APTA STANDARDS PROGRAM

RECOMMENDED PRACTICE

APTA SS-ISS-RP-008-24

First Published: May 8, 2024

Infrastructure and Systems Security Working Group

Safety and Security Certification

Abstract: This recommended practice provides guidance for managing and monitoring the safety and security certification (SSC) process for transportation systems and changes to system elements.

Keywords: accountable executive, as low as reasonably practicable (ALARP), building, bus rapid transit, capital improvement, capital project, certification, chief safety officer, concept, contractors, cybersecurity, design, design-build, design–bid–build, development, equipment, fixed guideway, hazard, major capital project, New Starts, nonrevenue vehicles, on-track equipment, organizational structure, planning, procedure, procurement, public-private partnerships, quality assurance, rail vehicles, right-of-way, risk, rulebook, rules, safety, safety assurance, safety-critical, schedule, security, Small Starts, SMS, structure, system modification, training, validation, verification

Summary: Safety and security certification (SSC) encompasses the series of processes that collectively verify the safety and security readiness of a project for public use. Since the November 2002 release of FTA-MA-90-5006-02-01, *Handbook for Transit Safety and Security Certification*, the public transportation industry has experienced significant project development and implementation changes that have impacted SSC approaches. This document summarizes and expands upon the Federal Transit Administration's SSC requirements to provide transit agencies guidance to support the management and monitoring of SSC processes.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the Infrastructure and Systems Security Working Group as directed by the Security Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

This is a new document.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Infrastructure and Systems Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Kevin Jones, Chair, *ADS System Safety Consulting*

Marsha Anderson Bomar
Michelle Appelbaum, *WSP*
Onala Atala, *AECOM*
Marla Blagg, *TriMet*
Louis Brown, *Jacobs*
John Cockle, *Kiewit Engineering*
Steven Culp, *MBTA*
Richard Czeck, *Detroit DOT*
Holly Durso, *Hatch LTK*
Ronald Edwards, *ADS System Safety Consulting*
Jason Eng, *San Francisco BART*
Thomas Eng, *LACMTA*
Ronald Ester, *MBTA*
Rebecca Frankhouser, *King County Metro*
Kevin Franklin, *San Francisco BART*
Polly Hanson, *APTA*
Walter Heinrich, *K&J Safety Consulting*
Patrick Johnson, *Sound Transit*
Jenny Kane, *Metra*
Michael Kram, *CapMetro*
Paul Lemke, *MARTA*
Thomas Lentz, *STV*
Claudia Mandurino, *Hitachi Rail STS*
David Mayer, *WMSC*
Pamela McCombe, *HNTB*
Andrew McKinnon, *Toronto Transit Commission*
Matthew Mitchell, *Sound Transit*
David Morgan, *STV*
Juan Morrison, *formerly Dovetail Consulting*
David Moskowitz, *Charlotte Area Transit System*
Vivian Papen, *STV*
Will Pelleteri, *Hatch LTK*
Kevin Reilly, *Hatch LTK*
Joyce Rose, *WSP USA*
Gerry Ruggiero, *ADS System Safety Consulting*
Harry Saporta, *WSP USA*
Nagal Shashidhara, *NJ Transit*
Michael Smith, *New Orleans RTA*
Gardner Tabon, *CapMetro*
Joseph Thampu, *Toronto Transit Commission*
Phillip Thomas, *Maryland Transit Administration*
Justin Vonashek, *MTA Metro-North Railroad*

Project team

Brian Alberts, *American Public Transportation Association*
Brian Heanue, *American Public Transportation Association*
Eugene Reed, *American Public Transportation Association*
Narayana Sundaram, *American Public Transportation Association*

Introduction

This introduction is not part of APTA SS-ISS-RP-008-24, "Safety and Security Certification."

Public transportation systems must place the safety and security of their workers, passengers and patrons; the general public; the environment; and their property above other interests throughout the life cycle of a system element. While the conceptualization, development and implementation of a system or system element typically occupies only a small portion of the life span of a system, decisions made during these life cycle phases can have profound impacts upon the safe, secure, and cost-effective use of the system for years or decades to come. To minimize safety and security risks to all stakeholders and interfacing systems, transportation systems must dedicate time and effort to ensuring that wise decisions are made during

conceptualization and development and must ensure that an assessment of the safety and security of the new system or system change is executed by the agency's safety function before placing the system into service.

The FTA specifies in various regulations and associated circulars which applicable systems and system changes must be safety and security certified before placing the system into service. The FTA makes recommendations in several guides, handbooks and interpretative documents when new systems and system changes should be safety and security certified before placing the system into service. Appendix A includes a summary of these regulations and recommendations.

Scope and purpose

This document describes recommended approaches for managing and monitoring the safety and security certification effort in transportation systems as required by the Federal Transit Administration. This recommended practice consolidates safety and security certification requirements and recommendations into a single document, clarifies the scope of the process, and provides recommendations to expand the process beyond rail transit.

Safety and Security Certification

1. Introduction

Integrating safety and security certification for transit projects and procurement facilitates Safety Risk Management (SRM) program to manage transit safety risks actively and follows the process for identifying, evaluating and mitigating safety risks in consideration of Safety Management System (SMS) principles. By implementing safety and security certification for transit projects, transit agencies can meet risk management requirements, managing and mitigating safety and security risks and hazards to an acceptable level, as defined in an agency's safety plan.

Safety and security certification (SSC) encompasses the series of processes that collectively verify the safety and security readiness of a project for public use. For instance, new or altered safety-critical systems have the potential to cause significant harm or damage if subsystems and components do not meet safety and security objectives and requirements. Thus, transit agencies should adopt a formal top-down approach for managing and mitigating safety and security risk.

In pursuing safety and security certification, transit agencies should align relevant agency policies, system design components, operations protocols and maintenance procedures to mitigate safety and security risk. Supporting activities include properly identifying physical, functional and operational characteristics of structures, systems and components (including software and firmware) to ensure that transit agencies properly identify, control and record physical and cybersecurity additions and changes for new and existing facilities.

The SSC process typically ends with the appropriate transportation agency leadership (such as the accountable executive and the chief safety officer [CSO]) certifying that the safety and security risks associated with the new system or system change are as low as reasonably practicable (ALARP) and authorizing the use of the system. At times, the safety and security certification process may also include concurrence by external regulatory bodies such as the Department of Transportation, Federal Transit Administration, Federal Railroad Administration, Department of Homeland Security, Transportation Security Administration, or state safety oversight agencies (SSOAs).

In addition, while not a specific objective of the certification process, identifying the system's attributes supports the inclusion of these elements as capital assets in an agency's transit asset management (TAM) system. Likewise, transit agencies can use the capstone readiness assessment of the certification process to verify that all new or modified transit assets are included in the TAM system, which will support controlled configuration and timely maintenance.

Finally, the safety and security certification process is an effective means of evaluating proposed changes to transit systems. Transit agencies should integrate safety and security certification into their change management and continuous improvement processes.

2. Safety and security certification framework

Safety and security certification employs standard processes and methodologies that cover a variety of project types. Transportation agencies should tailor these concepts as appropriate to their project's factors, such as scope, complexity and delivery method.

Transit agency safety and security decision-makers are responsible for deciding if a project is subject to safety and security certification and how the agency may tailor the certification approach. Agencies should evaluate all relevant projects regardless of the project approach (e.g., design–build, turnkey). Transit agencies should determine and document decisions based on relevant FTA and FRA regulatory and guidance documents, applicable SSOA requirements, a clear understanding of project details, institutional knowledge of the agency's systems, and knowledge of past incidents and safety analysis concepts.

2.1 Agency safety and security certification program

Prior to commencing a project requiring safety and security certification, transit agencies should address their overarching approach for creating a Safety and Security Certification Plan (SSCP), identifying an individual to manage the safety and security certification process, controlling safety and security certification documents, establishing committees and/or working groups, and addressing budgets and contractual requirements.

2.1.1 Create an Agency Safety and Security Certification Plan

The transportation agency should establish an overarching SSCP that defines the overall thresholds, processes, activities, and roles and responsibilities for safety and security certification at the agency. This document should provide a general framework within which project-specific SSCPs should align. The agency SSCP should also address agency nuances associated with certification of rail, bus, non-major capital and other relevant projects, and clearly outline how to handle contingencies, design and construction changes, and emergency work.

2.1.2 Manage the safety and security certification process

Transit agencies should appoint an individual to manage the safety and security certification process as described in the agency's Safety and Security Certification Plan. Transit agencies may assign an individual the management of safety and security certification as their sole responsibility or as one of multiple position responsibilities. Agencies may also assign safety and security managers on a project-by-project basis. For the purposes of this recommended practice, the individual assigned to manage this process will be called the safety and security certification manager (SSCM).

The SSCM has project-level independent oversight of the safety and security certification process and facilitates several of the activities related to certification. The SSCM can be internal or external to the organization. SSCMs should undergo training (e.g., Public Transportation Safety Certification Training Program (PTSCP)), as required by transit or federal agencies.

If using contractor support for the SSCM position, transit agencies should begin vetting prospective SSCMs during the planning phase. Typically, SSCM candidates submit resumes detailing their experience working with safety and security certification and the selected project delivery method.

SSCM responsibilities may include the following:

- Developing the project-specific SSMP or Safety and Security Certification Plan.
- Developing the preliminary hazard analysis (PHA) and threat and vulnerability assessment (TVA) and overseeing the risk mitigation process.

- Developing other risk assessment analyses, such as the operating hazard analysis (OHA).
- Facilitating PHA, TVA and OHA workshops.
- Developing the risk assessment reports.
- Organizing project level safety and security certification meetings.
- Developing the Safety and Security Certification Verification Report (SSCVR).

The SSCM should work alongside the project team to verify completion of all safety and security milestones. As the project transitions from design to construction verification, the SSCM should review the hazards in each design package for potential safety or security issues and open items or exceptions.

2.1.3 Control of safety and security certification documents

For traceability and auditing purposes, transit agencies should establish document control methods to confirm that the agency captures, tracks, updates, distributes, reports and stores all project documentation. The SSCM should be responsible for maintaining document control and official project document files related to safety and security certification. Similarly, the SSCM should be responsible for processing and logging all project correspondence and documentation in central files and distributing documentation to designated project personnel. Therefore, the transit agency should inform personnel to include the SSCM on all relevant correspondence and forward all project documentation to the SSCM.

Some material related to agency and project-specific safety and security certification may be sensitive security information (SSI). Transit personnel should follow their agency's SSI policy. See APTA SS-ISS-RP-002-21, "Sensitive Security Information Policy," for more information about protecting SSI information.

2.1.4 Establish safety and security certification committees and/or working groups

Transit agencies should establish committees and/or working groups to support safety and security certification activities that both integrate with the agency's existing safety and security committee structure and remain flexible and scalable to specific project needs and activities. The SSCM should work closely with the project team to confirm that the project regularly updates relevant safety and security certification teams and seeks reviews and approvals as required.

While the names and composition of these groups will vary from agency to agency, transit agencies should organize responsibilities similar to the following:

- **Safety and Security Certification Review Committee (SSCRC):** This leadership group is responsible for accepting and certifying safety and security elements. This committee may be part of another standing safety and/or security committee (e.g., at a smaller agency) or be solely responsible for certification oversight. This committee provides internal oversight, ensuring that related safety and security elements comply with applicable guidelines and integrate with existing agency standards for maintaining a safe and secure transportation system. Committee membership may vary from agency to agency but could include the chief safety officer, chief operating officer, chief engineer, chief financial officer and chief of police. This group should act on recommendations from the project's Safety and Security Certification Working Group (SSCWG). The accountable executive should issue this committee's decisions.

- **SSCWG:** This is a project-specific multidisciplinary group responsible for managing and coordinating all safety and security certification activities, reviewing safety-related test results, verifying a project's safety and security, and recommending approval of certification elements to the SSCRC before the elements enter service. Members of the group should include a wide range of experts based on the systems being installed and their impact on and integration into existing system infrastructure and fleets. While voting and nonvoting membership may vary from agency to agency, the working group should recommend dispositions for each safety element through a voting process. To facilitate communication across all parties, this group should include all relevant project and agency managers, staff, contractors, and other partners with expertise in systems engineering, facilities engineering, maintenance engineering, construction management, operations, systems integration, and system safety and security. Transit agencies often designate the CSO as this group's chair.

