Safety Case Management During Change

David Anderson, P.Eng.
Booz Allen Hamilton
Newark, NJ

ABSTRACT

Transit Systems require some form of certification prior to entry into passenger service, but what about after the system is in service? Systems evolve over time; change may be minor in nature, such as the upgrade of a component, or more complex, such as installation of a new line. Whenever change occurs there is a requirement to ensure that safety is maintained or improved. In addition, incidents, accidents and experiences arising from operations and maintenance need to be reviewed to ensure that any potential safety concerns are resolved. These activities should be documented in the form of a Safety Case. The maintenance of the Safety Case should include oversight by appropriate stakeholders to ensure that any change is suitable and well controlled. The Safety Case provides the burden of proof that the System is ready to carry passengers in revenue service and that its operation is safe for its workers and the public at large. This is not a one-time activity, but an on-going process critical to the operation of the System.
This paper discusses Safety Case Management in a transit setting based on the experience gained by safety practitioners, agencies and suppliers and presents an integrated approach to ensure that all changes receive the required scrutiny.

BACKGROUND

Before one can determine how a change will affect the Safety Case, the question must be asked, "What makes up a Safety Case?" When people talk about safety it is usually in context of performance in terms of accidents – the fewer accidents that have occurred, the safer it is. In actual fact, the absence of accidents does not necessarily mean the presence of safety. This approach also has a fatal flaw in that once an accident occurs, the logical conclusion is that the system is not safe; further it may never have been safe.
Safety certification is a process of identifying possible hazards and developing safeguards or mitigations, so that a mishap or accident related to the hazard does not manifest. A rigorous hazard identification process, with the development and application of mitigations for preventing injury or loss related to the hazard, generally forms the main part of any transit system Safety Case.

Addressing Hazards-Preventing Mishaps

We have identified that addressing hazards make up the bulk of a Safety Case, but how are they mitigated? MIL-STD-882, provides the following guidance on how to reduce the risk associated with a hazard:[1]

- Eliminate hazards through design selection;
- Incorporate safety devices;
- Provide warning devices; and
- Develop procedures and training.

These mitigating approaches are arranged in order of precedence. Eliminating the risk associated with a mishap is always preferable to managing the risk via a procedure. Whatever mitigation is selected to address a hazard, it is important that it can be verified. The verification usually takes the form of a record that can be documented and tracked.

Oversight by Authority

Transit Systems may be subject to oversight from federal agencies, such as the Office of Rail Regulation (ORR) in the UK or the Federal Railroad Administration (FRA) in the US. These agencies may require the Safety Case to be submitted for approval prior to revenue service. Other agencies, such as the Occupational Safety and Health Administration, may require compliance with regulations; the compliance, in the form of health and safety programs forms the verification for some mitigations. In addition, there may be a requirement for the operator to substantiate any deviation from that mandated by a regulatory body; a current safety analysis demonstrates due diligence has been performed in assessing any change that is made to a system.

Further, in the event of an audit or an accident, other agencies may review the Safety Case and conduct their own investigations. For example, the Occupational Safety and Health Administration (OSHA) govern

[1] MIL-STD-882C pp. 10.

worker's safety in the US and may investigate any accident related to worker's safety. In some cases, operational accidents may be investigated by additional bodies such as Transport Canada or the National Transportation Safety Board in the US.
The main point is that a Safety Case may be required initially, or at an unknown point in the future; and thus should be maintained so that it is current and relevant.

