Authors Companies Titles Sessions Text Search

Exit Home Help

This page is for navigational purposes only. Scroll down to view the text. In order to go back to one of the main screens, return to this screen by scrolling up or by clicking on the thumbnail.

# Safety Certification Of MUNI'S Advanced Train Control System: A View From The Trenches

Daniel J. Rosen and Patricia G. DeVlieg
S.F. MUNI Railway
San Francisco, CA

## ABSTRACT

San Francisco's Municipal Railway is currently in the throes of implementing our new Advanced Train Control System (ATCS). Revenue Service implementation is proceeding in stages, each of increasing complexity. With ATCS, MUNI for the first time is opening a new rail extension under the safety oversight of the California Public Utilities Commission (CPUC). Each revenue stage must be independently safety certified. Project staff, working with our Engineering and Safety consultants, provide the necessary technical documentation for safety certification. In addition, the process requires all operating departments to participate in the process, with regard to procedures review and training. For some, this requires a significant change to their normal way of doing business. Since the safety certification process is basically a documentation activity, some operating departments need assistance in understanding the requirements, developing the Standard Operating Procedures (SOPs), and tracking all the activities necessary to meet the safety certification audit requirements.

This paper will present how MUNI has defined and distilled the overall safety certification requirements into manageable deliverables for each area of responsibility; i.e.: track department; central control; vehicle maintenance, etc. The issues go beyond the bureaucratic and technical. Inevitably, there is also "culture shock" generated by any new system which is perceived to disrupt existing behaviors, as well as uneasiness created by MUNI's first exposure to oversight by an outside agency.

Solutions discussed will include: Convening a task force of all affected departments; tracking work via action items; defining specific deliverables; etc. This paper will present not only the "How to…", but will also include some "How not to …." advice, based on MUNI's experience.

## INTRODUCTION

San Francisco Municipal Railway (MUNI) is the public transit agency for the City and County of San Francisco, supporting 700,000 passenger boardings daily, roughly equal to the population of the City. MUNI operates four transit modes, the most celebrated being our cable cars, which are the last of their kind in the world. More conventional transit is provided by electric trolley, diesel bus, and streetcars. MUNI's streetcar fleet has a historic component, with 17 rehabilitated PCCs and 13 one-of-a-kind historic streetcars from around the world, which operate on our downtown surface feeder line. MUNI also provides light-rail service, in a mixed street and subway service into downtown.

MUNI's LRV (Light Rail Vehicle) fleet consists of 136 light rail vehicles: 77 new Breda LRV2s are currently being delivered, supplemented by 59 Boeing SLRVs, which are now 20 years old. MUNI schedules approximately 900 LRV trips daily through the subway, and carries about 130,000 passengers on 5 LRV lines. It is the safety certification of our recent major light-rail service expansion which is the subject of this paper.

### Projects Being Certified

Since the opening of the Market Street Subway in 1980, MUNI's LRV service has not expanded, other than a 3-mile J-line surface extension in 1993. All five surface LRV lines converge on the Market Street Subway, to serve five downtown stations, four of which are shared with BART (See Figure 1). All five lines turnback at Embarcadero Station. This stub-end turnback has long been identified as a significant throughput bottleneck, and plans for an expanded turnaround or turnback facility have been studied since the subway opened in 1980. Extensive redevelopment in the South-of-Market area (site of the new Giants' Ballpark) in recent years, has stimulated the need for extending LRV service past Embarcadero Station. Another longstanding incentive has been to link MUNI rail service to the CalTrain commuter rail operation which serves the Peninsula and South Bay.

To address the need for improved subway service, and to serve the South-of-Market area, MUNI embarked on three major rail infrastructure upgrades:

- MUNI Metro Turnback (MMT): 0.5-mile extension from Embarcadero Station, including underground turnback and storage tracks, with a surface "Ferry Portal" on the Embarcadero at Folsom Street.
- MUNI Metro Extension (MMX): 1.5 mile extension from the MMT's Ferry Portal to the CalTrain Depot, including 4 surface stations.
- Advanced Train Control System (ATCS): Replacement of the existing 100-Hz track-circuit based signal system with Communications Based Train Control (CBTC), with the goals of enhancing throughput, safety, and operational flexibility.

