Systems Assurance Management in Railway through the Project Life Cycle

Vivian Papen
Sound Transit
Seattle, WA

Ronald Harvey
Sound Transit
Seattle, WA

Hamid Qaasim
Sound Transit
Seattle, WA

Peregrin Spielholz
Sound Transit
Seattle, WA

ABSTRACT

Systems assurance management is essential for transit agencies to provide safe and reliable transit systems for the public. Systems assurance management is a framework for transit agencies and their contractors to ensure systems have been designed, constructed, and operated considering all critical factors related to safety, reliability, availability, and maintainability. Multiple government railway authorities around the world have been implementing, modifying and developing systems assurance management for a number of years. Those railway authorities have identified the importance of implementing systems assurance management through the project life cycle.

Several major factors should be considered in a transit organization before effective systems assurance management can be developed and implemented: 1) A supportive transit agencies' systems safety and assurance culture, 2) Technical knowledge of systems assurance management, and 3) And an understanding of the benefits of implementing systems assurance management. This paper will discuss how system safety culture affects the implementation of systems assurance management. It will also introduce a framework that can be used for systems assurance management and discuss how effective systems assurance management results in identifying and mitigating potential risks to improving project management, engineering, and operations.

INTRODUCTION

Transit systems provide a safe, reliable, fast and convenient means for the public to travel. Safety and reliability are two of the multiple critical factors that all government railway authorities need to consider as they plan, construct and modify any transit projects. Railway authorities around the world have been implementing, and modifying their existing systems assurance management standards and guidelines to fit their particular country's environment, culture and their transit system over the years. Those systems assurance management standards and guidelines provide frameworks for implementing systems assurance through the project life cycle and provide guidance for more reliable transit systems during operations.

Several transit system Incidents have occurred in the past few years, prompting Federal and local railway authorities to review the safety and reliability of transit systems and ensure transit systems safety and reliability management is implemented in a more stringent way. Systems assurance management provides a framework for railway authorities to ensure transit systems have been designed, constructed and installed as safely and reliable as possible. In addition, railway authorities can require their contractors to follow the systems assurance management framework for a more integrated system. Successful system assurance management requires multiple departments to participate and meet regularly. For transit agencies, systems safety and assurance culture can affect how the core departments participate in the process. Within a systems safety and assurance culture, all core participating departments require an understanding of systems assurance management and how their participation can affect and benefit the transit system. When transit agencies and their departments understand the importance of system assurance management, and their roles and responsibilities, the systems safety and assurance departments within the transit agencies can develop appropriate frameworks to follow and implement within the agencies.

SYSTEMS SAFETY AND ASSURANCE CULTURE

Systems safety and assurance culture has been implemented in safety-oriented industries, such as

Aviation, Oil & Gas, and Nuclear for many years. The systems safety and assurance culture plays an important role in providing safe and reliable products and services to the customers and communities within which they operate. Agencies' systems safety and assurance cultures affect employees' approach in reacting to situations that require systems safety and assurance as the first priority.

Agencies often use "Safe", "Reliable", and "Good Quality" as keywords in their agency objectives. It is important for these organizations to have the correct culture to achieve those objectives. Systems safety and assurance culture requires everyone within the agency to participate. If any departments within an agency fail to participate, it will be difficult to implement the culture. Systems safety and assurance culture is not only one department's responsibility. In order to successfully implement systems assurance management, multiple departments must participate in the systems safety and assurance process.

Agency management teams should understand systems assurance management and define the objectives of implementing systems safety and assurance within the agency. They also need to encourage employees to communicate with the systems safety and assurance department when they identify potential hazards, operational and maintenance issues and service issues regarding their products and services. By implementing an employee award program, the management team can provide incentive for employees to identify potential hazards, operational and maintenance issues and provide recommended mitigation measures.

Many departments within agencies do not know their roles in systems safety and assurance culture. Typically, most agency employees assume that design, construction and engineering departments are the only department required to participate in systems assurance management since they believe its focus is on product design. However, other departments such as operations and maintenance, customer service, and risk management must participate in the systems assurance management process. The agency management team should work with the systems safety and assurance department to explain the roles of each department in the systems assurance management process and the importance of their participation.

For employees to understand their roles in systems assurance management, system safety and assurance training programs should be developed. The agency management team should encourage all employees to participate in the training program. At a minimum, all employees should be trained in the basic systems assurance management process. This training program can provide the knowledge to all departments about the importance of working with the system safety and assurance department. Through this training program, all departments will have basic knowledge and awareness of systems assurance management. In addition, more detailed training courses can be provided to key personnel such as risk assessors, contract developers, operations supervisors, etc., in order to understand the procedures and tools used in systems assurance management.