  NOTE: Voting members may include the chief safety officer, certification manager, lead project designer, lead construction manager, project manager, system integration manager, O&M manager, QA manager, and security/police/cybersecurity representative. Nonvoting members may include the contract oversight representative, configuration manager(s), SSOA representative and other personnel as required for the business of the committee.

- **Other project-specific groups:** Transit agencies may form other groups to provide information and guidance. Other groups may include a Fire/Life Safety and Security Committee, Rail Activation/Operational Readiness Committee, and System Integration Testing Team.

2.1.5 Address budget and contractual requirements

Transit agencies should account for SSC activities within project budgets and schedules. Transit agencies should also ensure that requests for proposal, applicable interagency memoranda of understanding and other contractual documents clearly articulate the agency's safety and security certification requirements, as well as roles and responsibilities for internal stakeholders and external entities and contractors.

2.1.6 Engage with stakeholders

Transit agencies should collaborate and communicate with internal and external stakeholders to facilitate safety and security certification related activities and implement comprehensive and effective certification approaches.

2.2 Project-specific safety and security certification process

The FTA *Handbook for Transit Safety and Security Certification* describes the 10-step process for conducting safety and security certification, which this document applies. Transit agencies may tailor their project's safety and security certification process based on agency, jurisdiction and project requirements. The FTA handbook and this recommended practice describe the following 10-step process:

1. Identify certifiable elements.
2. Develop safety and security design criteria.
3. Develop and complete design criteria conformance checklist.
4. Perform construction specification conformance.
5. Identify additional safety and security test requirements.
6. Perform testing and validation in support of the SSC program.
7. Manage integrated tests for the SSC program.
8. Manage "open items" in the SSC program.
9. Verify operational readiness.
10. Conduct final determination of project readiness and issue safety and security certification.

Transit agencies should develop a project-specific SSCP to guide all processes associated with a project's safety and security certification. The project-specific SSCP should define all related roles and responsibilities and align with the agency's overarching SSCP. Typically, agencies make project teams responsible for developing the SSCP and the SSCRC (or similar leadership committee) responsible for reviewing and approving the SSCP.

To confirm that safety and security certification is incorporated into a project's schedule, transit agencies may use hold points and stage gates to prevent projects from getting ahead of the certification process. Agencies can apply a hold point or stage gate process to confirm that projects complete verification, and submit and approve proper documentation and evidence prior to beginning the next stage. This approach allows transit agencies to review and mitigate safety hazards and security vulnerabilities prior to an activity and offers opportunities to address prerequisites, such as design or construction documentation, prior to moving forward.

Transit agencies should document hold point and stage gate definitions, requirements and procedures that govern all project parties so that one group cannot move faster than others. All relevant parties should sign the hold point or stage gate document to indicate agreement, and the project team should add the document to the project's SSCP.

2.2.1 Identify certifiable elements

The project team should prepare and maintain a Safety and Security Certifiable Elements and Sub-Element List (CEL) that includes a project's systems and subsystems. Transit agencies should update the CEL as the project adds new systems or subsystems.

The Safety and Security Certification Working Group should have review responsibility for the Certifiable Elements and Sub-Elements List, while the Safety and Security Certification Review Committee should have approval authority.

A list of common rail certifiable elements, as well as sample checklists and forms used in other SSC steps, can be found in the *Handbook for Transit Safety and Security Certification*. Sample bus certifiable elements are listed in Appendix B.

2.2.2 Develop safety and security design criteria

Agencies should examine and implement their plans for reviewing and assessing safety and security risk. As part of developing design criteria, transit agencies should complete a hazard analysis and threat and vulnerability assessment to define safety and security requirements for the project. Transit agencies should conduct risk analysis workshops to create a list of hazards, threats and vulnerabilities based on reviewing the design package and coordinating with subject matter experts. For more information on conducting security risk assessments, see APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit."

Project design criteria and requirements should align with the system's overall safety and security requirements and incorporate the following:

- safety and security hazard/risk analysis and mitigation measures
- physical and cybersecurity threat and vulnerability assessment mitigation measures
- design criteria
- technical specifications
- safety and security codes
- industry standards
- transit agency operating history, incident data and lessons learned

New safety and security requirements may develop as the agency conducts additional analyses and the project design matures. Additional analyses may include a subsystem hazard analysis, system hazard analysis, fault tree analysis, failure modes and effects analysis (FMEA), human factors safety analysis, software safety analysis, sneak circuit analysis, and OHA. Transit agencies should continually update safety and security requirements based on new information and changes to operating equipment and the environment. Safety and security requirements should inform checklist development.

Agencies should then convene internal stakeholders (e.g., engineering, operations and maintenance) and other impacted parties (e.g., local transportation departments, first responders) to conduct initial and subsequent reviews as changes warrant. Transit agencies should review design submittals for elements included in the Certifiable Elements and Sub-Elements List and identify, discuss, resolve and document design-related issues, hazards, threats and vulnerabilities.

2.2.3 Develop and complete design criteria conformance checklist

Transit agencies should then create a Certifiable Items List (CIL) that identifies mitigation items and/or requirements for each safety and security certifiable element listed in the CEL. The CIL should include safety and security design criteria, mitigations resulting from hazard analyses, threat assessments, codes and requirements, plans and procedures, and any other items that will inform the safety and security certification process. Transit agencies should revise the CIL as new safety and security mitigations or requirements arise. Transit agencies should assign the review and approval of the project's CEL and CIL based upon responsibilities outlined in the agency Safety and Security Certification Plan.

Next, the project team should develop Safety and Security Certification Checklists that confirm design requirements. The purpose of the checklists is to organize information to confirm the delivery of actions and documentation that meet and verify the project's safety and security requirements.

To confirm proper management and verification of requirements, the project team should create checklists well in advance of the activities that are to be verified. Transit agencies should use agency-approved, project-specific documentation that clearly satisfies the identified requirement as verification evidence.

If a variance is needed, transit agencies should follow agency and project processes to configure changes. Configuration change processes should include an evaluation based on safety risk management. If a transit agency approves the variance for the requirement, the project team should provide documentation of the approved variance and the evidence that satisfies the requirement.

Transit agencies should assign the review and approval of the project's Safety and Security Certification Checklists based upon responsibilities outlined in the agency Safety and Security Certification Plan.

The Safety and Security Certification Working Group should review the completed checklists and recommend their approval. The SSCRC should approve the completed checklists.

2.2.4 Perform construction specification conformance

Performing construction specification conformance ensures that that each certifiable element of a project is constructed, installed and tested in conformance with the project safety and security design requirements and contract technical specifications. The project team should develop a construction specification conformance checklist before moving from the design phase to the construction phase of an element. The project team should collaborate with the project engineering and construction staff to develop a conformance checklist.

The conformance checklist should also track safety and security critical tests performed by the agency or construction contractor. Typical contractor tests may include manufacturing, performance and acceptance

tests, which can be used as evidence for certification. During construction, the need for tests in addition to those specified in contracts may arise. In these cases, the SSCRC should consult with the project's construction staff to perform and document additional necessary tests.

Once the project moves into its construction phase, the project team should provide the conformance checklist to the project engineering staff who are responsible for oversight of the construction phase, who in turn may request that the construction contractor verify the incorporation of the project's safety and security related requirements into the finished project.

Verification documentation may include field inspection reports, mill certifications, photos, visual inspection reports, test reports, independent laboratory tests and witnessing tests. Visual inspections may be used to verify a safety or security requirement that cannot be verified with other documentation. Verification documentation, including any comments, should be referenced on the conformance checklist and becomes part of the certification documentation.

During the verification process, the SSCM and SSCRC should monitor progress on conformance checklists to confirm that certification activities align with the project schedule. Any open items lacking documentation or experiencing problems achieving certification should be forwarded to the SSCRC for guidance or resolution.

Once the checklist is complete, the SSCM should audit the documentation to confirm support of identified requirements. The SSCM should then submit the audited checklist to the SSCRC with a recommendation for approval or disapproval. If the checklist was satisfactorily completed, a Certificate of Conformance should be issued for the element. If the committee finds the evidence to be insufficient to consider issuance of a Certificate of Conformance, it should take corrective action.

2.2.5 Identify additional safety and security test requirements

The project team should be responsible for developing, reviewing and implementing plans and procedures for all required safety and security related tests. The project team should also monitor and verify that responsible parties implement tests in accordance with safety and security requirements. Transit agencies should assign the review and approval of the project's test plans and procedures based upon responsibilities outlined in the agency Safety and Security Certification Plan.

The SSCM should review checklists against the project test plan to identify any additional tests needed to satisfy the safety and security requirements. The SSCM should then work with the project team to develop procedures and test criteria to be included in the test plan. The safety and security team should identify additional test requirements as early as possible to ensure completion of all needed testing.

2.2.6 Perform testing and validation in support of the SSC program

The project team should be responsible for developing and implementing test plans and procedures for all safety-related tests required in their respective technical provisions. The project team should review and approve the safety-related test plans and procedures submitted by the contractor. The project team should monitor and verify their implementation in accordance with contract requirements.

The project team should have primary responsibility for properly documenting, reporting and submitting test results. The project team should review submitted test reports and verify conformance with safety and security requirements to ensure that the system is validated for its purpose.

After conducting a thorough review, the project team should approve submitted test reports. For safety and security purposes, agencies should use test results as evidence for items on conformance checklists.

2.2.7 Manage integrated tests for the SSC program

Transit agencies should use integrated tests to verify the safe and secure performance of two or more disparate systems in a project. Examples include rail vehicles with tracks that they operate on and traction power systems that power them, and security camera systems with supervisory control and data acquisition (SCADA) and intrusion detection systems.

Contract specifications may not necessarily require integrated tests, but transit agencies should require integrated tests as part of an overall project to ensure that the various systems work together as intended and function safely. Transit agencies should define testing requirements and general processes in an Integrated Test Plan or System Integration Test Plan (SITP).

Prior to beginning any testing, transit agencies should develop a Conformance Checklist for integrated tests. The committee responsible for safety and security certification oversight should review and approve the checklist.

Before conducting an integrated test, transit agencies should confirm a minimum level of safety and/or security conformance to ensure that the systems can be integrated safely. The minimum level required is dependent upon the nature and scope of the test. The engineer responsible for the test should inform the SSCM of the intent to conduct an integration test and confirm that each system element involved in the test is safety/security certified or has met a minimum level of safety and is ready for integrated testing.

If safety and security certification of the elements required for the test is not complete, the person or group managing the certification effort should issue a permit or document to temporarily use the uncertified systems. This temporary use process should indicate that the certifiable element meets a required minimum level of safety and security and may be used for integrated testing purposes. The temporary use process should also include any restrictions or operating limitations. An example system that should require a temporary use document is the testing of rail vehicles integrated with track systems, signal systems, or other disparate systems with a safety impact. Temporary use documents are superseded upon issuance of final certificate of conformance for the elements.

After completing the aforementioned preconditions, transit agencies can begin conducting integrated testing. The SSC team should consider having a member witness integrated testing.

2.2.8 Manage “open items” in the SSC program

During certification activities, project teams should note instances of nonconformance with a safety or security requirement, capturing items that cannot be completed on the Open Items List (OIL).

Transit agencies should assign the management and coordination of the project’s OIL based upon responsibilities outlined in the agency Safety and Security Certification Plan. The responsible party must review each OIL item for its impact on safety and security, and each item must be either satisfied or managed to reduce risk to an acceptable level before conducting tests and/or commencing revenue operations. The project team should present the OIL to the SSCRC for review on an ongoing basis to confirm that the transit agency addresses all items prior to revenue service.

Refer to the FTA handbook for a sample format for documenting open items.