ATCS is being introduced into service in stages. ATCS Stage 1 introduced ATCS control in the MMT portion of the subway, with shuttle train service between Embarcadero Station and the CalTrain Depot.

In October 1997, it was announced that revenue service would begin on January 10, 1998. Service on the MMX required implementing all three projects: ATCS to control the MMT; the MMT connection to the MMX; and the MMX surface extension. MUNI's Safety Certification Plan (SCP) for ATCS Stage 1 was expanded to incorporate safety certification for the three projects.

## MUNI's Organizational Environment

The San Francisco Municipal Railway (MUNI) inaugurated service in 1912, and is the oldest publicly owned Transit Company in the United States. From its roots as a traditional transit company, MUNI's organizational environment has changed radically. MUNI has undergone a number of organizational restructurings. MUNI's internal structure has been carved and recarved into various organization styles: centralized versus decentralized; all authority at the Division or garage level, to authority at headquarters. These swings in organizational styles have had a direct effect on MUNI's Safety Certification in the following ways:

- MUNI allowed a 4-member System Safety Department that was created in 1980 to diminish to a staff of 1. This has had the effect of minimizing the role System Safety was able to play in Safety Certification.
- There has been no formal revision to the MUNI Rulebook (all modes: rail, bus, cable car, trolley) since 1971 and no formal change to the LRV Rules and Procedures in 20 years. The effect has been

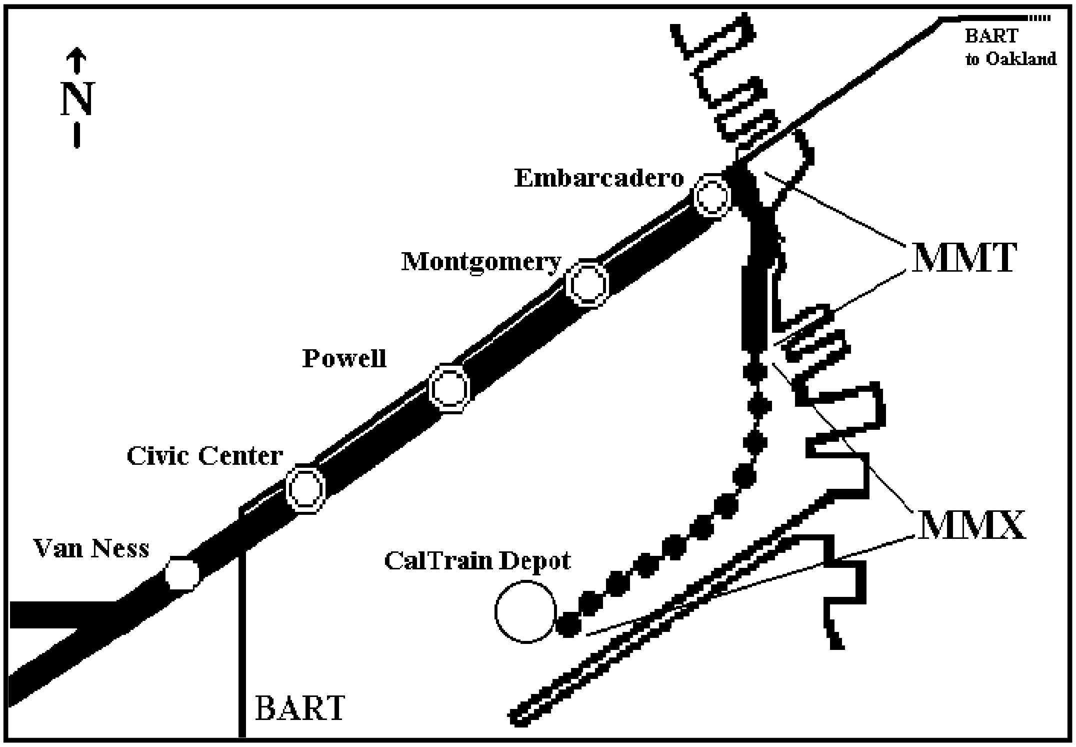


*Figure 1. Area of Downtown Subway and the MMX Shuttle Service Extension*

that no MUNI department has been charged with the responsibility of Rulebook revision.