Communication between other departments and system safety and assurance department needs to be developed after all departments have participated in training program, and those other departments should be encouraged to communicate with system safety and assurance department regularly. Communication is a critical factor that affects the successful implementation of systems safety and assurance management. The agency management team needs to encourage all departments to have regular meetings with the systems safety and assurance department to review potential hazards, operational & maintenance issues, public concerns, etc., and support ad hoc meetings when urgent situations are discovered that require mitigation measures coordinated between departments.

With support from management and a well developed systems safety and assurance culture, systems safety and assurance can be implemented agency-wide, increasing the ability of the agency to deliver "Safe", "Reliable", and "Good Quality" products and services to the public.

UNDERSTANDING SYSTEMS ASSURANCE MANAGEMENT

Systems assurance management must be implemented from the beginning of the project life cycle to achieve the best project results. The further a project progresses, the harder it becomes to use systems assurance management tools to successfully implement critical design changes. Systems assurance management provides guidelines for the agency to manage the Reliability, Availability, Maintainability, and Safety (RAMS) of its products and services. It is important for the agency and employees to understand systems assurance management before they are implemented. In addition, systems assurance management requires

multiple departments to contribute knowledge about the project to improve or provide critical design modification.

Many products and systems are subject to regulatory oversight, and require certification processes to document Reliability, Availability, Maintainability, and Safety (RAMS). Systems assurance management helps agencies monitor product and system design to achieve RAMS targets and avoid potential hazards. Often, federal or other authorities require agencies performing systems assurance management to verify designs are safe and reliable before starting revenue service. Systems assurance management provides guidelines to implement qualitative and quantitative hazard analysis at different project phases. It also assists agencies estimate maintenance costs, levels of equipment inventory required to meet availability targets, and create operation and maintenance plans and rule books.

During the conceptual (preliminary) and final design phases, the engineering, design, operation, and maintenance departments should participate in systems assurance management to review and discuss the existing design, operational and maintenance plan and targets, operational and maintenance prerequisites, and identify potential hazards to public and staff. After designs are completed, construction management departments should notify engineering, design, operation, maintenance, and systems safety and assurance departments of design changes. If any design changes are required during the construction and Installation phase, all the departments that participated in systems assurance management during the design phases should review modified designs and identify any new potential hazards that are introduced as a result of design changes.

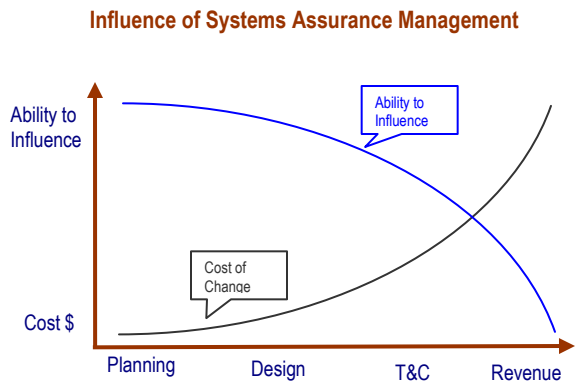
Testing and commissioning is another important project phase for systems assurance management because operational and maintenance targets are tested in this phase as products and systems operate in the designed environment. The department responsible for testing and commissioning should collect all product and system performance data and work with systems assurance management to analyze the data. In addition, monitoring of product and system performance is conducted to ensure products and systems perform as designed. If necessary, systems assurance management can perform root cause analysis to identify the cause of product and system failures that are not identified during the design phases or do not meet operational and maintenance targets. All departments that participate in systems assurance management during the design phases should review all design changes and identify any new potential hazards introduced by design changes during the testing and commissioning Phase.

During system operations or under revenue service, systems assurance management should work with operations and maintenance departments to monitor the performance of products and systems. Operations and maintenance departments should provide operational and maintenance data to systems assurance management for analysis. These analyses can help to prevent any unpredictable hazards or failure of products and systems, and ensure products and systems meet reliability, availability, and maintainability targets predicted during the design phase of the project life cycle. In addition, if any incidents occur during operations, operation and maintenance departments should work closely with engineering, design and systems safety and assurance departments to perform safety analysis and identify the cause of the incidents and any required design modification.

Systems assurance management assists the agency to assure the products and services provided to the public are safe and reliable as designed. In addition, it helps to ensure service is on time as scheduled and products and systems are easy to maintain.