GUIDING DOCUMENT

The Safety Case consists of a compilation of the known/expected hazards, their mitigations, and the verification or proof that the hazard has been considered and the residual risk identified. As indicated, however, this must all be documented. The System Safety Program Plan (SSPP), defined in MIL-STD-882, guides a system's safety effort. The guidance in IEC 62278 also includes Reliability, Availability and Maintainability (RAM) in addition to Safety (RAMS); this discussion only deals peripherally with reliability, as it relates to Probabilistic Risk Assessments.
It should be noted, that some Owner/Operators are implementing a Systems Assurance Program Plan (SAPP). The main enhancement associated with the SAPP is the inclusion of Quality Assurance/Quality Control (QA/QC) with RAMS. Although not the topic of this paper, the discussion will touch briefly on the suitability of this approach.
No matter the form, Transit Systems require a Safety Case to operate. The Safety Case should satisfy the basic question as to whether or not the system is safe to carry passengers.

The System Safety Program Plan

The requirement to manage safety can be contractual or regulatory in origin; in either case, a structured process yields the best results. A Transit System should have a System Safety Program Plan that sets out the safety methodology and a Hazard Log that clearly documents the hazard analysis process. The main focus is on the areas of responsibility, expertise and authority; simply put, safety means different things to different divisions within a transit system.
All Transit Systems have four main areas to consider related to safety: design, operations, maintenance and Occupational Health and Safety (OHS). No Transit System can be considered to be safe, unless all four facets are managed throughout the system's life cycle. These distinct areas do not exist in silos, but are interrelated to such an extent that a change in one area will usually impact the others. Managing these four facets require individuals with specialized skills and qualifications to work together to integrate the Safety Case.

Design Safety

Design Safety refers to the effort required to prove the equipment meets the overall safety criteria for its application. This will usually fall under the auspices of an Engineer responsible for the design. The general consensus would be that Design Safety occurs when the system is originally installed or when a Contractor is engaged to perform an upgrade or refurbishment. In actual fact, any time a system is modified there is a requirement to review the design and ensure that the safety of the overall system is maintained or improved. This usually involves some form of probabilistic risk assessment; again the Engineer is usually the person that possesses the skills required to analyze the design. Design Safety should be managed by a qualified Engineer. The approved design documents form the verification for mitigations related to design and functionality.

Operational Safety

Operational Safety refers to ensuring that hazards related to operating the Transit System are mitigated, such that mishaps do not manifest. Traditionally, rules and procedures that ensure that the railway can be operated safely in terms of train movements, have been the main mitigating factors for dealing with hazards. Depending on the configuration of the system (manual control with traditional signaling, full Communication Based Train Control (CBTC)) the hazards associated with collision, derailment and overspeed can be mitigated by design. Operations also deal with events related to malfunction or failure, at which point procedures must be used. Most system personnel will be affected to varying degrees by Operational Safety. Operational Safety procedures should include, but not be limited to:

- Rule Book;
- Central Control Manual;
- Field Operations Manual;
- Failure Management Plan; and
- Emergency Procedures, etc.

Operation procedures should be managed by the Operations Manager. The approved procedures will form the verification for the mitigations related to operations.
Maintenance Safety
Maintenance Safety refers not only to working safely, but also to ensuring that the repairs are performed correctly, such that in-service malfunctions do not occur. In this instance, we delineate between equipment failures that will normally occur and malfunctions caused by incorrect

maintenance. While the maintenance staff benefits directly from the imposition of a well managed Occupational Health and Safety (OHS) program, only manuals related to the equipment can ensure that the repair is performed safely and correctly.
Maintenance programs should be managed by a maintenance manager or supervisor. The approved maintenance procedures form the verification for mitigations related equipment condition and functionality.
Occupational Health and Safety
Occupational Health and Safety (OHS) refers to the programs required to address workplace safety. OHS is usually a regulatory requirement and thus may be mandatory for all industries in a given jurisdiction. Transit Systems have perhaps a more varied scope than other industries when it comes to OHS. Specifically, Transit Systems usually have dedicated maintenance activities and facilities (machine hazards), they use hazardous materials (chemical hazards), utilize high-voltage transmission (electrocution concerns) and have human interactions with the travelling public (medical, intrusions) to name few.
Maintenance and customer service personnel benefit the most from OHS programs, but they apply to everyone at the system. OHS procedures should include, but not be limited to:

- Hazard Communication(HazCom) Program;
- Bloodborne Pathogen Program;
- Confined Space Program;
- Personal Protective Equipment (PPE) Program;
- Fall Protection Program; and
- Lock-Out Tag-Out Program (LOTO), etc.