- MUNI does not yet have a unified maintenance training strategy in place, and the 3-year old maintenance training unit is chronically understaffed, with only three maintenance trainers for 1000 maintenance employees. Therefore, individual maintenance units develop their own independent training strategies. This has meant that documentation of training has varied from unit to unit, and project to project.
- Unlike most railroads, at MUNI there is no Rules Department.

### Culture Shock

Even in the best of circumstances, implementing a major new system generates organizational culture shock. Readying each of the three projects individually, while accepting a new LRV fleet, was already a major effort for MUNI. An added complication was the need to coordinate schedules and access to resources among the three projects so that completion converged on the same service-start/up date. The requirement to develop and implement a newly mandated Safety Certification Process added significantly to the overall complexity of the task, and had tremendous impacts on all aspects of rail operation.

By its very nature, ATCS by itself has had a major impact on MUNI's rail operations. ATCS moves the rail organization from a decentralized control environment to a centralized one; from a loose-knit, informal training approach to a formalized well-documented training approach; from "ok-he's-ready-to-go" to a formal certification of each individual; from "what do you mean there are no track circuits and no shunt protection for signal crews" to a maintenance environment governed by strict supervision from Central Control to grant subway access to signal maintenance crews.

Another culture shock has been the introduction of oversight by the California State Public Utilities Commission (CPUC). MUNI inaugurated service in 1912 as a self-certifying railway. Subsequently, the California State PUC was formed, and MUNI's rail operation was explicitly "grandfathered" out of CPUC oversight. Recent Federal legislation required that MUNI's rail operations come under CPUC safety oversight on January 1, 1996. The ATCS/MMT/MMX extension which commenced service on January 10, 1998 was the first major MUNI rail service extension subject to CPUC oversight.

## ATCS INDEPENDENT SAFETY REVIEW

Prior to MUNI's rail operations coming under CPUC oversight, the ATCS Contract had provided for contracting with an Independent Safety Consultant (ISC) to oversee the implementation of all safety-critical elements of ATCS. MUNI contracted with Lea + Elliott to serve as the ISC for MUNI's ATCS. The ISC was contracted to provide an independent safety audit of both hardware and software modifications to the standard Alcatel SELTRAC product required for MUNI's installation. The ISC's mandate includes:

- To Develop an ATCS-specific System Safety Program Plan (SSPP), including a problem identification and tracking methodology for safety issues, to ensure that all safety-related items are successfully tracked, and the proper resolution identified and documented;
- To Chair a Safety Advisory Board (SAB) to identify, examine and resolve safety-related issues that arise throughout the course of the ATCS procurement;
- To Review safety critical Alcatel submittals; also the role of humans (passengers and MUNI personnel) relative to their potential impact upon the overall safety of the ATCS, including operating procedures, maintenance and training programs and their relationship to ATCS safety;
- To Qualitatively Analyze Software of the ATCS supplier;
- To Monitor and Evaluate safety-related activities and inputs of the ATCS supplier throughout the procurement process, including ATCS design reviews;
- To Audit safety verification safety analyses, test results, records of prior experiences submitted by Alcatel, and observe and review at-plant and on-site tests and demonstrations of ATCS.

### Safety Advisory Board (SAB)

A primary task of the ISC has been to chair the ATCS Safety Advisory Board (SAB). The SAB is a team of individuals representing the diverse elements of the MUNI, as well as the outside expertise (consultants) employed to facilitate or oversee implementation of the ATCS. Representatives on the SAB include MUNI System Safety, Maintenance, Operations, ATCS Project staff, Booz-Allen & Hamilton (ATCS Engineering Consultant) and Lea + Elliott (ATCS Independent Safety Consultant.). Others in attendance at SAB meetings are representatives from the

CPUC and the FTA Project Management Oversight (PMO) team, as well as representatives from Alcatel (the ATCS Contractor).

The SAB meets at regular intervals, and tracks safety-related open items. The Board has the authority to assign tasks to Board members to resolve open safety items. Typically, these activities include, investigating specific ATCS design elements; documenting and recommending adjustments to MUNI's operations and maintenance practice; integrating safety elements of ATCS with adjacent systems, especially LRV2. In some cases the Board has directed MUNI to conduct specific tests to provide field evidence of ATCS or vehicle characteristics.

In the event of any safety-related incidents occurring in the course of the ATCS project, the SAB takes the lead role in evaluating the findings of the subsequent investigation, and the merit of any proposed mitigations.