EFFECT AND BENEFIT OF IMPLEMENTING SYSTEMS ASSURANCE MANAGEMENT

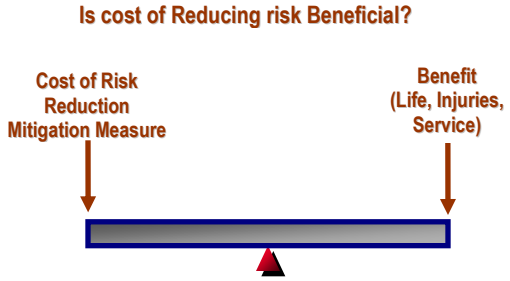
Transit agency reputations depend upon on-time service and safe and reliable products and systems. Systems assurance management assists agency to achieve product and service performance levels that are important to an expected by stakeholders and the public. At the same time, systems assurance management facilitates better financial planning for products and system design, system maintenance, system operations and helps reducing the cost of design changes when utilized at the beginning of the project life cycle.



During the design phase, hazard and risk analysis is performed in collaboration with the design and engineering department. Generic hazardous events are considered during preliminary hazard identification process to determine whether the design has included all necessary mitigation measures to avoid the hazardous events and minimize the risk. At the same time, the operations department can provide operational targets to the systems safety and assurance department and design and engineering department, so the design can be reviewed to determine whether the existing design can achieve the operational targets or whether additional facilities are needed to provide better service.

During the final design phase, systems assurance management tools such as analysis of the Mean Time Between Failure (MTBF) and the Mean Time to Repair (MTTR) of components and systems can assists design and engineering department determine which designs, and components (Lowest Replacement Unit) provide more reliable and available service to the public.. In addition, with MTBF data, the frequency of generic hazardous events can be predicted by Quantitative Risk Assessment (QRA). The risk management department can then use the data from QRA to assess agency risk and provide design and engineering whether or not design changes are required from a corporate risk standpoint. System safety and assurance department can also utilize the MTBF and MTTR summary data to propose improvement to maintenance plans for the products and services.

Design changes or modifications may be required during any project phase for a variety of reasons. Analysis methodologies in systems assurance management can help design engineers determine which design changes or design modifications are appropriate for given situations. The systems assurance management process identifies potential hazards introduced by specific design changes. If multiple design options are available, the systems assurance management process can identify potential hazards of each design option, provide risk ranking to each hazard, and control each risk accordingly. If the risk rankings for alternative designs are similar, cost/benefit analysis can be performed to identify implementation costs for each design modification and compare the risks and benefits introduced by each design modification. This helps the agency decide which design is more cost-effective and/or less risky to the agency. Moreover, Cost/benefit analysis can be performed to compare the mitigation measure implementation costs with the associated benefits to the systems.