OHS programs should be managed by a qualified Health and Safety Specialist. Approved OHS programs form the verification for mitigations related to working safely.
System Safety Working Group
Given the different skills required for the various facets of safety, it is unreasonable to expect one person to possess sufficient knowledge to manage the entire safety program. Each Transit System should regularly convene a System Safety Working Group (SSWG) to maintain the lines of communications between the various safety stakeholders. The SSWG should also include personnel that are not directly involved in a particular facet, but whose responsibilities pertain to all. This is the case for quality, document control and training.

Quality Control

The requirement to test and commission equipment is usually controlled and tracked by Quality Control (QC). QC also ensures that any procured equipment, as installed or tested, complies with the respective procurement contract. QC may control the configuration management plan; any change to the system needs to be reviewed in terms of configuration management. As a result, QC should be involved in the safety process to ensure that the equipment is installed, tested and functions correctly and that any software is the correct version.
The QC department provides the test reports that act as verification for mitigations related to correct equipment functionality.

Configuration Management

Perhaps the single most important activity in maintaining the safety of a system is the task of Configuration Management. This applies to two main areas, equipment configuration and control of documentation. Equipment Configuration Management ensures that both hardware and software are correct according to the design. Document control ensures any schematic, drawing or document in use on the system is the correct version. Maintenance manuals must be maintained to prevent any inadvertent maintenance errors related to out of date instructions.
Configuration Management is the mitigation for hazards related to version and design control; the Configuration Management Plan is the verification for that mitigation.

Training

All personnel require Training in order to perform their duties correctly. In addition, there may be regulatory requirements for certification and/or recertification. A Training Department should be established to manage training programs and forecast any retraining required for certifications. The trainer is therefore able to clearly present the status of any person's qualifications, should the need arise.
The training record is the verification for the mitigation that competent personnel operate and maintain the system.
Understanding Mitigation Verification
As stated earlier, hazard mitigation cannot just be a phrase, it has to be proven. The proof has to be documented so that it can withstand scrutiny. The following are examples of verification for the safety case:

- A signed design document;
- A signed test report;
- A signed training record;
- An approved maintenance procedure;
- An approved operations procedure; and
- An OHS Program.

SAFETY CASE MANAGEMENT DURING CHANGE

The question could be asked: "What changes affect safety?" The answer is any change that is related to a hazard, whether that hazard is currently defined or new to the system. The "analyze everything" approach is frequently ineffectual and thus rarely productive. The best approach is to explore the various types of change and consider what the impact they could have on safety. The following changes are encountered in most Transit Systems:

- Hiring new personnel;
- Installation of new equipment;
- Installation of new service;
- New or change in law;
- Incidents and accidents;
- Safety observations; and
- The passage of time.

New Personnel

All systems must hire personnel, whether they are the initial cadre or as a result of attrition. The effect is the same, they must receive training in order to develop competence in the sphere of responsibility to which they are assigned. The training should include testing to prove understanding and competence. As a minimum, training should comply with any regulatory requirements. The training records should be maintained to prove when the training occurred and should be signed by the recipient and the training manager.

Hiring new personnel, especially if it is an overall augmentation to the workforce, can present additional problems. Management has the responsibility for supervision, as an increase in personnel may result in a requirement to promote more supervisors. A key component in any Safety Case is that personnel are supervised while performing their tasks. The Safety Case should be reviewed to ensure that any mitigation related to supervision is correct.
In addition to hiring personnel, systems frequently have contractors perform work on their premises. It is the responsibility of the contractor to ensure that their personnel are qualified to perform the work, but the Transit System is responsible to ensure the contractor is protected from system hazards. This may involve training, issuing personal protective equipment and supervision by Transit System personnel.