## OVERVIEW OF SCP (SAFETY CERTIFICATION PLAN)

MUNI's Safety Certification process provided for certification of three Capital Projects: ATCS-Stage 1, the MMT Subway extension and turnback facility, and the MMX surface extension. Both the MMT and MMX rail extensions were near completion prior to the commencement of CPUC oversight. In meetings with the CPUC, it was determined that the design, engineering and construction practices already in place on MMT and MMX would satisfy CPUC requirements. However, certification for training, and rules and procedures for all three projects, as well as ATCS safety verification and validation certification, would be required in the SCP.

Requiring that three projects be certified meant that elements from each were rolled into one unified Safety Certification Plan. The SCP that had been developed by the ATCS Consultant, BAH, dealt exclusively with the ATCS Stage 1 Safety Certification requirements. Therefore when the decision was made to combine certification for the three projects into one, the SCP was expanded to include elements from the other projects.

Additional elements from the MMT and MMX projects that were incorporated into the existing SCP for ATCS included: Ventilation and Undertrain Deluge training (MMT), SF Fire Department (SFFD) orientation and familiarization training (MMT), Central Control Emergency procedures (MMT & ATCS), rules and procedures revision (MMT/MMX/ATCS). Operations and maintenance training elements were expanded to include all three projects. Train operators had to become familiar with new territory, (the MMT, and

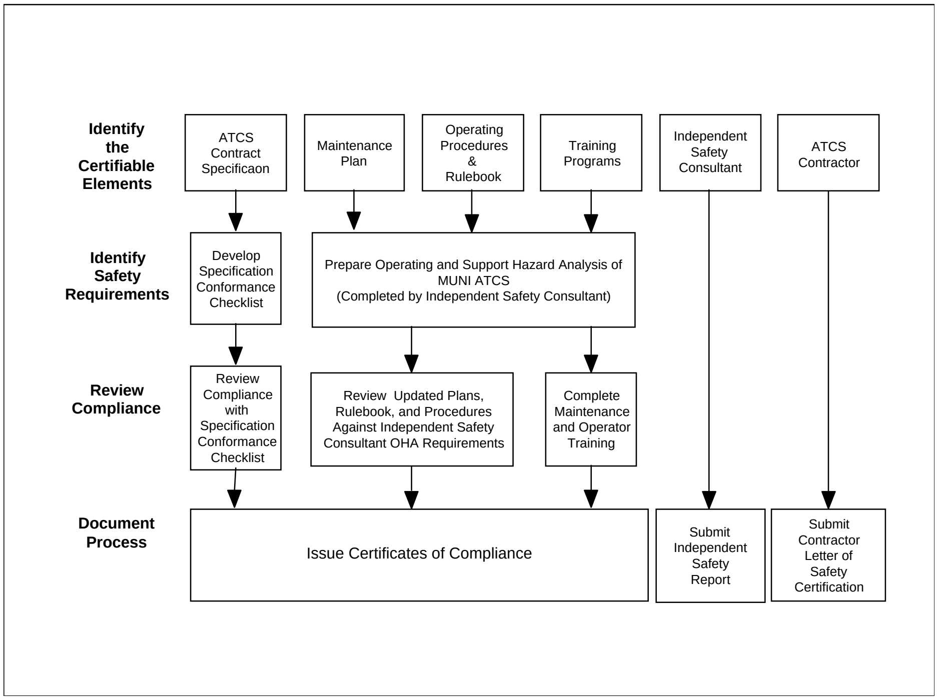

Identify the Certifiable Elements
ATCS Contract Specificaon
Maintenance Plan
Operating Procedures & Rulebook
Training Programs
Independent Safety Consultant
ATCS Contractor
Identify Safety Requirements
Develop Specification Conformance Checklist
Prepare Operating and Support Hazard Analysis of MUNI ATCS (Completed by Independent Safety Consultant)
Review Compliance
Review Compliance with Specification Conformance Checklist
Review Updated Plans, Rulebook, and Procedures Against Independent Safety Consultant OHA Requirements
Complete Maintenance and Operator Training
Document Process
Issue Certificates of Compliance
Submit Independent Safety Report
Submit Contractor Letter of Safety Certification

*Figure 2. Stage 1 ATCS Safety Certification Process*

MMX) as well as ATCS. Maintenance staff were trained on components of ATCS, MMT switches and facility systems, as well as the surface Vital Processor Interlockings (VPI) and track signals and switches (MMX). Documentation for all of these activities had to be included as part of the SCP.