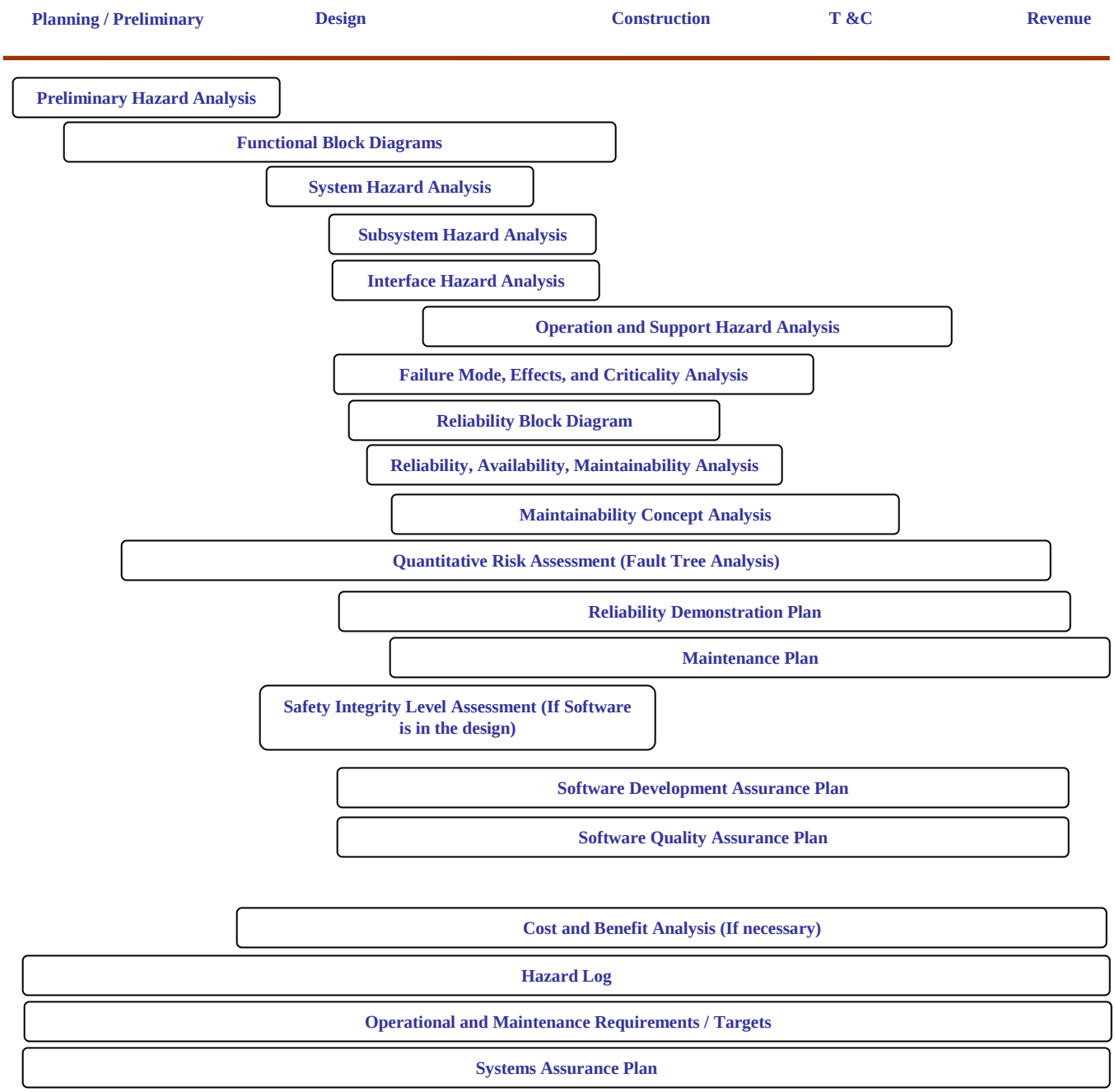


As systems assurance management requires different departments and disciplines to participate, it leads to designing of more user-friendly products and systems for operations and maintenance. Operations and maintenance departments can review the designs with design and engineering departments to optimize operations and maintenance performance by identifying associated needs and requirements.

Operations can review the human-machine interface design to improve usability, and maintenance personnel can review the design for such items as easy to access Lowest Replacement Units, diagnostics and identification of the root causes of the failures and reduction of time to perform maintenance on the systems.

Systems assurance management facilitates an agency's ability to monitor system or product design, and identify potential risks to the agency and public before the design is finalized, saving later costs due to design errors. In addition, it can help an agency align the operation and maintenance plan with the operation and maintenance budget.

RECOMMENDED SYSTEMS ASSURANCE MANAGEMENT FRAMEWORK



CONCLUSION

Providing safe and reliable transit service to the public is a priority. Systems assurance management can assist organizations achieve this objective. Systems assurance management is a, proactive process that minimizes the probability of hazardous events before they occur. All departments need to take into consideration the disastrous potential without the proper and necessary systems assurance management. The time, effort and expense to implement systems assurance management is small compared to that which is required to prepare, design, and construct a transit system. It takes considerable discussion and collaboration with multiple disciplines, and detailed systems assurance analyses to predict, prevent, and mitigate potential hazardous events. When a well developed system safety and assurance culture is implemented, all departments within the agency are motivated to understand and participate in systems assurance management. As a result, the agency vastly improves its ability to design, construct and operate a safe and reliable state-of-the-art transit system.

REFERENCE

Engineering Safety Management (The Yellow Book), Rail Safety and Standards Board on behalf of the UK Rail industry, 2007

EN 50126 / IEC 62278 – Railway applications – The Specification and Demonstration of Reliability, availability, Maintainability and Safety (RAMS), International Electrotechnical Commission, 2002

EN 50128 / IEC 62279 – Railway applications – Communications, signaling and processing systems - Software for railway control and protection systems, International Electrotechnical Commission, 2002

Hazard analysis Guidelines for Transit Project, U.S Department of Transportation – Federal Transit administration, January 2000

IEC 61508 – Functional Safety of electrical / electronic / programmable electronic safety-related systems, International Electrotechnical Commission, 2000

Manual for the Development of System Safety Program Plans for Commuter RailRoads, American Public Transportation Association – Commuter Rail Safety Management Program, 2006

MIL-STD-882C – Military Standard System Safety Program Requirements, 1993