2.2.9 Verify operational readiness

During the initial stage of construction verification, transit agencies should begin to review hazard analyses and TVAs to determine if there are any hazards or threats that may impact operations. The SSCM should

identify these items, organizing them into a separate list to serve as the initial draft of the OHA. Transit agencies should decompose the list into subcategories or elements (e.g., signals, traction electrification systems, yard/shop) and have them reviewed by subject matter experts.

Agency operations and maintenance teams should be responsible for updating or developing operations and maintenance procedures, rulebooks, standard and emergency operating procedures, and training plans and programs related to the new systems or programs. Transit agencies should conduct exercises with internal and external stakeholders during pre-revenue operations to verify preparation. Depending on the procedure, plan or program, the project team should review the submittal for conformance with the safety and security requirements.

Transit agencies should also review and update related safety and security plans and processes.

2.2.10 Conduct final determination of project readiness and issue safety and security certification

Transit agencies should issue a project's system safety and security certificate using the following four-step process that results in the final SSCVR.

The SSCVR process includes:

1. The project team certifies that design conforms with the design criteria and CIL.
2. The project team certifies completion of the work in accordance with safety and security requirements and verifies documentation.
3. The project team works with appropriate departments to verify that existing and new plans and procedures support safe operations and maintenance activities as they relate to the project.
4. A safety and security certification committee or working group, as outlined in the agency SSCP, verifies that the project conforms to the safety and security certification process based on design and construction documentation, new operations and maintenance procedures, and integrated testing and training records.

In the event of open items, transit agencies may issue an interim safety and security certificate for the project to begin revenue service, documenting any restrictions or limitations to service. Transit agencies should consider reevaluating an interim certificate after a predetermined time frame identified by the SSCRC until transitioning to the final SSCVR.

Upon successful resolution of all open items and completion of the SSCVR process, the accountable executive and/or the chief safety officer should issue safety and security certification.

2.3 Activities following project safety and security certification

Following the issuance of the project's safety and security certification, transit agencies should address several follow-on safety and security assurance activities, as the project's outcomes may establish new or revised safety and security baselines. Transit agencies should apply these outcomes to update agency project design criteria and specifications, safety and security audits and reviews, risk registers, configuration management, and safety and security certification processes.

2.3.1 Update design criteria and specifications

Transit agencies should incorporate project engineering design criteria, specifications, as-built drawings, and manuals to establish or update design criteria and specifications for inspection, maintenance and future agency projects.

2.3.2 Update safety and security audits and reviews

Transit agencies should update internal safety and security related audits and reviews based on items and mitigations identified during the project's certification process, and any new assets, systems or subsystems introduced to the agency by the project. Revised audits and reviews should identify safety risks and assess the effectiveness of mitigation measures.

2.3.3 Update risk register

Transit agencies should update the agency's risk register to include any new safety hazards or security threats or vulnerabilities that the project introduced.

2.3.4 Update systems configuration

Configuration management includes transit agency activities to properly identify, document and communicate changes to physical, functional and operational characteristics of structures, systems, components (including software) and facilities.

An outcome of safety and security certification may be design changes affecting the physical and operating characteristics of a transit agency's systems, structures and facilities. Transit agencies should develop a Configuration Management Plan that includes a listing of systems subject to the configuration management process and documents changes based on the magnitude of their impact. Transit agencies should then update the plan to include any new and modified systems designed and constructed for a project. Transit agencies should implement configuration management and formal document control procedures for operating and maintenance documents and training affected by the design change. Affected documents typically include standard operating procedures, emergency operating procedures, safety and operating rules, training materials, drawings, and engineering reference information.

Transit agencies should maintain records of configuration management activities to demonstrate how organizations and individuals made decisions and satisfactorily performed and completed activities. Transit agencies should maintain records in accordance with individual state records retention requirements and agency policy. Checklists and other recording mechanisms may be used by the agency.

2.3.5 Update the agency's safety and security certification process

Transit agencies should coordinate with project stakeholders to conduct a debrief of the project's safety and security certification process. Transit agencies should update the agency's SSCP and processes based on validated observations and lessons learned.

2.4 Modified safety and security certification activities

Agencies may choose to modify some activities based on project circumstances and requirements. Transit agencies should describe these modified safety and security approaches in the agency SSCP, detailing roles and responsibilities for reviewing and approving the modified approaches.

Similarly, while this document uses the term "safety and security certification" to generally mean a documented process for demonstrating that the safety and security of a project has met a standard, transit agencies may use the term "safety and/or security verification" for projects that do not apply the entire safety and security certification process. The safety and security verification process should be commensurate with the complexity of the involved project, and the agency SSCP should define acceptable minimum actions or steps. This flexibility allows transit agencies to determine appropriate processes for each project while verifying and documenting the incorporation of safety and security requirements.

Modified verification approaches may include the following:

- **Technical review:** Some items may need only an expert review of a project or an assessment of a trial period. Should a transit agency discover the need for additional mitigations, the responsible group should review whether the project requires safety and security certification.
- **Safety or security acceptance/walk-through:** Agencies may request a safety or security review for verification purposes even if projects have acceptable safety hazards or security vulnerabilities. There may also be projects where an agency completes design and construction without conducting a hazard analysis or developing a conformance checklist in advance.

Examples where transit agencies may elect to adopt a modified approach include but are not limited to the following:

- **Emergency work:** During certain events, it may not be possible to complete normal risk analyses, design criteria or construction checklists. Emergency work may be unexpected, time-sensitive work to correct an unacceptable safety risk, such as the need for a retaining wall from a landslip.

  NOTE: "Unacceptable safety risk" is based on the transit agency's own standards as defined in its agency Safety Plan and supporting procedures.

- **Use of an off-the-shelf product:** Most off-the-shelf items have already been designed and tested, making design criteria or an associated conformance checklist impracticable. Therefore, a product certificate may be accepted by a committee or certification manager in lieu of a design or a construction certification checklist. The certification checklist should focus on the integration of these items into the system.
- **Projects started before it is decided the safety and security certification process is applicable:** Although undesirable, an agency may decide to apply a safety and security certification process to a project that has already been started and made significant progress. In this case, a committee or certification manager may decide to start the certification process with the current project phase rather than backtrack to the design process. A certification in this manner could also be used when the SSOA, FTA/project management oversight consultant (PMOC), or other oversight agency directs that a system change needs safety and security certification after a project has started.

Should the accountable executive, chief safety officer or chief security officer determine that an agency needs to complete a project-specific safety or security verification for one of the aforementioned reasons, some or all of the following events should still occur:

- Review project documents for safety and security content.
- Identify safety and security elements and a CEL/CIL that a committee or certification manager can approve.
- Assess hazards and vulnerabilities with the creation of a hazard analysis and/or threat and vulnerability matrix.
- Create checklists for specific phases of the project and seek approval from a certification committee or manager.
- Manage integrated testing and validation, "open items" and risk register.
- Verify operational readiness through drills, updating procedures and training.
- Create certificate(s) of compliance and/or a Final Certification Verification Report for the item or project.

2.5 Certification for modifications and rehabilitation

Over the course of their life cycles, systems are likely to require modification or rehabilitation due to age, the need for conformance with new safety or security requirements, or the need for compatibility with other transit system elements. For rehabilitations of entire fleets or groups of vehicles, transit agencies should focus on implementing a repeatable certification process, as opposed to considering each car as its own unit.

The need for certification of modified equipment should be based on the safety and security criticality of the modification, as identified through a safety analysis. If the modified or rehabilitated systems include modification or rehabilitation to safety- or security-critical subsystems or components, the equipment should be decertified (if originally certified through a safety and security certification process) or removed from service with a safety hold/impound until such time as the modification/rehabilitation has been completed.

Recertification of the system is typically limited to the rehabilitated/modified subsystem, rather than the entire system. For example, an upgrade of the propulsion system on a rail vehicle likely would require certification of the new propulsion system design, construction, installation and testing, which includes testing compatibility with other vehicles that may be coupled to it. In addition to verifying that the modified or rehabilitated subsystem complies with the safety-related design criteria, technical specification and test requirements, the certification process also should include assurance that drawings, manuals and other safety-critical operating and maintenance documentation, procedures and training have been revised to reflect the upgrade. Conversely, modification to rail vehicle passenger seating material may be limited to flammability and smoke emission test results to confirm conformance with smoke, flammability and configuration management requirements. Accordingly, the verification steps involved for a particular project are dependent on the type of project and its potential safety and security impacts. Transit agencies should determine the level of review or certification required based on the modification’s safety and security impact.

Upon completion of the work, a document, such as a Certificate of Conformance–Rehabilitation/Modification Project, should be prepared and signed by all affected departments, as identified in the agency’s SSCP. For decertified equipment, the new certificate serves as authorization to place the equipment back into service.

3. Capital infrastructure project delivery methods

Transit agencies should closely align their SSC approach with all project delivery methods. **Table 1** outlines typical project delivery methods with method- and step-specific nuances for SSC, using design–bid–build as the baseline. Refer to FTA PMOC guidelines and Appendix D for more material on delivery methods.

TABLE 1
Typical Project Delivery Methods for SCC

General					
Design–Bid–Build (DBB)	**Design–Build (DB)**	**Design–Build–Operate–Maintain (DBOM)**	**Turnkey**	**Public–Private Partnerships (P3/PPP)**	**Construction Manager at Risk (CMAR/CM@R)**
►A traditional method of transit project delivery ►Linear process where one task follows completion of another with no overlap ►The transit agency provides Certificates of Conformance (CoC) at the end of Design and Construction phases ►Transit agencies clearly delineate agency and contractor SSC activities, including phasing, timing, etc.	►A traditional method of transit project delivery ►Maintains consistency throughout the project as it allows a transit agency to contract with one entity for design and construction services	►A traditional method of transit project delivery ►Same as DB project delivery, except that contractors also deliver operations and maintenance as part of the contract	►Turnkey provider develops the transit agency's initial concept and plan, and designs and constructs the system ►The transit agency accepts the project after construction concludes ►The transit agency turns over the project to another entity to deliver operations and maintenance ►The transit agency coordinates SSC activities between the turnkey developer and subcontractors	►May not hit FTA dollar threshold that requires SSC process ►Concessionaire is typically responsible for all SSC activities, with the transit agency ensuring compliance with its SSC process, unless the SSOA or P3 agreement specifies otherwise ►The agency should clearly define SSC responsibilities in the P3 agreement; any overlooked activities will become its responsibility ►The transit agency and concessionaire maintain close coordination throughout project delivery	►Can be applied to any other delivery method where construction services are contracted ►CMAR contractor provides design comments during the design phase ►CMAR contractor delivers SSC activities only during the construction phase ►The agency should clearly define SSC responsibilities in the contract; any overlooked activities will become its responsibility or necessitate a contract modification
Step 1: Identify certifiable elements					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency should determine if the agency or contractor will develop the CEL ►CEs are based on PHA, TVA and design criteria ►The build contractor should provide input into CEs, or may need to update the CEL during the construction phase	►Same as DBB	►Same as DBB	►The turnkey operator is responsible for all CE development activities, with transit agency observing or participating	►The concessionaire typically identifies CE and prepares CEL	►Transit agencies typically identify CE and CEL prior to engaging the CMAR contractor ►The CMAR contractor may need to update the CEL during the construction phase

TABLE 1

Typical Project Delivery Methods for SCC

Step 2: Develop safety and security design criteria					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency ensures the development of safety and security design criteria based on agency documents and the results from the PHA and TVA ►The transit agency will decide if the transit agency or the design contractor will create design criteria	►Same as DBB	►Same as DBB	►The transit agency provides design criteria ►The turnkey operator provides input into design criteria	►The transit agency typically provides initial safety and security design criteria before engaging P3 partners ►P3 partners revise the design criteria base on P3 partner needs and requirements	►The transit agency prepares design criteria prior to engaging the CMAR contractor ►CMAR constructability comments may cause the designer to update the design criteria
Step 3: Develop and complete design criteria conformance checklist					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The DBB design team develops and completes the Design Criteria Conformance Checklist (DCCC) ►The transit agency approves the completed DCCC prior to starting construction and material procurement ►The transit agency should consider including the DCCC in construction bid documents ►The transit agency and designer sign the design CoC and the transit agency issues the design CoC	►The DB design team develops and completes the DCCC ►Design can extend through the end of construction ►The transit agency often issues the CoC at the end of the project ►The DB contractor conducts design change reviews throughout the project ►The transit agency approves the completed DCCC	►Same as DB	►The turnkey operator is responsible for developing the DCCC, with the transit agency observing or participating	►The concessionaire develops and completes the DCCC ►The transit agency approves the completed DCCC	►The transit agency typically prepares the DCCC prior to engaging the CMAR ►The CMAR is not part of the design team and does not complete the DCCC

