Securing Critical OT Systems in a Railroad – Pitfalls and Best Practices

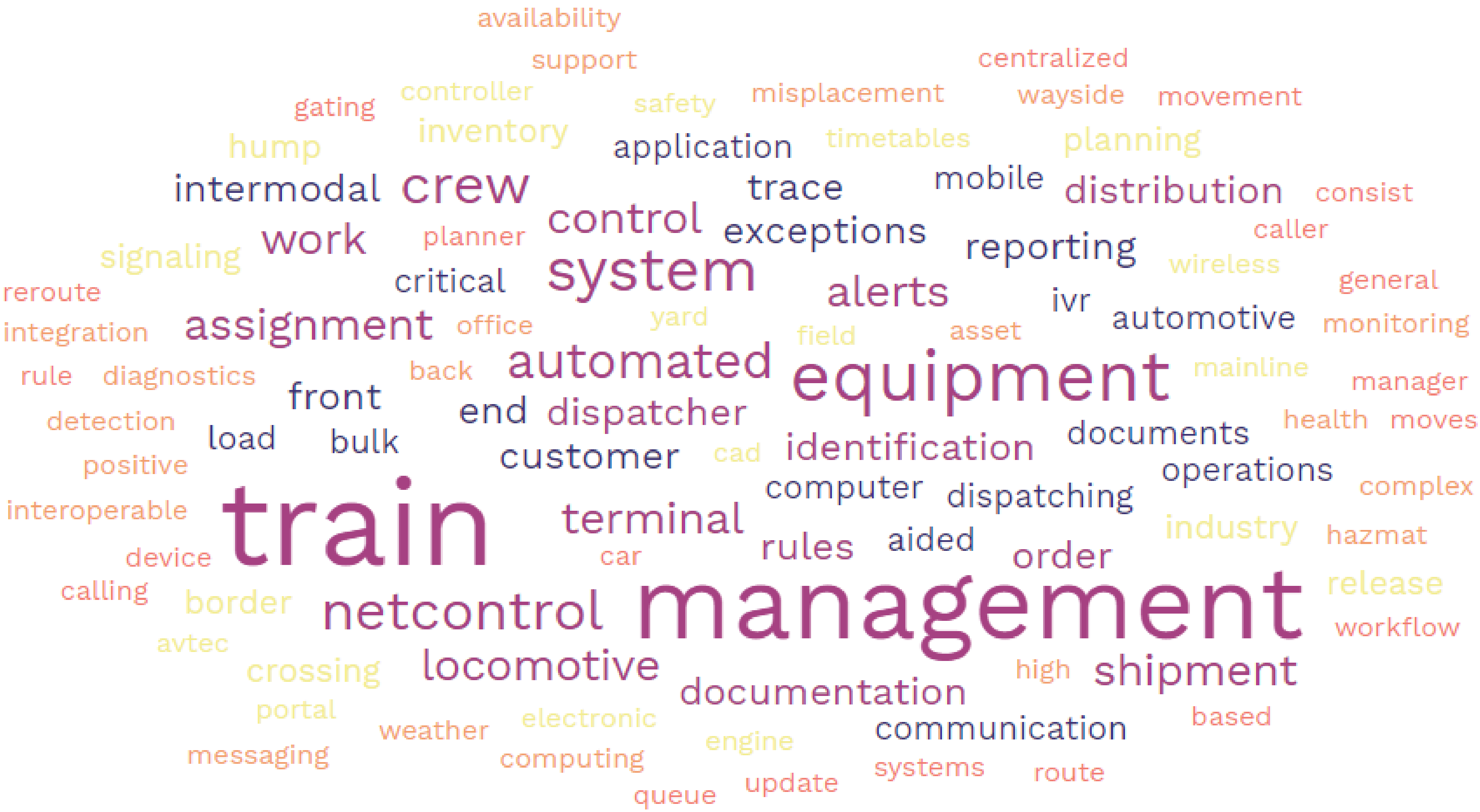
Graham Nasby, Sr. Manager - OT Security Architecture, CN Rail

May 23-24, 2023 – Third Annual Rail Cybersecurity USA – Chicago Illinois USA

How do you define Operational Technology?

How does your organization define OT?

