Evaluating Operational Technology & Transit Systems Outages

Report #: 2023-08

Executive Summary

Operational Technology (OT) systems, inclusive of Supervisory Control and Data Acquisition (SCADA) systems and Transit Systems, facilitate the safe and efficient operations of ST rail systems, stations, garages, and other facilities.

The systems and networks monitor, alert, and control various functions such as Fire, Life and Safety systems, security cameras, access control, train position and more. These systems are managed collaboratively between Operations (OPS) and Information Technology (IT) and are supported by various agency groups including the Portfolio Services Office (PSO) and partners at King County Metro (KCM).

Audit Objective

We audited OT & Transit Systems to ensure acceptable system outage frequencies and durations were clearly defined, and actual outages were within these limits. This evaluation included analysis of roles, responsibilities, resolution processes, key performance indicators (KPIs), and any service impacts or incidents from January 2021 to August 2023.

Audit Results

From January to August 2023, Sound Transit encountered 12 major incidents, resulting in over 90 hours of operational system outages. These incidents caused functions such as the Emergency Fan Network, Uninterruptable Power Supply, Train Control systems and others to go offline for an average of 7.5 hours per incident.

It was found that key performance indicators (KPIs) for the acceptable number of incidences or duration of incidences were not defined or shared among stakeholders.

Finding: No defined acceptable range of system disruption time and frequency.

In 2023 there have been consistent system outages and acceptable ranges for outage frequency and duration have not been defined. We found that work is in progress to create cross-departmental standards and key performance indicators for OT and Transit Systems; however, work is not yet complete.

Observation: Current processes are not aligned with best practices

The agency could move beyond impact mitigation and further progress towards ‘best-in-class’ system management through benchmarking with peers and alignment with industry best practices.

Audit Results

The following table summarizes the analysis performed and the associated exceptions:

Analysis Performed	Results	Finding or Observation
Analysis of 2023 “Major Incidents”	Sound Transit experienced 12 ‘major incidents’, causing system outages with an average duration of 7.5 hours from January to August 2023.	**Finding 1**: No defined acceptable range of system disruption time and frequency.
Comparison of current state to best practices (APTA, ISO, NIST) and other transit agencies.	Current practices do not align with the best practice standards and have not been benchmarked against peers.	**Observation 1**: Current processes are not aligned with best practices

Positive Practices

During the audit we observed the following positive practice and continuous improvements:

- Continuous improvement and updating of available ‘how-to’ documentation for system management by the Operations Technology group.
- Commitment and dedication first and foremost to passenger safety and restoration of operations by all stakeholder groups.

<u>Finding #1: No defined acceptable range of system disruption time and frequency (3A – High)</u>

We found that from January to August 2023[1], Sound Transit encountered 12 major incidents, resulting in 90 hours and two minutes of operational system outages[2]’. On average, there were 1.5 incidents per month, each lasting around 7.5 hours. These incidents sometimes affected multiple systems simultaneously while others were isolated to only one system.

Our research of these incidents found that there were no defined Key Performance Indicators (KPIs) or an acceptable number of disruption occurrences or duration of system outages shared among primary stakeholder groups. Although IT maintains ‘Service-Level Agreements’ for expected services and resolution when outages occur, other stakeholders stated that they were not aware of any defined acceptable durations or frequencies.

In lieu of KPIs or other rating definitions for expected average resolution, we utilized our risk rating ‘frequency’ scale to evaluate the observed conditions. The average frequency and

[1] From January 1st through August 8th of 2023.

[2] IT defines a ‘Major Incident’ as “the highest-impacting, highest-urgency unplanned outage or issue that causes a business disruption. At Sound Transit, a Major Incident can directly affect users or be any level of degradation that brings a risk of work stoppage, impact to transportation schedules, safety, and/or financial implications. Any (non-VIP) Priority 1 or Priority 2 Incident.”

duration of events for 2023 suggests a “High” risk rating of “3A” (refer to *Appendix B: Audit Finding Risk Rating Process*).

Recommendation:

We recommend agency management consider establishing clear, objective KPIs or other metrics developed jointly and agreed upon by primary stakeholders of OT and Transit Systems.

These KPIs should help meet the informational needs to make data-informed decisions and identify when risk tolerances have exceeded an acceptable level; allowing appropriate next steps to be taken. We suggest using data from other transit agencies and authorities to learn about what peer agencies have defined as acceptable and how it has affected their operations.

Observation #1: Current processes are not aligned with self-identified best practices and standards.