TABLE 1

Typical Project Delivery Methods for SCC

Step 4: Perform construction specification conformance					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency or DBB contractor completes the Construction Specification Conformance Checklist (CSCC) ►The transit agency or DBB contractor may also verify the DCCC for the construction phase ►The transit agency approves completed checklists ►The transit agency issues the CoC, which is signed by both the transit agency and DBB contractor	►The DB contractor usually develops and completes the CSCC ►The transit agency approves completed checklists	►Same as DB	►The turnkey operator is responsible for developing the CSCC, with the transit agency observing or participating	►The concessionaire usually develops and completes the CSCC ►The transit agency approves completed checklists	►Same as DBB
Step 5: Identify additional safety and security test requirements					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency and DBB contractor jointly review specifications and identify additional safety and security test requirements ►Subject matter experts review tests, which the transit agency accepts ►Additional tests may necessitate a contract modification	►Same as DBB	►Same as DBB	►The turnkey operator coordinates with other subcontractors to perform SSC activities, with the transit agency observing or participating	►Same as DBB	►This activity is typically not within the CMAR contractor's scope of service ►The transit agency needs to identify safety and security test requirements

TABLE 1

Typical Project Delivery Methods for SCC

Step 6: Perform testing and validation in support of the SSC program					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The engineer of record (EOR) reviews and accepts test results ►The project team captures testing per the SSCP ►The project team defines testing and validation in the test plan ►The transit agency reviews and approves test and validation results	►The DB contractor applies project resources earlier to complete testing program	►Same as DB	►Same as DB	►The concessionaire performs tests, coordinating closely with the project team	►The CMAR contractor performs the same test and validation activities as any other delivery method when construction services are contracted
Step 7: Manage integrated tests for the SSC program					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency decides if it will manage integrated testing, contract with a systems integrator separate from DBB, or contract with the DBB contractor ►The transit agency or contractor identifies integrated tests, coordinating with the SSC team	►Same as DBB	►Same as DBB	►The turnkey operator coordinates with other subcontractors to manage integrated testing, with the transit agency observing or approving	►The systems integrator role is typically included in the concessionaire's team	►May not be within the CMAR contractor's scope of service ►The transit agency needs to determine if it wants the CMAR contractor to manage integrated testing and, if so, include the activity in the contract
Step 8: Manage "open items" in the SSC program					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency verifies operational readiness with the support of the DBB contractor ►The transit agency typically develops and completes operational conformance checklists	►Same as DBB	►The DBOM contractor verifies operational readiness ►The transit agency reviews and approves operational readiness	►Same as DBOM	►The concessionaire typically verifies operational readiness, coordinating closely with the project team	►Same as DBB

TABLE 1
Typical Project Delivery Methods for SCC

Step 9: Verify operational readiness					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The transit agency verifies operational readiness with the support of the DBB contractor ►The transit agency typically develops and completes operational conformance checklists	►Same as DBB	►The DBOM contractor verifies operational readiness ►The transit agency reviews and approves operational readiness	►Same as DBOM	►The concessionaire typically verifies operational readiness, coordinating closely with the project team	►Same as DBB
Step 10: Conduct final determination of project readiness and issue safety and security certification					
DBB	**DB**	**DBOM**	**Turnkey**	**P3**	**CMAR**
►The agency conducts final determination, typically based on the SSCVR ►The agency decides if it or the DBB contractor prepares the SSCVR and certificate ►The transit agency is responsible for resolving open items and complying with restrictions listed in SSC certificate ►The SSCVR should include both design and construction verification ►The transit agency issues the certificate	►Same as DBB	►Same as DBB	►The turnkey operator completes the SSCVR ►The transit agency approves the SSCVR and issues safety and security certification	►The P3 partnership agreement should assign the concessionaire responsibility for preparing the SSCVR ►The transit agency approves the SSCVR and issues safety and security certification	►Same as DBB

4. Rail passenger vehicles and on-track equipment

Rail vehicles and on-track equipment are elements of all rail transit systems that have safety-critical subsystems and the potential to cause significant harm or damage if the subsystems and components do not meet safety and security objectives and requirements. For this reason, agencies that provide rail transit passenger services should adopt a formal top-down approach to managing safety and security risk. Transit agencies should use the safety and security certification process (as described in Section 2.2) for rail projects, to include rail passenger vehicles and on-track equipment.

The following sections describe two rail-specific applications of safety and security certification.

4.1 Rail passenger vehicles

For rail passenger vehicles, the development and completion of the safety and security design conformance checklist applies to the entire fleet, not individual units, because there is one design or specification for the rail passenger vehicle fleet. For example, fire and smoke safety requirements or crashworthiness are applicable to all rail passenger vehicles and would not differ from rail vehicle to rail vehicle within the same fleet. The development and completion of construction and installation checklists applies to the entire fleet, but each individual rail passenger vehicle will require individual construction and installation checklists. For example, if building 10 rail passenger vehicles, transit agencies should verify the rail vehicle design in its entirety and verify each of the 10 rail vehicles for conformance against the construction and installation checklists individually.

The individual rail passenger vehicle checklist should include safety and security requirements that the transit agency must ensure on an individual basis. Vehicle acceleration (propulsion) and deceleration (braking) requirements are examples that transit agencies should verify to ensure that excessive acceleration or deceleration does not cause injury. Similarly, transit agencies should validate compatibility when coupled to other comparable rail vehicles (married pairs, for example) by each individual rail vehicle and certified as a married or coupled pair. Accordingly, CELs for rail passenger vehicles should be logically broken into sub-elements by individual rail passenger vehicles requiring certification. Rail car systems and subsystems that might have hazards or vulnerabilities to consider include energy sources, electrical systems, fueling systems, mechanical systems, pneumatic and hydraulic systems, temperature control systems, fire and life safety systems, ergonomics, passenger interface systems, geolocating systems, positive train control, and on-board signal systems.

Transit agencies should develop and complete functionality validation and verification test conformance checklists based upon the rail vehicle sub-element and develop and complete integrated test conformance checklists representing the entire fleet.

See Section 2.5 for modifications and rehabilitation for more information on certifying rail car modifications and rehabilitation.

4.2 On-track equipment

On-track equipment includes specialty vehicles designed to assist in a wide range of rail transit maintenance activities. On-track equipment may be equipped only with steel wheels for travel on rails of the transit network or be dual-equipped, with rubber tires to operate on city streets and highways and steel wheels to operate on rails. Transit agencies may need to certify on-track equipment if a risk analysis identifies mitigation measures and applicable codes and industry standards that should be verified. Typical safety examples include verification of equipment controls, interlocks to prevent accidental activation, insulation characteristics when working on energized traction power systems, vehicle shunting or other safety-critical requirements.

For dual-mode on-track equipment, transit agencies may not need to certify the vehicle itself, as the vehicle must meet Federal Motor Vehicle Safety Standards. However, transit agencies should certify specialty equipment mounted on the vehicle, any alterations or modifications to the existing vehicle, and the vehicle's function as identified by a safety analysis, applicable codes and industry standards.

5. Bus projects

Transit agencies should consider using the safety and security certification process (as described in Section 2.2) for bus projects, to include buses, bus rapid transit (BRT), and facilities. Simply, safety and

security certification provides proactive tools and analyses that identify potential safety problems before they result in collisions and incidents.

The following sections describe three bus-specific applications of safety and security certification.

5.1 Buses

Bus systems can apply the safety and security certification processes to develop unbiased evaluations and understand cost impacts during a bus's life cycle, performance, and the integration of safety and security certification milestone scheduling with the overall project scheduling. Furthermore, the safety and security certification process promotes a clear understanding of public safety consequences when risks are not evaluated and mitigated properly.

5.2 Bus facilities

Bus facilities have many of the same systems as rail facilities. Similar systems include fire and life safety systems, maintenance equipment, work pits, battery rooms, crew rooms, and offices. Additionally, electric buses are now becoming more popular, and this has introduced high-voltage charging systems at these facilities. Thus, transit agencies should apply safety and security certification for bus facilities as needed to ensure safe and secure operations.

5.3 Bus rapid transit

The FTA defines BRT as "a high-capacity bus-based transit system that delivers fast and efficient service that may include dedicated lanes, busways, traffic signal priority, off-board fare collection, elevated platforms and enhanced stations." While BRT systems are increasingly becoming more popular throughout the United States, there are no formal, required mechanisms for safety and security certification. Many transit agencies (and SSOAs, where applicable) are choosing to require safety and security certification since BRT uses a fixed guideway, while in some instances, an FTA grant may contain safety and security certification requirements.

Transit agencies operating BRT should implement the safety and security certification process to ensure that completed BRT projects are safe and secure for passengers, transit employees, public safety personnel and the general public when turned over for revenue operation. Transit agencies should detail application of safety and security certification processes for BRT systems in the agency SSCP. Similarly, transit agencies should develop a project-specific SSCP to guide the project through all required certification steps.

6. Other non-major capital projects

Transit agencies will likely implement many projects, upgrades and rehabilitations that will not meet FTA thresholds for major capital projects but will still incorporate safety-critical items or have safety-critical functions that transit agencies should review prior to placing into service. Non-major capital projects that may require safety and security certification may include but are not limited to "in-fill" stations, station rehabilitations, SCADA upgrades, elevator or escalator installation or rehabilitations, signaling updates, and grade crossing improvements.

Transit agencies should include their safety and security certification approach for non-major capital projects in their agency SSCP to help manage safety and security risk. Agencies may determine the need to implement the full safety and security certification process for non-major capital projects or decide that a more limited or modified certification process for smaller projects suffices. Section 2.4 outlines modified approaches for safety and security certification.

7. State safety oversight

Each SSOA has a guiding document outlining its authority, staffing, responsibilities and interface with the overseen transit agencies—often referred to as a System Safety Program Standard or Program Standards Manual (hereafter "Program Standard"). Most Program Standards contain chapters or sections dedicated to system modification, major capital projects and SSC.

States tailor their oversight programs to state needs. While all SSOAs are required per 49 CFR §674 to perform safety oversight, some states opt to also perform security oversight of the covered transportation systems. SSOAs typically do not prescribe mean or method; rather they verify that the transit agency is compliant with federal, state and local requirements and is following its own safety-related standards and procedures.

7.1 Communicating SSC expectations with SSOA

It is important for the transit agency and SSOA to confer ahead of each project that may be subject to certification. Early, frequent communication to establish an understanding of what the parties can expect from one another is recommended. The SSOA should communicate its expectations of the transit agency for a given project and its general plan for oversight activity.

The project meeting schedule should be made available so SSOA personnel may participate as deemed fit. An SSOA will typically participate in or observe the following types of meetings: FTA Project Management Oversight, Safety and Security Certification Review Committee, Safety and Security Certification Working Group, Configuration Management/Change Committee, Fire/Life Safety Committee, System Integration Testing Team, Operational Readiness/Rail Activation Committee, and any ad hoc or special committees.

7.2 Typical SSOA responsibilities related to SSC

Table 2 outlines typical SSOA responsibilities related to SSC activities.