Installation of New Equipment

New equipment could be installed to address obsolescence issues or to provide a capability that did not previously exist. Depending on the type of equipment, a hazard could be mitigated by the operation or maintenance procedure. Procurement of new equipment should automatically trigger a review of the training program, to ensure that all personnel are capable to safely operate the equipment. New equipment may, however, mean new hazards and these hazards must be addressed. The type of equipment can also affect the level of effort required when updating the Safety Case. Commercial Off The Shelf (COTS) equipment or equipment procured without a contract, may come with little or no supporting Safety Case. Its integration into the system should be performed by the SSWG. The SSWG must conduct and document a hazard analysis that clearly outlines how risk is mitigated for the new equipment.
The potential impact to the OHS program needs to be considered. For example, imagine new electrical equipment, as a minimum a Lockout-Tagout procedure will be required if the equipment is to be maintained. Are there any new solvents or chemicals to be used during its servicing? If so, has the Material Safety Data Sheet (MSDS) been forwarded to the Safety Manager for review and inclusion in the Hazard Communication Program? Does the solvent require any specialized personal protective equipment? If so, does the Personal Protective Equipment Program already include the requirement or does this mean a revision to the Program?

New Service

New systems are being built and existing system are being extended. New system contracts may require the contractor to produce a Safety Case, but minor extensions may not. Further, even if a Safety Case is provided, does the new system include different operating environments, tunnels, elevated sections, or bridges? These types of changes may have far reaching impacts on operations. New operations procedures may need to be drafted, liaison with Emergency Response Agencies (ERA), to ensure that any mitigation related to emergency response is adequate, may need to be initiated.

In addition, training for emergency scenarios may need to be conducted. Joint exercises, to familiarize the ERA with the system, may be required. As a minimum the ERA needs to be briefed on the procedure to access the system and the hazards associated with it. A change to an existing system could affect the ERAs ability to perform

their duties. Consider an on-board medical emergency; the Operations Center needs to coordinate with the ERA where they need to respond. A change to the Transit system may require a new type of response for the ERA, they may need new equipment. This has to be reflected in the Safety Case.

Changes in Laws/Regulations

Changes in laws or regulations should also trigger a review of the Safety Case to ensure that mitigations are valid. A change to the health and safety regulations may mean that new types of PPE need to be procured and training on its use conducted. Federally mandated programs, such as Positive Train Control, may entail: new design, equipment, procedures, training and will result in a new baseline for the safety case.

Incidents and Accidents

Incidents and accidents may occur during the life of the System. Incidents, or near misses, are particularly important as they can often, if properly investigated, highlight problem areas and allow a system to prevent related accidents from occurring. The occurrence of an incident or accident should be investigated in a non-partisan, non-prosecutorial approach that is geared towards finding root causes rather than assigning blame. Root Cause Analyses (RCA) may result in recommendations that affect all facets of safety; the object of the investigation is to determine what could or has occurred, so that it can be remedied before it happens or happens again.

An important note on the response to incidents and accidents, passion must not be allowed to overcome good judgment. This is often easier said than done, however, when faced with scrutiny from senior management or Clients. The knee-jerk reaction is often an attempt to be seen to be decisive; it would be better to consider carefully and then take appropriate action. Beware the solution that arrives minutes after the accident report. Recommendations resulting from incidents and accidents must be capable of being implemented and must address the root cause. Solutions that entail hiring also entail training, procuring equipment such as Personal Protective Equipment , and may be long term; is there any interim risk? Further, is the solution feasible; does it create another hazard? In any case, when the RCA is finished it should be reviewed by the SSWG to ensure any safety recommendations/shortfalls are addressed.