What does “critical” mean to you? To others?



availability
support centralized
gating controller safety misplacement wayside movement
hump inventory application timetables planning
intermodal crew trace mobile distribution consist
work planner control exceptions reporting caller
signaling critical system alerts ivr wireless general
reroute
integration assignment office yard field asset automotive monitoring
rule diagnostics back automated equipment mainline manager
front end dispatcher
detection health moves
load bulk customer cad identification documents
positive operations
computer dispatching complex
interoperable train terminal industry
rules aided hazmat
device car order
calling border netcontrol management release
avtec workflow
crossing locomotive high shipment
documentation
portal electronic based
weather communication
engine
messaging computing
systems route
update
queue

Key Components of a Rail OT Cyber Security Program

What are you protecting?

1. Clear definition of what is OT
2. High Level Systems Inventory
3. Process for Classifying Systems: IT, OT or in-between
4. Process for Determining Criticality
5. Identify Risk Scenarios for your Critical Systems
6. OT Asset Inventory
7. Keeping Documentation up to date

Tooling & Process

1. Establish OT Cyber Security Policy - leverage NIST framework
2. Automated OT Asset Inventory Tooling
3. Server and End-Point Protection
4. Active Vulnerability Management: Scanning, Anti-Virus
5. Network and Firewall Monitoring
6. Patching Program
7. Patching Program to Manage Hard to Patch Systems
8. Penetration Testing and Vulnerability Testing Program

Building More Robust Systems

1. System Lifecycle Management
2. Network Segmentation & Active Firewalls Between Zones
3. Managing OT system access and user accounts
4. Software Architecture Standards, Positions and Templates
5. Security Architecture Standards, Positions and Templates
6. Security Reviews
7. Building in Event Logging / Monitoring

Tooling & Process

1. Identifying Risks to OT Systems
2. Developing Controls to Mitigate Risks
3. Company-wide Security Standards
4. Regular Security Reviews
5. Documenting and Regularly Reviewing Exceptions
6. OT-specific threat intelligence and education programs
7. Building OT intelligence into a Security Operations Centre
8. OT Incident Response – Working with Internal OT Teams

“Taking the time to understand what each OT system does, it’s risk profile, the team that owns it, and how it affects operations”

Some Common OT Cyber Security Pitfalls

1. Trying to manually maintain OT Asset Inventories without Automated Tools
2. Trying to keep OT Systems Fully Air-Gapped – thinking it is too risky to add connectivity to monitor them
3. Having too few OT network zones and/or having too firewall rules that are not nuanced enough
4. Not having additional protections and controls for OT user accounts
5. Not keeping track of Vulnerabilities / Patches for Older OT Systems
6. Not Regularly Reviewing Older Systems and Regularly Documenting What can be Patched (and what can't)
7. Missing documentation & drawings for OT Systems or (worse) trying to keep too many documents up to date
8. Not regularly reviewing "break glass" procedures used to access OT systems in an emergency
9. Feeding Logs from OT systems directly into an IT-focused Security Operational Centre without context
10. Relying only on IT-focused vulnerability alerts/notifications for OT systems
11. Not having Vendor Support Agreements in place for operational OT systems
12. Not Engaging with internal OT System owners to better understand how their systems work and their needs

Some OT Cyber Security Best Practices

1. Take the time to understand how various OT systems are used, what they do, and their impact on operations
2. Maintain both a high-level and detailed listings of OT systems and the assets in them
3. Use OT-focused Automated Tools for doing OT Asset Inventory, but be careful with automated scanning tools
4. Have a clear definitions for “OT” and “critical” and have documented processes for classifying systems
5. Use Network Segmentation & Firewall Rules to separate OT systems, including back-office and field segments
6. Have additional protections for OT user accounts, particularly for admin/technician access to OT systems
7. Design redundancy into OT systems, so that if IT systems have an issue, OT systems can continue to function
8. Have a Strong OT Security Policy Framework with Policies, Standards, Guidelines, Positions, and Patterns
9. Provide a process for documenting, and regularly reviewing any exceptions needed for specific OT systems
10. Use Compensating Controls when legacy OT systems cannot accommodate modern cyber security controls
11. Use OT-focused tools to implement server and end-point vulnerability detection and protection
12. Provide system development teams with security architecture requirements, positions and patterns

CN