TABLE 2
Typical SSOA Responsibilities Related to SSC

Document or Activity	Responsibilities
Agency Safety Plan (ASP)	An SSOA should ensure that SSC activities are included in the ASP.
SSCP (agency- and/or project-specific)	An SSOA may require a transit agency to establish an SSCP, revise an existing SSCP, or provide advisory comments on the document and revisions.
Management of change/ system modification procedure	An SSOA may require transit agencies to establish change management procedures, revise an existing procedure, and/or incorporate advisory comments.
Design Criteria Manual (DCM)/ Basis of Design (BOD)	An SSOA may request and review the agency- or project-specific DCM/BOD at the beginning of the project. The SSOA may use the DCM/BOD as a reference document when reviewing SSC-related documents as the project progresses.
Inspections/observations	An SSOA may choose to inspect capital project work sites, meet with personnel or review project records. As part of its safety oversight function, inspections generally include project safety risks. As part of its safety certification oversight, the SSOA may inspect for adherence to transit agency and project procedures.
SSCVR	An SSOA may review the SSCVR to confirm that the transit agency completed the certification process and adequately documented any open items restrictions and/or exceptions and corrective action plans. The SSOA may find it beneficial to request SSCVRs in an iterative fashion when the SSOA components are ready.
Meeting participation	An SSOA should participate in project meetings to provide SSC input and oversight.

7.3 SSOA document review

An SSOA may request to review, and may provide comment on, numerous documents pertaining to certification. SSOAs may provide guidance on how the project team could better document an activity or better mitigate safety risk. In circumstances of noncompliance with a federal, state or local requirement, or an unacceptable safety risk, an SSOA may require the project team to take action.

The project team and the SSOA should confer about document review protocol. Given the volume of material it is generally helpful to either grant SSOA personnel access to the project's electronic document management system(s) or to establish a cloud-based file sharing protocol. Both parties should understand one another's expectations when it comes to document revisions and rounds of comments and responses.

7.4 SSOA concurrence with final safety and security certification

Many SSOAs issue a concurrence letter documenting review of and concurrence with the final SSCVR. Some require the transit agency to obtain such concurrence prior to entering the new system or asset into service. The SSCVR letter serves as the SSOA's documentation that it has completed a review of the certification process and that no unacceptable safety risks persist. The SSOA may issue conditions within this letter or commit to enhanced monitoring if there is a particular safety concern.

In the closing weeks and days ahead of initiation/reentry into service, the project team and SSOA should coordinate closely to ensure sufficient time for any SSOA-required review and concurrence issuance. The SSOA may share this letter with FTA personnel as part of a coordinated oversight effort.

8. FRA safety and security certification

Formal safety and security certification in the commuter and passenger rail environment has historically been performed only when required by an FTA major capital project funding agreement or FRA regulations for train control system development. However, FRA rule 49 CFR §270.103(s)(3) requires safety certification for commuter and passenger rail in several other instances, which include:

- initiation of new operations;
- extension, rehabilitation, or modification of existing systems; or
- replacement of vehicles and equipment.

The FRA's regulation does not prescribe how commuter and passenger rail entities should implement certification, but the preamble cites the FTA's *Handbook for Transit Safety and Security Certification* as an example of an adequate model to follow to achieve compliance. The overall safety and security certification framework is detailed in Chapter 2 of the handbook.

Since the operating and regulatory environments for commuter and passenger rail systems differ significantly from transit systems, commuter and passenger rail operators should tailor their safety and security certification plans to address each system's unique characteristics. Passenger and commuter rail-specific considerations to address in their safety and security certification plans may include the following:

- Roles and responsibilities for host/tenant railroad operating agreements and contractual agreements for rail operations and maintenance functions.
- A formal statement identifying senior management commitment from all stakeholders.
- Commitment of resources for the operating entity, host railroad, tenant railroad and/or contract operators, as applicable.
- Establishment of a collaborative approach to managing risk across host/tenant relationships, including change management.

- Development of PHA and TVA processes to identify certifiable elements and items that are the responsibility of others (e.g., host railroad).
- Processes for achieving agreement on the specification and verification of safety mitigation measures.

Related APTA standards

APTA-SS-CCS-RP-001-10, "Securing Control and Communications Systems in Transit Environments Part 1"
APTA-SS-CCS-RP-002-13, "Securing Control and Communications Systems in Rail Transit Environments Part 2"
APTA-SS-CCS-WP-003-15, "Securing Control and Communications Systems in Rail Transit Environments, Part IIIa"
APTA SS-CCS-RP-004-16, "Securing Control and Communications Systems in Rail Transit Environments Part IIIb"
APTA SS-CCS-WP-005-19, "Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure"
APTA SS-CCS-RP-006-22, "Operational Technology Cybersecurity Maturity Framework (OT-CMF)"
APTA SS-ECS-RP-001-14, "Cybersecurity Considerations for Public Transit"
APTA SS-ESC-RP-002-19, "Enterprise Cybersecurity Training and Awareness"
APTA SS-ECS-RP-003-19, "Enterprise Cybersecurity Involving the Board of Directors and the Executive Suite"
APTA SS-SIS-S-017-21, "Security Risk Assessment for Public Transit"

References

American Public Transportation Association, Standard Bus Procurement Guidelines, APTA Standards Development Program, 2013.

Black's Law Dictionary, 11th edition, West Group, 2019.

Code of Federal Regulations:
29 CFR §1910.119(b)
29 CFR §1910.2
49 CFR §633.5
49 CFR §655.4
49 CFR §672
49 CFR §673
49 CFR §674

Department of Defense, "System Safety," MIL-STD-882E, May 2012.

Federal Highway Administration, Moving Ahead for Progress in the 21st Century Act (MAP-21), July 2012.

Federal Transit Administration:
FTA-MA-90-5006-02-01, *Handbook for Transit Safety and Security Certification*
FTA Project and Construction Management Guideline March 2016
FTA Circular 5800.1
FTA Circular 5200
Safety Advisory SA-22-2

International Building Code, International Code Council, 2000.

International Existing Building Code, International Code Council, 2018

Rail Cybersecurity Mitigation Actions and Testing – SD 1580/82-2022-01

Cybersecurity Assessment Tool for Transit (CATT)

NIST Cybersecurity Framework

Definitions

alteration: 1. Any construction or renovation to an existing structure other than repair or addition [*International Building Code*]. 2. Any change to an existing piece of equipment or vehicle other than a repair, replacement-in-kind, rehabilitation or refurbishment intended to return the item to a state of good repair. 3. Modification of a process, procedure, piece of equipment, vehicle, building or structure (including track and automatic train control components).

certifiable elements: Project elements that can affect the safety of transportation agency passengers, employees, contractors, public safety personnel or the general public (e.g., stations).

Certifiable Elements List (CEL): A list of certifiable elements.

certifiable items: Individual items/components that make up the certifiable elements. Each item of a certifiable element must be verified before the element as a whole can be verified.

Certifiable Items List (CIL): A list of certifiable items.

Certifiable Sub-Elements: Sub-elements that can affect the safety of transportation agency passengers, employees, contractors, public safety personnel or the general public (e.g., platforms).

chief safety officer (CSO): An adequately trained individual who has responsibility for safety and reports directly to a transit agency's chief executive officer, general manager, president or equivalent officer.

commercial-off-the-shelf: Commercial items that require no unique modifications or maintenance over the life cycle of the product to meet the needs of the procuring organization.

cybersecurity: The process of prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and nonrepudiation.

design team: The team that is responsible for the design of the project or system elements. The designer of record is part of the design team.

element: A system or any item or collection of items that make up a system, such as a subsystem, assembly, sub-assembly, component or part.

facility: All or any portion of buildings, structures, site improvements, elements, and pedestrian or vehicular routes located on a site.

fixed guideway: Any public transportation facility that utilizes and occupies a separate ROW or rails. This includes but is not limited to heavy rail, light rail, commuter rail, automated guideway transit, people movers and exclusive facilities for buses (e.g., bus rapid transit).

Full Funding Grant Agreement: A means for providing Section 5309 funds to projects with a federal share of $25 million or more. FFGAs establish terms and conditions for the federal financial participation in a New Starts project.

hazard: Any real or potential condition that can cause injury, illness or death; damage to, or loss of, facilities, equipment, rolling stock, or infrastructure of a public transportation system; or damage to the environment.

hold point: A process used to ensure that proper documents have been submitted and accepted for a certain activity prior to the beginning of the next stage, usually in the testing or integration phase.

life cycle: The sequence of events a project proceeds through from conceptualization through design, implementation, startup, operation and maintenance, demobilization/decommissioning, and demolition—that is, "cradle to grave."

major capital project: A project that:

1. Involves the construction, expansion, rehabilitation or modernization of a fixed guideway that:
    a. has a total project cost of $300 million or more and receives federal funds of $100 million or more; and
    b. is not exclusively for the acquisition, maintenance or rehabilitation of vehicles or other rolling stock; or
2. The administrator determines to be a major capital project because project management oversight will benefit the federal government or the recipient, and the project is not exclusively for the acquisition, maintenance or rehabilitation of rolling stock or other vehicles. Typically, this means a project that:
    a. involves new technology;
    b. is of a unique nature for the recipient; or
    c. involves a recipient whose past record indicates the appropriateness of extending project management oversight.

mishap: An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

modernization: The use of proven new materials, components or subsystems to meet higher standards of productivity than are possible with the original equipment or materials.

New Starts Project: Any rail fixed guideway system funded under FTA's 49 U.S.C. §5309 discretionary construction program.

oversight: Supervision of an activity, operation or process by management, a regulatory organization or an independent body with supervisory authority.

passenger: A person who is on board, boarding, or alighting from a transportation vehicle for the purpose of travel.

patron: A person, other than a passenger or employee, who is utilizing transportation agency services or facilities.

probability: An expression of the likelihood of occurrence of a mishap.

procedure: A document that describes how to implement one or several activities of a business process. The document identifies the sequence of steps, and specifies for each step what needs to be done, when and by whom.

project manager: The person in overall charge of the planning and execution of a particular project.

rail transit agency: The organization that operates rail transit service and related activities. Also called *transit system*, *transportation agency*, *transit agency*, *operating agency*, *operating authority*, *transit authority* or other similar terms.

rail transit vehicle: The rail transit agency's rolling stock, including but not limited to passenger and maintenance vehicles.

refurbishment: The renovation, restoration, redecoration, revamping or overhaul of equipment and facilities to adequate standards of performance and a state of good repair, which if neglected could cause safety hazards or serious disruption of service.

rehabilitation: 1. Any work undertaken in an existing building. 2. The substitution of new materials, components or subsystems having basically the same fit and function as the worn or weakened original equipment.

right-of-way: The area through which a rail vehicle travels (the vehicle's dynamic train envelope).

risk: A combination of the severity of the mishap and the probability that the mishap will occur.

safety: Freedom from unintentional acts or circumstances.

safety and security certification (SSC): The series of processes that collectively verify the safety and security readiness of a project for public use.

safety-critical: 1. A term applied to a condition, event, operation, process or item whose severity consequence is either catastrophic or critical (e.g., safety-critical function, safety-critical path and safety-critical component). 2. A system or element that, without the deployment of safety barriers or controls, could fail such that critical or catastrophic consequences could be realized.

safety-critical function: A function whose failure to operate or incorrect operation will directly result in a mishap of either catastrophic or critical severity.

safety-critical item: An item that has been determined through analysis to potentially contribute to a hazard with catastrophic or critical mishap potential, or that may be implemented to mitigate a hazard with catastrophic or critical mishap potential.

safety risk acceptance: The activity whereby a public transportation agency controls the probability or severity of the potential consequences of hazards.

safety-sensitive function: Performance of any of the following duties by employees or contractors:

- Operating a revenue service vehicle, including when not in revenue service.
- Operating a nonrevenue service vehicle, when required to be operated by a holder of a CDL.
- Controlling dispatch or movement of a revenue service vehicle.
- Maintaining (including repairs, overhaul and rebuilding) a revenue service vehicle or equipment used in revenue service.
- Carrying a firearm for security purposes.

severity: The magnitude of potential consequences of a mishap to include death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or monetary loss.