Information Technology’s Information Security group (known as InfoSec) and the Operational Technology (OT) group have developed a manual, consisting of 12 sub-manuals that outline the ideal management of operational systems in areas such as Data Management, Physical Security and Access Management, among others.

In these documents the groups identify areas where the practices outlined align with the NIST 800 series and ISO 27002:2017 standards for Information Security. However, as we observed throughout our audit, these standards are largely not being met. Additionally, OT strives to meet or exceed the American Public Transportation Association (APTA) standard “Securing Control and Communications Systems in Transit Environments”.

Moreover, some stakeholders have adopted standards like IEC 62443 (for security for Industrial automation and control systems), although not all have done so.

There is an opportunity for the agency to re-examine its practices, benchmark itself and compare practices to peer transit agencies, and re-align processes to better reflect industry best practices and create consistency across the agency.

Background

Operational Technology systems, which include Supervisory Control and Data Acquisition (known as SCADA), and other Transit Systems work together to monitor, alert and control critical aspects of operating ST rail systems, stations, garages, and other facilities in a safe and efficient manner. The systems and networks run on monitor, alert, and control a variety of functions such as Fire, Life and Safety systems, CCTV cameras, access control, train position, communication, and information systems, and more.

These systems are managed collaboratively between different groups at Sound Transit including the Operational Technology (OT) group, Information Technology (IT) group, contracted staff with King County Metro (KCM) and support from ST's Portfolio Services Office (PSO). Together, these groups ensure that day-to-day operational networks remain running, and that the agency can operate a safe and efficient service for riders.

The operational systems and networks work in conjunction to gather information, distribute it across the core ST network to other networks, systems, and staff who monitor for any issues. Most systems are connected through a core network, some being directly connected, some with limited connection and others that are isolated from the network. This helps protect operational systems such as SCADA and Transit Systems from external intrusion.

This structure also adds complexity and a need for increased coordination among groups to ensure that all systems are operating as intended and that issues are diagnosed and resolved quickly to restore operations. Consistent processes and defined ownership aid in securing these systems both physically and technologically to help ensure that they are not influenced by error or bad actors.

For this audit, we examined 36 operational systems. Across those systems, 15 unique primary stakeholder groups or divisions were identified. Those 15 stakeholder groups are directly involved in the design, operation, or management of their respective systems.

Methodology

Standards

We conducted this performance audit in accordance with our charter and Generally Accepted Government Auditing Standards (GAGAS or "Yellow Book") issued by the United States Government Accountability Office (GAO), the International Standards for the Professional Practice of Internal Auditing and the Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF or "Red Book") which includes the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the International Standards for the Professional Practice of Internal Auditing (the Standards), and the Definition of Internal Auditing.

These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Also, the Audit Division is committed to following safety oversight standards set forth by the Federal Transit Administration (FTA), Federal Railroad Administration (FRA), and all other relevant auditing requirements or standards.

Audit Processes

Our audits are risk-based and focus on the areas with the highest potential risk impacts or likelihood at the time of observation. Each audit starts by examining the current processes in place relative to (1) Laws or Regulatory Requirements, (2) Agency Policies and Procedures and (3) Industry Best Practices. During the “Planning” phase, we assess the engagement-specific conditions and risk, which informs the engagement objectives and scope. Relevant controls to mitigate these risks are also identified.

The audit “Field Work” phase then examines the design of the identified controls to determine if the intent meets the regulations, policies, etc. If the controls are designed to adequately mitigate the risk (control environment), we move on to assess the degree to which the controls are mitigating the risk (control activities). Any areas identified where the control environment or activities do not adequately mitigate the identified risk are identified as an exception. Exceptions are then defined as Findings if they are significant or Observations if they are an opportunity for improvement.

All Findings are risk-rated based on potential likelihood and impact based on attributes outlined in the appendices of this report.

Diversity, Equity, and Inclusion Review

During this audit we considered whether there were inequitable impacts to any specific stations or systems, as well as whether resources appeared to be distributed in an equitable manner.

We noted no (0) instances of disproportionate impacts or distribution of assets or resources related to OT or Transit Systems within the scope of this audit.

Appendices

Appendix A: Sound Transit's Title VI notice of rights

Sound Transit conducts Title VI equity analyses for service and fare decisions to ensure they are made as equitably as possible.