The guiding document for this effort was a Safety certification Plan (SCP) drafted by Booz-Allen & Hamilton and adopted by MUNI. Figure 2 provides an overview of the SCP process. The work of the SCP is distilled into the list of Certifiable Elements and Deliverables, which make up the final report, and are listed below:

### SCP Certifiable Elements

1. ATCS Contract, by the ATCS Engineering Consultant (BAH)
2. Central Control Operating Manual, by MUNI and BAH
3. LRV Operating Rules and Procedures, by MUNI
4. Central Control Operator Training Program, by Contractors and MUNI
5. Vehicle Operator Training Program, by MUNI
6. Rail Inspectors Training Program, by MUNI
7. Independent Safety Consultant (ISC) Review, by ATCS ISC (L+E)
8. MUNI Maintenance Plan, by Contractors and MUNI
9. Safety Advisory Board Open Items, by ATCS ISC (L+E)

### SCP Deliverables

1. Certificates of Compliance for each Certifiable Element
2. Procedure Review Checklists
3. Specification Conformance Checklist
4. Operations and Maintenance Training Records
5. Report of the Independent Safety Consultant
6. Contractor's Statement of Safety Certification

## TEN ELEMENTS FOR SUCCESS

By following the SCP, MUNI was able to meet all the requirements and begin Revenue Service on the January 10, 1998 start date. Listed below are lessons learned from MUNI's experience:

### 1. Skills Needed On the Team To Be Successful

What skills do you need on your team to successfully complete the SCP?

OVERVIEW person from the Transit Property who understands the SCP process, who can liaison with consultant and professional Safety Experts. If possible, this person should also be able to put the SCP in terms your people will understand, i.e. someone who can talk with the Track Foreman and explain what the SCP is.

ORGANIZER person who is systematic and organized, a great filer, a detail person, a person who loves to make checklists to see that all tasks are carried out.

MICRO MANAGER who can insure all the tasks are being done. Since this is a far-flung effort involving many different departments, consultants, and other agencies, it needs pretty tight rein. This person also must be able to diplomatically remind people who may have not followed through on assigned tasks.

CLERICAL person who is self-directed, organized and systematic to collate, copy and assemble the final document. Our SCP was two volumes.

### 2. Department Buy-In—Outreach Into the Organization

We recommend getting affected departments involved as early as possible. Our SCP started late in the game because there was trouble fixing a service start-up date. Mid-level managers, supervisors, and foremen should be given a working knowledge of what the SCP is. Over and above formal training, circulating Frequently Asked Questions (FAQs) was favorably received by staff at all levels (see Figure 3).

### 3. Letting Staff Know What Their Responsibilities Are In The SCP Process

We formed a Start-up Technical Advisory Committee (TAC), with project staff from ATCS, MMT and MMX, as well as MUNI line managers, to coordinate the start-up activities. The SCP was identified as an ATCS Project team task item that was tracked by the Start-up TAC. The TAC forum was used to educate MUNI's line managers on their responsibilities under the SCP. This forum helped change their perception that this was something being done to them, to an understanding that this was a collaborative effort. Responsibilities of line managers included: to review rules and procedures; to document training sessions; to develop and approve lesson plans; to keep detailed files, and the like. A word to the wise: When your SCP is complete, disseminate copies of the final report to TAC members, with a "Thank You" for a job well done. (Thirty copies of the two-volume final report were distributed throughout MUNI.)

## FREQUENTLY ASKED QUESTIONS ON MMX SHUTTLE SERVICE, Number 3

**Q: What are the expected benefits of ATCS?**

**Answerman:** When ATCS is fully functional, it will allow MUNI to operate more trains per hour in the subway. ("increased throughput" for your buzzword collection). This will put an END TO SCHEDULED COUPLING at the portals! ATCS trains will travel at the maximum authorized speed through the subway automatically, reducing travel time for passengers. Turnback time will be reduced from today's 3 minutes to a matter of seconds. There are many other benefits:

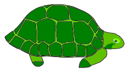
- increased safety
- centralized system overview & control
- data logging on vehicles & wayside
- new signal equipment, replacing old stuff
- new automated passenger announcements, on vehicles & at stations

**Q: Why do LRV2s have an IATP system?**

**Answerman:** MUNI extended the ATCS schedule to allow for an important upgrade of the ATCS computer systems. Without the upgrade, we would have been stuck with old time minicomputers at Central Control, which were "proven in service" as required, but very outdated. This schedule change meant that LRV2s would arrive before ATCS was ready, and could not run in the subway. What to do?