Small Starts Program: A Federal Transit Administration grant program for capital costs associated with new fixed guideway systems, extensions and bus corridor improvements. Grants must be for under $75 million in New Starts funds, and total project costs must be under $250 million.

software: A combination of associated computer instructions and computer data that enable a computer to perform computational or control functions. Software includes computer programs, procedures, rules and any associated documentation pertaining to the operation of a computer system. It also includes new development, complex programmable logic devices (firmware), NDI, COTS, GOTS, reused, GFE and transportation agency–developed software used in the system.

standard operating procedure: A set of step-by-step instructions compiled by an organization to help workers carry out routine operations including maintenance activities

state of good repair: 1. A condition in which assets are fit for the purpose for which they were intended. 2. Synonymous with the term “capital replacement” and encompasses refurbishment, rehabilitation and modernization.

system: The organization of hardware, software, material, facilities, personnel, data and services needed to perform a designated function within a stated environment with specified results.

transportation agency: The organization that operates transportation service and related activities. Also called *transit system*, *rail transit agency*, *transit agency*, *operating agency*, *operating authority*, *transit authority* or other similar term.

Abbreviations and acronyms

A&E	architectural and engineering
ALARP	as low as reasonably practicable
ASP	Agency Safety Plan
BOD	Basis of Design
CCTV	closed-circuit television
CDL	commercial driver’s license
CDRL	Contract Deliverable Requirements Lists
CE	certifiable element
CEL	Certifiable Elements and Sub-Elements List
CIL	Certifiable Items List
CFR	Code of Federal Regulations
CMAR	construction manager at risk
CNG	compressed natural gas

CoC	Certificates of Conformance
COTS	commercial-off-the-shelf
CSCC	Construction Specification Conformance Checklist
CSO	chief safety officer
DB	design–build
DBB	design–bid–build
DBOM	design–build–operate–maintain
DCC	Design Conformance Checklist
DCM	Design Criteria Manual
DOR	designer of record
FMCSA	Federal Motor Carrier Safety Administration
FMEA	failure modes and effects analysis
FTA	Federal Transit Administration
FRA	Federal Railroad Administration
GFE	government-furnished equipment
GMP	guaranteed maximum price
GOTS	government-off-the-shelf
MCP	major capital project
NTSB	National Transportation Safety Board
O&M	Operations and Maintenance
OHA	operations hazard analysis
OIL	Open Items List
P3	public–private partnership
PHA	Preliminary Hazard Analysis
PMOC	project management oversight consultant
PMP	Project Management Plan
PRO	Pre-Revenue Operations
QA	quality assurance
QMS	quality management system
RAP	Rail Activation Plan
RFP	request for proposal
ROW	right-of-way
RTA	rail transit agency
SCADA	supervisory control and data acquisition
SITP	System Integration Test Plan
SMS	Safety Management System
SOP	standard operating procedure
SRM	Safety Risk Management
SSC	safety and security certification
SSCM	safety and security certification manager
SSCRC	Safety and Security Certification Review Committee
SSCWG	Safety and Security Certification Working Group
SSCVR	Safety and Security Certification Verification Report
SSCP	Safety and Security Certification Plan
SSMP	Safety and Security Management Plan
SSP	System Safety Program
SSPP	System Safety Program Plan
SSOA	state safety oversight agency
TAM	transit asset management
TVA	threat and vulnerability assessment

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	Rail CEO Approval	Policy & Planning Approval	Publish Date
First published	Dec. 1, 2023	March 2, 2024	April 21, 2024	April 25, 2024	May 8, 2024

Appendix A: Safety and security certification references

Various FTA regulations, circulars, handbooks and interpretative documents describe requirements and recommendations addressing safety and security certification. These references include the following:

- **49 CFR §673.27(c)** requires rail transportation agencies (RTAs) to "establish a process for identifying and assessing changes that may introduce new hazards or impact the transit agency's safety performance" and "if [the RTA] determines that a change may impact its safety performance, then the transit agency must evaluate the proposed change through its Safety Risk Management process."

- **49 CFR §673 Section IV section-by-section analysis** specifies that the FTA expects RTAs to implement 49 CFR §673(c) through a "safety certification process that [ensures] that safety concerns and hazards are adequately addressed prior to the initiation of passenger operations for News [sic] Starts and other major capital projects to extend, rehabilitate, or modify an existing system, or to replace vehicles and equipment." While documentation (evidence) of tests, inspections and other verification and validation activities gathered by quality assurance personnel are used as evidence that the system is safe and secure to use, safety and security certification is *not* a quality assurance activity, nor is it an element of a quality management system (QMS).

- **49 CFR §633 Project Management Oversight (§633.19)** specifies dollar thresholds for safety and security certification. The total project cost of $300 million or more with project receipt of federal funds of $100 million or more

- **The FTA's *Handbook for Transit Safety and Security Certification* (FTA-MA-90-5006-02-01)** details safety and security certification for the rail industry. Issued in November 2002, the *Handbook* is based upon MIL-STD-882 *System Safety* (current revision is "E," issued May 11, 2012). The FTA primarily wrote FTA-MA-90-5006-02-01 to address the safety and security certification of new rail transit systems and major capital projects. However, the scope of safety and security certification has expanded in the intervening decades as it has been recognized that system modifications and non-major projects can benefit from the application of the safety and security certification process.

- **Chapter 2 of FTA-MA-90-5006-02-01 and Subsection 6.7 of FTA C 5800.1** identifies systems that require safety and security certification. These systems include but are not limited to systemwide elements (e.g., passenger vehicles, catenary), fixed facilities (e.g., stations, pedestrian bridges), plans, procedures and training (e.g., emergency preparedness plans, rule books), and operations and emergency training (e.g., training for personnel performing safety-sensitive functions).

- **FTA-MA-90-5006-02-01** defines the safety and security certification process as "the series of processes that collectively verify the safety and security readiness of a project for public use." As the FTA does not explicitly define "project" and the term can be ambiguous, each transportation agency should define the term in system-level program documents.

- **49 CFR §673, Public Transportation Agency Safety Plan, Subsection 673.27, Safety Assurance** specifies:

> (a) Safety assurance process. A transit agency must develop and implement a safety assurance process, consistent with this subpart. A rail fixed guideway public transportation system, and a recipient or subrecipient of Federal financial assistance under 49 U.S.C. Chapter 53 that operates more than one hundred vehicles in peak revenue service, must include in its safety assurance process each of the requirements in paragraphs (b), (c), and (d) of this section…

> (c) Management of change. (1) A transit agency must establish a process for identifying and assessing changes that may introduce new hazards or impact the transit agency's safety performance.
>
> (2) If a transit agency determines that a change may impact its safety performance, then the transit agency must evaluate the proposed change through its Safety Risk Management process.

- **49 CFR §673, Public Transportation Agency Safety Plan, Subsection §673.27, Safety Assurance, Article IV, section-by-section analysis** specifies:

> Pursuant to §673.27(c), rail fixed guideway public transportation systems and recipients and subrecipients that are subject to this rule and operate more than one hundred vehicles in peak revenue service must manage changes in their systems. These transit agencies must develop processes for identifying and assessing changes that may introduce new hazards or impact safety performance. If a transit agency determines that a change might impact safety, then the transit agency would need to evaluate the change using Safety Risk Management activities established under §673.25. These changes would include changes to operations or maintenance procedures, changes to service, the design and construction of major capital projects (such as New Starts and Small Starts projects and associated certifications), organizational changes, and any other changes to a transit agency's system that may impact safety performance. Each rail transit agency should include a description of the safety certification process that it uses to ensure that safety concerns and hazards are adequately addressed prior to the initiation of passenger operations for News [sic] Starts and other major capital projects to extend, rehabilitate, or modify an existing system, or to replace vehicles and equipment…

- **Public Law 112-141, Moving Ahead for Progress in the 21st Century Act (MAP-21), Subsection 5329(d)(1)(C)** states that each public transit agency shall specify in its Public Transportation Agency Safety Plan "strategies to minimize the exposure of the public, personnel, and property to hazards and unsafe conditions."

- **FTA C 5800.1, Safety and Security Management Guidance for Major Capital Projects** provides safety and security guidance for recipients with major capital projects covered by 49 CFR §633, "Project Management Oversight." This circular identifies specific safety and security activities that a recipient must perform and document in a Safety and Security Management Plan (SSMP). In this circular, FTA explains that the SSMP is part of the recipient's Project Management Plan (PMP). As part of the PMP, the SSMP must be updated whenever the PMP is required.

- **The FTA's March 2016 Project and Construction Management Guidelines** specify:

> Section 2.1 identifies that the "process to plan, design, program, and implement a transit capital project, particularly a major transit capital project" includes "Safety and Security Management [activities] including safety and security certification of the project."

Section 2.2.11.1 clarifies the intent of the FTA regarding safety and security certification of major capital projects (MCPs):

> The FTA's aim with issuance of Circular 5800.1 was to strengthen the role of safety and security oversight and management in all phases of project development. FTA was particularly concerned about construction management, where safety and security responsibilities were often devolved solely to the contractor with the Project Sponsor's organization having very little involvement in day-to-day activities.

Section 2.2.11.4 clarifies the intent of the FTA regarding safety and security certification of non-major capital projects and small projects:

> The process described for Project Sponsors required to prepare an SSMP should be adjusted by Project Sponsors for other projects based upon the scale and requirements of the project being implemented. Typically, safety and security certification and hazard analysis will be required of the project at a minimum. The principles that ensure that safety and security are considered at each phase of a project are just as important for a small project as for an [Major Capital Project (MCP)]. In fact, because the small project's safety and security staffs may be far smaller than those of an MCP, it is particularly important that these functions not be delegated to those with little expertise or interest in seeing that they are adequately addressed throughout all project phases.

- **TSA's Rail Cybersecurity Mitigation Actions and Testing – SD 1580/82-2022-01, Section III, F** requires submission of Cybersecurity Assessment Program annually.

- Transit agencies can use the safety and security certification process to demonstrate compliance with the **29 CFR §1910 General Duty Clause** requirement that "each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees."

Appendix B: Bus Certifiable Elements and Sub-Elements List

The following Certifiable Elements List (CEL) is derived from APTA's Bus Procurement Guidelines. The FTA Handbook for Transit Safety and Security Certification has additional example CELs for rail-related projects. Each system will have other requirements that should be reflected in the CEL:

Overall requirements
Training

Operating environment
Noise
Fire safety
Fire suppression
Bus height
Step/floor height
Ramp clearances
Interior headroom

Engine
Engine (CNG)
Propulsion system (hybrid)
Transmission cooling
Hybrid drive system cooling
Transmission (conventional powertrain)
Retarder (transit coach)

Power requirements
Top speed
Gradability
Acceleration
Operating range

Passenger seating

Passenger assists

Hydraulic systems
Fluid lines
Fittings and clamps
Charge air piping
Radiator
Oil and hydraulic lines
Fuel
Fuel lines

Emissions and exhaust
Exhaust emissions
Exhaust systems
Exhaust aftertreatment

Altoona testing
Structural validation
Distortion
Resonance and vibration

Engine compartment bulkheads

Crashworthiness (transit coach)

Corrosion

Towing

Jacking

Hoisting

Floor
Design (transit coach)
Design (commuter coach)
Design (articulated transit coach)
Strength
Floor covering

Interior lighting
Passenger
Driver's area

Fare collection

Platforms
Driver's area
Driver's platform
Farebox
Rear step area to rear area (transit coach)

Wheel housing
Design and construction
Design and construction (transit coach)
Articulated joint (articulated transit coach)
Bellows

Wheels and tires

Steering
Steering wheel

Brakes
Service brakes
Actuation
Friction material
Hubs and drums (transit coach)
Hubs and drums (commuter coach)
Passenger door interlocks

Pneumatic system

General electrical requirements
Batteries
Grounds
Low-voltage/low-current wiring and terminals
Electrical components
Electrical compartments
Multiplexing data communications

Driver's area
Glare
Visors/sun shades
Driver's controls
Brakes and accelerator pedals
Shield

Windshield wipers and washers

Driver's seat

Mirrors
Curbside mirrors
Street-side mirrors

Emergency exit (egress) configuration
Door controller
Door open/close
Door projection (transit coach)
Door height above pavement
Closing force

Accessibility provisions
Securement system
Roof ventilation/escape hatches

Communications
Camera surveillance system
Public address system
Automatic passenger counter (APC)
Radio handset and control system
Event data recorders (EDR)

Rear door interlocks (transit coach)
Emergency operation

Appendix C: Bus certification

The action plan in **Table 3** outlines the steps and helpful hints to achieve both a successful bus safety and security certification and successful bus procurement:

TABLE 3
Bus Security Certification Action Plan

1. Complete safety and security certification methodology.	
Task	**Comments**
Draft safety and security certification methodology for specific bus procurement project.	• Scalable. • Determine if new bus specifications exist. If not, use APTA's Standard Bus Procurement Guidelines (see References). • Critical for the project team to be informed of their process.
Finalize safety and security certification methodology.	
Conduct "page turn" session with project team, including project manager, to review the methodology.	• Treat the meeting as a familiarization session. Questions should be encouraged.
Submit methodology to appropriate meeting for approval.	• Decide on the mechanism for reviewing and approving the certification documents, hazard analyses and checklists. • Will this process be a separate Safety and Security Certification Committee meeting or part of the bus procurement project meetings? • Requires approval from agency leadership.
Approve safety and security certification methodology.	
Add SSC activities into the overall schedule (Safety Milestone Schedule).	• Work with scheduler to add certification milestone dates. • Needs to be part of the master schedule.
Appoint SSCM for implementing the safety and security certification methodology.	• Depends on the agency.
NOTE: During each step of the bus procurement safety and security certification, the project manager should review the level of risk and make a determination regarding its acceptance versus the allocation of additional resources to resolve it.	
2. Prepare Certifiable Elements List (CEL).	
Task	**Comments**
Use APTA Standard Bus Procurement Guidelines.	• Contains elements and sub-elements. • Project manager will review level of risk. • No need to reinvent the wheel
Submit to designers and project manager for review.	• See sample CEL in next section.
Hold workshop with the project team to review the CEL.	