More information on Sound Transit's Title VI notice of rights and the procedures to file a complaint may be obtained by:

- Phone: 888-889-6368; TTY Relay 711.
- Email: stdiscriminationcomplaint@soundtransit.org;
- Mailing to Sound Transit, Attn: Customer Service, 401 S. Jackson St. Seattle, Washington 98104-2826; or
- Visiting our offices located at 401 S. Jackson St. Seattle, Washington 98104.

A complaint may be filed directly with the Federal Transit Administration Office of Civil Rights, Attention: Complaint Team, East Building, 5th Floor – TCR, 1200 New Jersey Avenue, SE, Washington, DC 20590 or call 888-446-4511.

Report Prepared by:

Kayla Schoonhoven Digitally signed by Kayla Schoonhoven
Date: 2024.02.29 10:20:19 -08'00'

Kayla Schoonhoven, Sr. Performance Auditor (Lead Auditor)

Reviewed (QA/QC) by:

Heather F. Wright Digitally signed by Heather F. Wright
Date: 2024.03.04 09:29:42 -08'00'

Heather Wright, Deputy Director, Audit Division

Approved for release by:

Patrick Johnson Digitally signed by Patrick Johnson
Date: 2024.03.04 09:47:54 -08'00'

Patrick Johnson, Director, Audit Division

Appendix B: Audit Finding Risk Rating Process

To aid process owners in prioritization of the audit findings resulting from the audit, a level of audit risk will be assigned by assessing two factors: 1.) The probability that the associated problem will occur in the future, and 2. the impact or severity of that problem in relation to the overall business process.

Using the same Risk Assessment Matrix already in used throughout the agency and based on the MIL-STD-882-E; audit findings are qualitatively assessed based on the worst credible case that is anticipated from the result of human error, design inadequacies, component failure or a malfunction.

Risk Rating Scale

	Severity	Catastrophic (1)	Critical (2)	Major (3)	Marginal (4)	Negligible (5)
Probability	Frequent (A)	High (1A)	High (2A)	High (3A)	Serious (4A)	Medium (5A)
	Probable (B)	High (1B)	High (2B)	Serious (3B)	Serious (4B)	Medium (5B)
	Occasional (C)	High (1C)	Serious (2C)	Serious (3C)	Medium (4C)	Low (5C)
	Remote (D)	Serious (1D)	Medium (2D)	Medium (3D)	Low (4D)	Low (5D)
	Improbable (E)	Medium (1E)	Medium (2E)	Low (3E)	Low (4E)	Low (5E)
	Eliminated (F)	**Eliminated**				

Resolution Requirements

Risk Score	Risk Level	Risk Rating	Minimum Actions	Risk Acceptance / Responsibility
1A, 1B, 1C, 2A, 2B, 3A	High	Unacceptable	Stop work & immediate correction required to reduce risk.	Not Acceptable. Executive Team is informed.
1D, 2C, 3B, 3C, 4A, 4B	Serious	Undesirable	Mitigation strategy required to reduce risk within 30 days of identification of risk.	Acceptable with risk controls and monitoring. Director-level committee review and approval.
1E, 2D, 2E, 3D, 4C, 5A, 5B	Medium	Acceptable w/ review	Monitor and consider actions to further reduce risks.	Acceptable with risk controls and monitoring. Technical Level committee review and approval.
3E, 4D, 4E, 5C, 5D, 5E	Low	Acceptable	Acceptable without further mitigation. May be accepted by the business unit in coordination with Audit and Safety.	Acceptable without further mitigation. May be acceptable by the business unit with coordination with Audit and Safety.
N/A	Eliminated	Eliminated	No actions needed.	N/A

