ensuring visibility and proper documentation of critical patches helps meet regulatory and compliance requirements, which often mandate timely vulnerability management.
- **Audit Trails**: Visibility into patching activities provides a clear audit trail, demonstrating due diligence in maintaining a secure infrastructure.

3. Operational Integrity

- **Minimized Downtime**: With visibility into which patches are critical and which systems they affect, organizations can better plan and execute patching activities without causing significant operational downtime.
- **Resource Allocation**: Proper visibility allows for more efficient allocation of resources, ensuring that critical patches receive the attention and urgency they require.

Features:

REPLIL INDUSTRIAL PATCH MANAGER (IPM)	REPLIL OT PATCH SANDBOX (OPS)
Risk-Based Patch Prioritization • **Criticality Assessment**: Categorize patches based on the criticality and risk associated with each asset. Patches that address vulnerabilities in high-risk or high-value assets should be prioritized. • **Impact Analysis**: Evaluate the potential impact of deploying patches on operational continuity. Prioritize patches that fix critical vulnerabilities without significantly disrupting operations. **Scheduled Patch Deployment** • **Patch Scheduling**: Develop a patching schedule that aligns with operational	**Testing and Validation** • **Pre-Deployment Testing**: Test patches in a controlled environment that replicates the production setting to ensure compatibility and effectiveness. This step helps identify potential issues before full deployment. • **Post-Deployment Validation**: Conduct thorough post-deployment checks to verify that patches have been successfully applied and that they do not negatively impact system functionality. • **Advance Test Cases**: Automatically execute, test & validate (desktop / web)

downtimes to minimize disruptions. Utilize maintenance windows or planned downtimes for deploying critical patches. • **Phased Rollouts**: Implement patches in a phased manner, starting with less critical systems to observe any unforeseen impacts before deploying to critical systems. **Automated Patch Management** • **Automation Tools**: Utilize Replil Industrial Patch Manager and Replil OT Patch Manager to automate the patching process. Automation ensures timely patch application and reduces the risk of human error. **Continuous Monitoring**: • Implement continuous monitoring to detect new vulnerabilities and assess the need for patches in real-time. Automated alerts can help promptly address critical vulnerabilities.	based critical applications expected state before & after the installation of a patch.

Click for more details

REPLIL Industrial Patch Manager | REPLIL OT Patch Sandbox

Book a demo to secure critical infrastructure: sales@replil.com