TABLE 3
Bus Security Certification Action Plan

3. Develop Safety and Security Certification Plan (SSCP).	
Task	**Comments**
Develop draft SSCP. Finalize SSCP. Approve SSCP. Appoint SSCM to implement SSCP.	Separate SSCP not necessary if: • Part of a larger project that has an SSCP. • The agency has a current SSCP. • The project team decides the methodology is acceptable for the procurement. • No need for duplication. • Cannot skip this step if the methodology has not been approved.
Determine when external agencies require the SSCP or methodology for review.	• Review the SSOA's manual for safety certification and add those deliverables to the Safety Milestone Schedule.
4. Establish Safety and Security Certification Committee (SSCC).	
Task	**Comments**
Form SSCC or Project Committee.	Not required if: • Safety and Security Review Committee is already established. • May be part of the project meetings for bus procurement. • Avoid duplicate meetings.
Review Safety Milestone Schedule.	
Review and approve all documents.	
5. Perform hazard analysis.	
Task	**Comments**
Determine type of hazard analysis. Fault tree, process hazard analysis and operations hazard analysis are recommended. Further information regarding how to conduct a PHA is provided in the next section.	• Fault tree to capture incidents and near-miss events. • FMEA should be obtained from the manufacturers for review. • However, based on time and financial constraints, a PHA and OHA may suffice. • Use the APTA Technical Standards for ideas. • PHA can be used also, but fault tree describes the event whereas the PHA describes the hazard and the risk consequences. • OHA required to ensure that procedures and training are undertaken
Hold a workshop with all disciplines and project management to evaluate the identified hazards and determine their feasibility into the bus design.	
Submit hazard analysis to the SSCC or other project meeting.	
An Open Items List should be prepared from the hazard analysis and reviewed at the meeting.	• The OIL should be tracked to closure and reviewed by the committee. All unacceptable and undesirable open items should have approved restrictions and/or exceptions before the buses enter revenue operation. • Temporary use permits may have to be issued for items that have not been approved.

TABLE 3
Bus Security Certification Action Plan

6. Complete design criteria or design standards.	
Task	**Comments**
NOTE: If preparation of design criteria is not required and there are no current design criteria, then skip to construction conformance.	
Draft safety and security design criteria.	• Use APTA Standard Bus Procurement Guidelines (see References) as a great start and reference.
Complete final safety and security design criteria.	• Unique to the agency. • Make sure the hazard resolutions are included in the design criteria.
7. Complete Design Conformance Checklists for prototype bus design.	
Task	**Comments**
NOTE: Required only if a novel prototype design is being done. If no design is being done, skip to construction conformance.	
Draft Design Conformance Checklists using the design criteria.	
Have a workshop with project team to review the DCCs.	• Designers should provide feedback and comments.
8. Review compliance with DCCs.	
Task	**Comments**
Finalize DCCs and issue to project team for final review.	• Designers should initial their discipline DCCs. Project manager should sign off for each discipline.
Issue DCCs to SSCC.	
Approve DCCs.	
Provide documentation to configuration management and to external agencies.	• Should already be included in the Safety Milestone Schedule.
Provide documentation to procurement before issuance of RFP. SSC methodology and/or SSCP should be included in the technical specifications.	• Should accompany contract documents, along with the technical specifications for solicitation of proposals. • The completion of the design (technical specifications) and completion of the DCCs should occur at the same time.
9. Complete Construction Conformance Checklists for verifying "as-built" compliance with design specifications for pilot bus.	
Task	**Comments**
Contractor builds a pilot bus.	
Prepare Construction Conformance Checklists based on technical specifications, and include the checklists in the first article inspection.	• Contractor and agency inspectors (resident inspectors) attend the first article inspection. • Have resident inspectors complete the checklists at that time. • Creates economies of scale.
Use the manufacturer's Federal Motor Vehicle Safety Standards certifications for those items that apply.	• Reduces burden on the transit agency.

TABLE 3
Bus Security Certification Action Plan

Use certificates and Contract Deliverable Requirements Lists (CDRLs) for undercoating, flooring, fire resistance, crashworthiness, electronic functionality, striping layout, camera layouts and power plant.	• Certificates from manufacturers provide confirmation of product reliability.
Use manufacturers' formal quality assurance program and quality manufacturing certificates for COTS items.	• Certificates from the manufacturer determine that failure modes have been conducted and that reliability and sustainability meet national standards. • Agency not required to conduct failure modes analysis when the burden should be on the manufacturer.
Review committee should approve these checklists and restrictions and/or exceptions.	
An OIL should be prepared and tracked to closure.	• For open Items that are not closed, temporary restrictions or exceptions are required.
Provide documentation to configuration management.	
10. Develop verification and testing plans for safety and security requirements.	
Task	**Comments**
Post-delivery testing or acceptance testing is required.	
Review acceptance testing plans, and determine if any additional safety testing is required.	• Inspectors will be able to conduct all tests. • Have a procedure for submission of all test results to the SSCM. • Avoids duplication.
Review testing schedule.	• Make sure the safety milestone schedule and the testing schedule are reviewed together and adjusted accordingly.
Use Altoona Test Reports when applicable.	• Obtain a copy of the test report during the procurement step or the safety and security methodology step.
Conduct testing of new bus models.	• Use 49 USC §5323(c) and FTA's implementing regulation at 49 CFR §665 for testing requirements: "A manufacturer of a new bus model or a bus produced with a major change in components or configuration shall provide a copy of the final test report to the recipient at a point in the procurement process specified by the recipient, which will be prior to the recipient's final acceptance of the first vehicle."
Submit all test plans to SSCC for approval.	
11. Develop or update safety requirements for procedures, rulebooks and training.	
NOTE: Agencies should make certain this requirement is part of their Certifiable Elements List.	
12. Perform final operational readiness review.	
Task	**Comments**
Submit all operations test plans to SSCC for approval.	• Field-test each operator on critical functions. • Conduct one or more full-scale exercises with fire, law enforcement and EMS. • Conduct familiarization training for fire and law enforcement.
Verify all open items.	
13. Issue certificates of compliance and issue final Safety and Security Certification Verification Report.	
NOTE: Restrictions and/or exceptions should be included in the Safety and Security Certification Verification Report.	

Appendix D: Additional information on capital infrastructure project delivery methods

While the SSC process for any project should closely align with the process outlined in Section 2.2, this appendix describes nuances associated with each capital infrastructure project delivery method. Refer to the FTA PMOC guidelines and FTA Project and Construction Management Guidelines for additional information on delivery methods.

Design–bid–build

Design−bid−build (DBB) was the traditional method of project delivery and has been the most widely used. DBB is a linear process where one task follows completion of another with no overlap. It commences with a transportation agency selecting a design team to prepare design/construction documents.

The design team is selected separately from the general contractor and reports directly to the agency. Most often the design team will prepare these documents and provide them to the agency to be advertised publicly to any general contractor or to a select, prequalified group that is invited to bid what they believe the total cost of construction will be. This bid is inclusive of various other bids from subcontractors for each specific trade, and the general contractor's fee is generally built in.

A DBB contract is most suited for less complicated projects that are budget-sensitive but not necessarily schedule-sensitive or subject to change. The agency can define and control the design through the architectural consultant.

Construction manager at risk (CMAR)

The construction manager at risk (CMAR) process is an alternative DBB project delivery method in which the contractor is brought in during the early stages of design to work alongside the architectural and engineering (A&E) team. The CMAR contractor brings a pre-construction team to partner with the A&E to provide constructability and market conditions feedback, as well as material options, as the design progresses. They prepare estimates at milestones (30%, 60%, 90% and 100% design) to ensure that the project, as it is designed, stays within budget.

Using the CMAR delivery method allows flexibility with respect to when during the design process enough is known to start construction. The pre-construction team can determine at any point during design to pull a component or work package out and start construction on it. Most often, this occurs between 60% and 100% drawing, when there is enough information for the contractor to be able to put the guaranteed pricing together. This methodology permits the project schedule to be shorter than a typical DBB situation, as there are concurrent operations of design and construction.

This element of the CMAR process requires a close and possibly expedited SSC process. Practically, this means quickly advancing certain aspects of safety and security certification, such as safety and security design criteria, certifiable elements and certifiable items. To accomplish this, close coordination and communication is required between the safety and security certification team and the CMAR contractor. The transportation agency staff should serve as a bridge between the design contractor and construction contractor as the project transitions through these phases as it relates to certification.

CMAR: Certification activities and responsibilities

The design contractor and CMAR construction contractors are identified with respect to the certification responsibilities they would assume when this methodology is applied. It should be noted that using CMAR for delivery means that some portions of the work may not go to 100% design before construction. Early

work packages may be pulled and advanced. In these cases, the process needs to be flexible to document as needed but allow the work to proceed.

The Safety and Security Certification Working Group as a whole will review the recommended structure of responsibilities and make the final determination. The transportation authority retains the responsibility of reviewing the compiled deliverables, ensuring that all activities are performed satisfactorily, and making the official submittals to oversight organizations as required.

In the case of early work packages, there should be early engagement with the designer of record (DOR) to follow the safety and security certification process, and the CMAR should be involved in review from the project outset. The DOR should prepare documentation of deliverables required, which then go to the CMAR for their execution.

Once the guaranteed maximum price (GMP) is established, the responsibility to perform the SSC activities should rest with both the design and construction contractors, and the deliverable asset(s) required should be well-defined and understood by all parties.

Design–build

The design–build (DB) project delivery method allows for the transportation agency to contract directly with one entity to provide both the design and construction for a project. In this case the design–builder assumes responsibility for both the design services and construction work. For safety and security certification, the process begins in the policy development, which enables the agency to provide guidance on the roles, responsibilities, deliverables and expected outcomes of the design–builder's certification program.

In a DB project, the SSCM is typically from a single entity and does not require the transfer of the position from one phase to the other.