Risk Matrices

Severity	**Catastrophic (1)**	**Critical (2)**	**Major (3)**	**Marginal (4)**	**Negligible (5)**
System Disruption / Operations	> 24 hrs. Substantial or total loss of operations	12 – 24 hrs. Partial shutdown of operation	4 – 12 hrs. Prolonged disruption of operations	1 – 4 hrs. Brief disruption of operations	<1 hour Minor to No disruption
Financial	>$5,000,000	$1,000,000 – 4,999,999	$249,999 – 999,999	$10,000 – 249,999	< $10,000
Reputational	Prolonged negative media coverage for >30 days and / or irreparable reputational damage, resulting in government intervention	Ongoing negative media coverage for >14 days but ≤ 30 days causing serious reputational damage, resulting in government intervention.	Ongoing negative media coverage >7 days but ≤14, causing major reputational damage and possible government intervention	Ongoing negative media coverage for ≥ 24 hours but ≤ 7 days, causing some reputational damage	Negative media coverage for ≤ 24 hours, causing minor reputational damage
Injury	Several deaths (≥3) and / or numerous (≥3) serious injuries (excluding suicides or by natural causes)	1 -2 deaths and/or 2 or more serious injuries	Multiple minor injuries and possible serious injury (Ambulance transport)	Minor injury such as bruising, abrasions, bleeding; possible medical services required	No injuries
Equipment	Total loss of equipment or system interruption requiring more than 30 days to repair.	Significant loss of equipment or system interruption requiring more than 14 days but less than 30 days to repair.	Some loss of equipment or system interruption requiring more than 24 hours but less than 14 days to repair.	Minor system loss of equipment or system interruption requiring less than 24 hours to repair.	Minor damage to equipment or minor system interruption with no immediate repair necessary.
Regulatory	Cease and desist orders are delivered by regulators. Critical assets and facilities are forced by regulators to be shut down.	Governmental, regulator investigations, and enforcement actions, lasting longer than a year. Violations that result in multiple large non-financial sanctions; **OR** Regulators force the removal and replacement of management positions. Regulators begin agency monitoring activities.	Violations that result in significant fines or penalties above and beyond what is codified or a regulator enforces non-financial sanctions; **OR** Significant new and updated regulations are enacted as a result of an event.	Violations that result in fines or penalties	Self-reported or regulator identified violations with no fines or penalties

Probability Level	Likelihood of event in specific item	MTBE in Operating Hours **	Occurrence in time
Frequent (A)	Will occur frequently.	<1,000 oh	1 per week, likely to occur several times per month
Probable (B)	Will occur several times.	1,000 – 100,000 oh	1 per month, likely to occur several times per year
Occasional (C)	Likely to occur sometime.	100,000 – 1,000,000 oh	Once per year, likely to occur several times within 10 years
Remote (D)	Unlikely but possible to occur.	1,000,000 – 100,000,000 oh	1 per 10 years or likely to occur several times within 100 years
Improbable (E)	So unlikely, occur may not be experienced.	>100,000,000 oh	1 per 100 years
Eliminated (F)	Risk removed / eliminated	Never	N/A

Appendix C: Management Response

Prepared by: Scott Bash

Date: February 28, 2024

Audit: Evaluating Operational Technology & Transit Systems Outages Audit (AUD-PA-2023-08 OT & Transit Systems)

Management Response:

Management agrees with the audit report finding.

Finding #1: No defined acceptable range of system disruption time and frequency (3A – High)

Management Response / Action Plan:

Thank you for the opportunity to respond to the OT & Transit Systems Audit that addresses the Operational Technology (OT) systems, inclusive of Supervisory Control and Data Acquisition (SCADA) systems and Transit Systems. Management agrees that Key Performance Indicators (KPI) are needed for individual systems including overall availability and business continuity. It is also recommended that an Agency operating philosophy should be reviewed against the Core Systems architectures (e.g., redundancy) to determine if system changes are required to meet current and future operational needs. System stewards should be assigned, and the roles and responsibilities formally documented for all parties supporting these OT core systems.

PSO Engineering is leading efforts to develop an asset management plan for the network and systems. This corrective action work should be part of that effort. The coordination of the OT & Transit Systems requires stakeholder involvement across many teams within Sound Transit, King County, and other external partners that support and maintain the systems. The collection of OT & Transit system domain includes approximately 40 systems. This effort will need to be prioritized to address the most critical systems first.

<u>Timeline for corrective action</u>:

Management has determined the following steps should remediate the audit findings:

1. Operations to prepare a Concept of Operations (CONOPS) document for the Link Core Systems that describes a proposed system concept and how that concept would be operated in the intended environment. The development of the CONOPS will require Operations, Information Technology, and the PSO Engineering teams to collaborate and communicate the vision for the operational system to meet the requirements of the system users and applicable regulations and codes. (Late Q2 2025)
2. Operations to lead the effort to document all roles and responsibilities in supporting the Core Systems (Late Q4 2024)
3. Operations to form a group comprised of major stakeholders to determine KPIs and document the process for tracking, reporting, and analyzing the metrics (Early Q3 2025)
   - Work to determine KPIs related to acceptable downtime of Transit System Core Systems (SCADA and OT systems)
   - Establish a business process to publish acceptable downtime requirements.
   - Define the process to collect, report, and analyze the metrics on a periodic basis.
4. Operations to lead efforts to develop a plan to address all technology changes to meet KPIs and determine the accountable parties for the execution of the work. (End of Q4 2025)