To allow LRV2s to run with the existing signal system, Alcatel designed an Interim Automatic Train Protection (IATP) system. IATP uses the ATCS Vehicle On-Board Computer (VOBC) and temporary cab-signal antennas to pickup and decode the 3 speed codes we are familiar with. Once the ATCS is fully operational in the subway, IATP will be removed.

**Q: Why does it take so long to test the ATCS?**



**Answerman:** Who remembers how long it took to debug and test our existing (simple!) cab-signal system during Metro startup? Now we are commissioning a more complex system, and have only nights available for testing. And debugging software is never easy, especially when it must be proven safe. Remember, even Windows '95 was late and it crashes at any speed!

**Q: We hear rumors that the ATCS Project is 10 years late and costs $100 million dollars. What is the truth?**

**Answerman:** The project started in August 1992, for completion in August 1995; project budget $68M = $52M Alcatel + $16M (sales tax + support + contingency). When MUNI agreed to upgrade to the new central computers (see IATP question above), the contract schedule was extended to 1997. There were more problems, and more MUNI-initiated change orders, and we extended the schedule again; currently the project budget stands at $80M: ($50.8 Alcatel + $29.2M support). Alcatel's cut actually went down, due to a reduction in fleet size. We are late, but are targeting project completion by the end of 1998.

*Figure 3*

### 4. SCP Milestones

We recommend defining a way to measure progress as it occurs throughout development of the SCP documentation. This was another shortcoming in our process. Since we started late, we were on a very tight schedule, so the final report seemed to appear out of nowhere. A better approach would be to determine intermediate milestones and acknowledge each interim accomplishment. Set a target date for SCP completion well in advance of revenue service start up. MUNI did not have that luxury and the final report was hand-carried to the CPUC a day before revenue service began.

### 5. Don't Lose Sight of Important Things

"Don't miss the tree for the forest." The SCP process requires a significant effort. After you say "Yes everything is covered in the SCP.", ask yourself, "Are the top 10 rules and procedures that affect day-to-day operation covered?" Identify the real emergency situations that are most likely to occur. Review how all new staff are prepared. (Do they have the materials, handouts, manuals on hand?). Spot checks can help with this effort. Since MUNI was new at this, our focus was too much on satisfying the oversight agency and making sure we had a complete package.

### 6. System Safety's Role

Use the System Safety unit to perform an audit function. Do this before start up if you have the time, but for sure, immediately after startup once things settle down. The auditor should check how field staff respond to:

EMERGENCY OPERATING PROCEDURES: (If Central Control asked you to activate the Emergency Fans, how you would do it?)

ABNORMAL SITUATIONS: (What do you have to do to insure safe movement of trains through this failed switch?).

We did not do such an audit, and had a couple of small incidents and minor accidents. They occurred in spite of the fact that the SCP documented the rules and procedures necessary for safe operation.

### 7. Identify Critical Rules and Procedures

This is an outgrowth of the shortcomings of number 5 and number 6. As part of the next ATCS Staged Release, a rules and procedures review committee was formed. Operations, Training, Central Control, the Rail Division Superintendent and Maintenance Representative comprise the committee, whose task is to provide the top 10 incidents for which adherence to rules and procedures is critical for safe operation. These will be reissued in a special guide, checklist, etc. and emphasized in all training given prior to the start of revenue service.

### 8. Ongoing Documentation

This is "motherhood and apple pie", but it cannot be over emphasized. Provide standard "templates" for documentation activities, to simplify the task and provide for a consistent documentation packet as the final SCP deliverable. Two areas where templates may be especially useful are review of rules and procedures and training documentation.