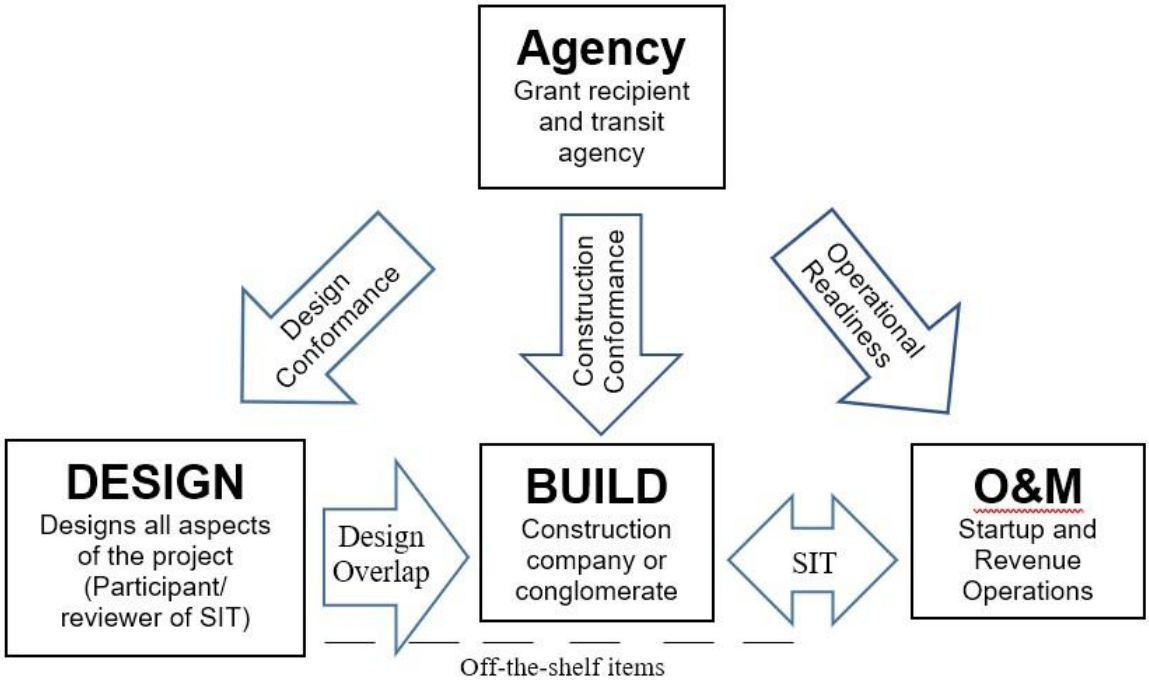
Design–build–operate–maintain

This section builds from Section 2.2 and discusses important recommendations for design–build–operate–maintain (DBOM). Increasingly, transportation agencies may not only contract out the design and construction of a project, but contract another party that will also operate and/or maintain the system. This decision could be made at the onset of the project or partway through the design–construction phase. These three groups—the designer, the builder and the operator—each represent one section of safety and security certification of a project. (It is possible that the designer will also be the construction contractor and/or the operations and maintenance [O&M] provider, reducing some complexity of the issues of a DBOM.)

The transportation agency, as owner to the project, is responsible for coordination between the various groups to ensure that the project is completed, tested and entered into revenue service. At the same time, the transportation agency, designer and builder may have their own set of oversight contractors to assist in their responsibility. The transportation agency is responsible for bringing all these groups together to ensure that the certification process is completed. This includes the design criteria conformance, construction specification conformance, and coordination for the system integration testing that will occur between the design, build and O&M portions. Operational readiness will largely rely on O&M but may include the builder for training, manuals or other assistance.

The DBOM project delivery approach is depicted in **Figure 1**.

FIGURE 1
DBOM Project Roles



DBOM: Common issues

DBOMs require a large amount of coordination between the different groups. Design, build and operational issues will overlap during the project. Construction may start before all systems have reached 100% design. This is commonly done in order to shorten the design–build portion of the project and to induce some project cost savings. An area of concern arises when the design is ongoing throughout the project with the result that design certification may not be done until late in the construction process or even during pre-revenue. Lack of coordination among the designer and the other groups can create issues with completing certification on time.

Similar issues can occur during construction. System integration testing requires coordination by the builder and O&M provider, as construction and installation of all systems may not be fully completed by the time some systems integration and testing may begin. For example, this might involve vehicle testing on the guideway prior to stations being completed. Hence, systems may need to be certified in a certain order, causing an "accordion" type effect with documentation. This type of coordination to oversee certification is the responsibility of the transportation agency, but all contractors should be made aware of their role and the process throughout the progression of the project.

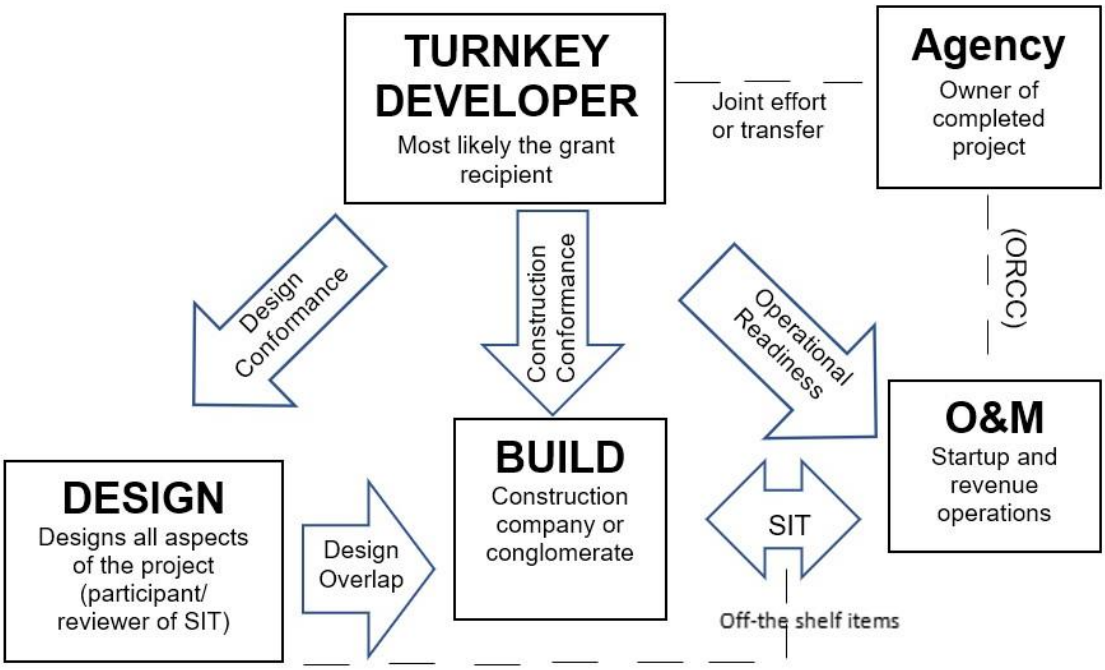
Another issue comes when there are construction changes by the builder that require changes in design. As the designer and builder are separate entities, the transportation agency should have a strong configuration management program for the project. A small change in the length or width of the passenger vehicle can trickle down to larger issues with stations, signaling, storage tracks or other infrastructure issues. Likewise, this causes issues in completing safety and security certification, as modifications or changes result in additional documentation needed to verify conformance to the checklist items to close them out.

Turnkey

The way a project is completed is becoming more complex, as agencies are determining the best way to finance a project as well. In turnkey projects, the final owner (transportation agency) of a project may be

completely separate from the design–build portion part of the project, including the part of safety and security certification, which is handled by the turnkey developer. In these cases, the roles and responsibilities chart may resemble **Figure 2**.

FIGURE 2
Turnkey Project Roles



In this example, the turnkey developer may be responsible for the design, build, funding and integration of the system as a whole. Additionally, they may select the O&M provider. Once the project is complete, they will turn the project over to the transportation agency, which is responsible for overseeing the revenue operations of the O&M portion of the contract. This format allows a different option for the operational readiness portion, where it could be removed from the turnkey developer and given to the transportation agency to complete. In either case, close coordination is needed between the turnkey developer and the transportation agency.

Turnkey: Common issues

From the beginning of the design process, the turnkey developer and the transportation agency will need to work together to ensure a smooth transition into pre-revenue and revenue operations. The transportation agency may not be as well-versed in the project-specific SSC issues and may need the support of the turnkey developer in understanding how certification was completed, along with open issues or mitigations put in place. The transportation agency may not even be ready to integrate into the project until just prior to pre-revenue, depending on hiring the necessary personnel. The final SSCVR should be the responsibility of the turnkey developer.

All certification documentation and configuration management documents will need to be transferred from the turnkey developer to the transportation agency for future use. Exact records will be needed from the turnkey developer so the transportation agency can trace any issues that may arise due to design or construction issues that might occur once in service. As the transportation agency will eventually be audited

and held accountable for the safety of the system, the agency's understanding of safety and security certification and change management during design and construction is critical even if they were not present.

Tracking of the risk register and open items needs to be transferred from one entity to the other. These are items that have been tracked throughout the construction process and should have been discussed with the design and build teams. This transfer will also require the continuous engagement by the transportation agency of what items are on the list, why they are there, mitigations in place, and plans or ongoing corrections to close these items.

Public–private partnerships (P3)

A public–private partnership (P3) describes various types of agreements between public and private entities. A P3 is typically formed by multiple firms that bring varied and extensive experience managing a project. Public–private partnerships can be used to procure new-build facilities, including developing new transportation assets, or to upgrade or expand an existing facility or transportation system.

Using a P3 method allows public agencies to fill both the technical knowledge gap and the funding gap through private involvement. Private sector input can also help spur technological and management innovation, which is critical for complex projects. A P3 contract also provides an instrument to allocate risks to the entity best suited to manage and mitigate them over an extended term, including a post-construction O&M period.

The main difference between a DBOM and a P3 project is the financing for the project. The P3 project utilizes private financing to fund the project. The P3 concessionaire recoups its investment from fare revenue and progress payments from the transportation agency.

> **NOTE:** P3 concessions are public–private agreements in which a private sector concessionaire takes on some of the risks and rewards of financing, constructing (or leasing), and operating and maintaining a transportation facility in exchange for the right to future revenues or payments for a specified term.

Clear lines of delineation should be found within the P3 agreement. The following items should be clearly defined in the P3 agreement, including roles and responsibilities:

- scope of work
- risk assessment, mitigation, allocation
- performance requirements
- design
- hazard, threat and vulnerability evaluation
- identification of project certifiable elements/items
- design verification
- construction verification
- safety and security test requirements
- testing and validation
- Safety and Security Certification Committees
- Safety and Security Certification Certificates
- training
- certification activities and responsibilities

TABLE 4

P3 Certification Activities and Responsibilities

Certification Task	Primary Responsibility	Review/Approval Responsibility*
Develop safety and security design criteria.	Concessionaire	Transportation agency or owner
Develop Safety and Security Management Plan that complements the agency plan.	Concessionaire	Transportation agency or owner
Develop Safety and Security Certification Plan that complements the agency plan.	Concessionaire	Transportation agency or owner
Establish Safety and Security Certification Committees/Working Groups.	Transportation agency or concessionaire, based on agency preference	Transportation agency or owner
Participate in safety and security certification committees/working groups.	Transportation agency and concessionaire	N/A
Develop hazard analysis (PHA, FMEA, OHA).	Concessionaire	Transportation agency or owner
Develop design criteria conformance checklist.	Concessionaire	Transportation agency or owner
Develop threat and vulnerability assessment.	Concessionaire	Transportation agency or owner
Develop Certifiable Elements List and Certifiable Items List.	Concessionaire	Transportation agency or owner
Develop Construction Specification Conformance Checklist.	Concessionaire	Transportation agency or owner
Develop Safety and Security Verification Tracking Log.	Concessionaire	Transportation agency or owner
Develop test program plans.	Concessionaire	Transportation agency or owner
Perform integrated testing.	Concessionaire	Transportation agency or owner
Perform safety and security review of engineering design.	Concessionaire	Transportation agency or owner
Develop operations and maintenance plans.	Concessionaire	Transportation agency or owner
Develop/perform procedures and training.	Concessionaire	Transportation agency or owner
Issue final safety and security certification.	Concessionaire	Transportation agency or owner, signed by the CSO and the accountable executive
Develop/submit Safety and Security Certification Verification Report.	Concessionaire	Transportation agency or owner

*****The owner of the project may not necessarily be the transportation agency. However, if the project owner receives FTA money, then it needs to follow this process.