Safety Observations

In many cases, hazards are known to individuals, in some cases well known, but appropriate action has not been taken. Maybe the hazard is not appropriately identified or raised to the correct level. In some cases however, the laissez faire attitude is "we all know it's there." This may work until a new employee arrives and isn't aware. The proper action is to identify the hazard and raise it to the Joint Health and Safety Committee. The hazard should be documented on a Hazard Observation/Identification Form. The form should include a unique identifying number, so that it can be tracked. A suitable form can be developed by the System or one can be used from a text. The form should be brought before the SSWG, so that it can be analyzed and compared to the Safety Case. If the hazard is new, or if it shows that the previous mitigating actions were ineffective, a solution must be identified and the safety case updated.

A joint health and safety committee should be established in the workplace. One of the main benefits of such a committee is that the site safety inspections can be performed more frequently. Site safety inspections are one of the most important tools in preventing workplace injuries.

The Passage of Time

One change that we all must contend with is the passage of time. As time passes, components wear out, equipment becomes obsolete and people forget. Aging equipment can exhibit new hazards that need to be addressed. Obsolescence is usually cured by replacing older equipment with newer models. If a contractor is hired to perform the refurbishment, the contract can include a Safety Case for that equipment. If system personnel perform the upgrade, the SSWG should be tasked with reviewing the existing Safety Case or development of a new one for the specific equipment. Just as new personnel require training, employees that have been on the job for a longer period of time may need their training to be refreshed.

The Safety Case should be reviewed in light of the passage of time. Particular attention should be paid to any hazard that has only procedures or training listed as mitigations. In addition, tasks that are performed infrequently may require specific task retraining to ensure that personnel and the system are suitably protected.

Identifying a Hazard

When a change has occurred it has to be reviewed in order to determine whether any new hazards have been introduced into the system. A good approach is to refer to a hazard list, such as that presented in the Hazard Analysis Guidelines.[2] The generic hazard list can greatly simplify the analysis process and shorten the review time. The important point is that there are reference material and texts that should be consulted rather than starting from scratch.

RESOURCES

System safety references are a necessity when reviewing or developing a safety case. Publications such as the Hazard Analysis Guidelines for Transit Projects, Handbook for Transit Safety and Security Certification and MIL-STD-882 are free for download off the internet. These are sufficient for most applications, but specific hazard analyses may require more in-depth guidance such as that provided in Hazard Analysis Techniques for System Safety.

SAFETY CASE REVIEW

The safety case should be reviewed on a regular basis; specific reviews should be triggered when a change occurs. There are a variety of review methods such as external audits, internal review or requesting a peer review. External audits can be arranged via a services contract with a consultant or agency. General Managers can order internal safety case reviews on a predetermined or random basis. Owners with multiple systems can have the staff of one system audit the other. The Peer Review occurs when personnel from a different operating company or location perform an independent review; these can be reciprocal in nature thereby decreasing costs.

CONCLUSION

The SSWG should coordinate with the stakeholders and responsible parties to ensure that the Safety of the System is maintained and that all changes consider the varying facets of safety. The Safety Case is not a dusty binder that sits on a manager's bookcase; it is a living process that changes with the system, and is only effective when it is properly managed, updated and followed.

[2] DOT-FTA-MA- 26-5005-00-01 Hazard Analysis Guidelines for Transit Projects pp. 27-32.

REFERENCES

Vincoli, Jeffrey W. CSP 1997 Basic Guide To System Safety, John Wiley & Sons, Inc. New York
Ericson, Clifton A. 2005 Hazard Analysis Techniques for System Safety, John Wiley & Sons, Inc. New York
MIL-STD-882C System Safety Program Requirements
IEC 62278 Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
FTA-MA-90-5006-02-01 Handbook for Transit Safety and Security Certification
DOT-FTA-MA- 26-5005-00-01 Hazard Analysis Guidelines for Transit Projects
Manual for the Development of System Safety Program Plans for Commuter Railroads – American Public Transportation Association