### 9. Safety Advisory Board and Independent Safety Consultant (ISC)

Using an Independent Safety Consultant for safety oversight on a project is new to MUNI with the ATCS project, and has proven to be a very successful innovation. The ISC has been invaluable in grounding ATCS safety assurance by providing professional and objective guidance. The ATCS ISC has been well received within MUNI, and it is expected that future projects with significant safety-critical elements will adopt the same strategy of bringing an ISC on-board.

### 10. Software Safety Verification & Validation

MUNI's business is delivering transit service, not software development. Rather than maintaining software development expertise in-house, MUNI has been well-served by including software safety verification & validation (V&V) in the ISC's scope of work. This effort has included maintaining the following documentation:

- Safety V&V Matrix: Incorporated into Alcatel's V&V Process Report (a required submittal), the V&V Matrix lists all ATCS safety requirements, their respective mitigations, and the means by which each is verified. Verification is by analysis and/or test. Tests include unit tests, engineering integration tests, system integration tests and/or field commissioning tests.
- O&SHA (Operating & Support Hazard Analysis): This analysis lists potentially hazardous operations, maintenance and test activities which are procedurally dependent. These are derived from the ATCS Technical Specification itself, design reviews, plan and program reviews, safety analyses, and tests results. Associated hazards are characterized

according to severity, probability and required mitigation. Verification is generally through design review, procedures review, and test and/or demonstration.

- Test Monitoring Plan: All tests required for commissioning the ATCS were tracked in this database. Tests to verify safety requirements or O&SHA mitigations were cross referenced. Test procedure status, including all submittals, reviews, re-submittals and approvals, was maintained and continuously updated.
- Safety Certification Specification Conformance Checklist (by BAH): Safety requirements were extracted from the Contract Technical Specifications and entered into a checklist. Each requirement was then matched with associated evidence of verification that the requirement was met, through design review, Alcatel submittal, analysis and/or test.

## CONCLUSION

MUNI successfully completed the Safety Certification Process and inaugurated a new revenue service requiring the integration of three large capital projects. In doing so, MUNI demonstrated that with proper staff, technical support from consultants, an organized approach, and a working knowledge of the SCP, success is achievable in any transit environment.

The lessons learned which are key to success are summarized below:

1. Allow sufficient time;
2. Involve staff in the process as soon as possible;
3. Prepare and follow a detailed plan;
4. Make tasks for line-staff specific, easy to understand, and easy to document;
5. Get clear expectation from oversight agency as to what they require;
6. Document relevant activities consistently and at the time they occur.

## ACKNOWLEDGMENTS

Any opinions, omissions or errors contained herein are the sole responsibility of the authors. The authors also wish to thank the following individuals, who contributed greatly to the success of ATCS Stage 1 Safety Certification: Tom Griego (BAH), Charlie Martin (L+E), Cindy Sugimoto (L+E), Steve Beebe (Virginkar & Assoc), Jim Elliston (Cornerstone Consilium), Joery Nacion (MUNI).

## TABLE 1

## MUNI ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ATCS | Advanced Train Control System |
| BAH | Booz-Allen & Hamilton (ATCS & LRV2 Engineering Consultant) |
| BART | Bay Area Rapid Transit |
| CBTC | Communications Based Train Control |
| CPUC | California Public Utilities Commission |
| FAQ | Frequently Asked Questions |
| FTA | Federal Transportation Administration |
| L+E | Lea+Elliott (ATCS Independent Safety Consultant) |
| LRV | Light Rail Vehicle |
| LRV2 | MUNI's second Light Rail Vehicle (built by Breda) |
| MMT | MUNI Metro Turnback (new subway extension, turnback tracks, & surface portal) |
| MMX | MUNI Metro Extension (new surface extension, with 4 surface platforms) |
| MUNI | San Francisco Municipal Railway |
| OJT | On-the-Job Training |
| O&SHA | Operating and Support Hazard Analysis |
| PCC | Presidential Conference Car |
| PMO | Project Management Oversight |
| SAB | Safety Advisory Board (for ATCS) |
| SCP | Safety Certification Plan |
| SFFD | San Francisco Fire Department |
| SLRV | Standard Light Rail Vehicle (built by Boeing-Vertol) |
| SSPP | System Safety Program Plan |
| TAC | Technical Advisory Committee (MUNI's start-up task force) |
| VPI | Vital Processor Interlocking (surface interlocking control, for MMX) |
| V&V | Verification & Validation |