PROVIDING FOR SAFETY IN RAIL MEGAPROJECTS

This article explores how to address safety as railway programs become increasingly complex.

The safety of workers, the public, passengers and lineside neighbours is at the heart of every decision taken during the lifecycles of rail projects. The increasing complexity of these projects necessitates a systems integration (SI) approach to properly address both the technical and human factors that affect safety.

To achieve optimal safety of the whole operating system, SI identifies the safety requirements at every level of a project and at each step, starting from initial design to delivery and maintenance. SI also considers the factors that advance or potentially weaken the safety of the whole operating system.

Relationship Between Humans and Machines

The safety risk associated with technical, operational and organizational change projects currently underway worldwide are controlled through risk management frameworks. But railway system technology continues to change at an accelerating pace, introducing unknowns and creating new risks for both the projects as well as the operating rail system. The use of new technology and processes to support safety-critical functions in megaprojects can give rise to new types of machine failures and human errors.

On top of that, the operation of each system can involve different types of complexity that can leave program leaders with an incomplete understanding regarding the potential behaviour of that system. Complicating matters further, as digital technology and software are widely used, humans and automated devices are increasingly sharing control of railway systems, and the relationship between humans and machines is becoming more complex. New distributions of human errors are appearing, and new factors are emerging that may lead to railway system accidents.

Museum Station, Australia

Holistic Versus Siloed Approach

In complex systems, safety and reliability are two different properties. Accidents often result from interactions among components; though each component satisfies its unique requirements, the system turns out to be unsafe. The Mars Polar Lander loss, for instance, resulted from failure of component interaction.

High reliability does not translate into safe operation of rail systems. In fact, reliability is not necessary for safety. Building safer systems requires going beyond the usual focus on the reliability of components to focus on whole system hazards and eliminating or reducing their occurrence.

Current regulations have served as guides for the provision of safety in project delivery, though review of regulatory language points to the growing need for a new way of thinking about safety in rail system megaprojects.

The Common Safety Method for Risk Evaluation and Assessment (CSM-RA) is a European Union (EU) regulation introduced by the European Commission to provide a common process for risk analysis and evaluation across the EU member states. The CSM-RA process is "considered complete when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered."[1]

Today's large-scale projects are building toward the next-generation digital railway—the transformation of the rail network where cutting-edge technology and systems support safety-critical functions such as control, command and signalling. As we continue to deliver megaprojects similar to Crossrail and HS2 in the United Kingdom (UK), for example, and strive to realize the vision of a digital railway, two crucial questions arise:

> *How can we be confident that we understand what our safety requirements should be? Are we really sure that all reasonably foreseeable hazards have been identified?*

The Grayrigg derailment in 2007 was the most recent mainline train accident in the UK to result in a passenger fatality; the UK railway is one of the safest in Europe according to the Report on Railway Safety and Interoperability. Engineering safety management practices, as outlined in the Yellow Book published by the Rail Safety and Standards Board, have been a staple of the railway engineer's "toolbox," established long before the CSM-RA became mandatory in the UK. The tried-and-tested safety techniques described within are still used today. Globally, other industries (e.g. aviation, oil and gas) claiming strong safety records have a history of using those traditional techniques. Yet these industries are now moving toward new techniques to deal with the increasing complexity of their systems. Shouldn't the rail industry follow suit?

Exploring the Impact of Digitalization

The introduction of new technologies and digitalized (e.g. Digital Railway in the UK and European Rail Traffic Management System in Europe) solutions in railway systems has led to the increased complexity of these systems, and to the emergence of new types of unintended system performance or unpredicted system behaviour. Automation is changing the nature of roles as evidenced by train drivers, most whom have increasingly assumed supervisory responsibility; this emphasis requires a high level of attention and cognitively complex decision-making. New technologies then create new types of risk regarding machine failure and human error.

The CSM-RA is not prescriptive regarding the techniques and tools to be used. Complexity, though, does mandate that the means and methods selected should be appropriate to consider new types of errors and also adequately assess and manage the risk being introduced. Bringing systems of increasing complexity into operational use raises the question: Are the conventional tools and techniques currently relied upon in the rail industry the most appropriate for today's challenges?

Using Effective Techniques

System-Theoretic Process Analysis (STPA) is a relatively new hazard analysis technique and the only systems approach to safety that has been extensively and repeatedly tested by large companies like Boeing, Continental AG, General Motors, Fedex, and Ford.[2] STPA includes component interaction accidents and can be

[1] Official Journal of the European Union, No. 352/2009, Report EU No. 402/2013

[2] Nancy G. Leveson and John P. Thomas, STPA Handbook, March 2018

applied as a part of the CSM-RA. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed on their own. In other words, the system may consist of reliable components but the behaviour emerging from their interaction is unsafe. STPA is a proactive analysis method that analyzes the potential cause of accidents during development so that hazards can be eliminated or controlled.

STPA has earned interest from industry, government and academia. Application areas include aviation, air traffic control, medical devices, oil and gas, automotive, railways, chemicals, space, human factors, domestic robots, security, defense, and workplace safety.

Industries around the world have started to experiment with STPA, and industry standards have incorporated STPA as a safety assessment method. Here is a list of standards and guides:

- ISO/PAS 21448 for Road vehicles – *Safety of the intended functionality*[3] : STPA is used to assess the Safety Of The Intended Functionality (SOTIF) of digital systems.
- ASTM WK60748 – Standard Guide for Application of STPA to Aircraft[4]
- SAE AIR6913 – *Using STPA during Development and Safety Assessment of Civil Aircraft*[5]
- RTCA DO-356A – *Airworthiness Security Methods and Considerations* – Also, an extension of STPA, i.e. STPA-sec, was used for cybersecurity of digital systems.[6]
- SAE – *Recommended Practice for STPA in Automotive Safety Critical Systems*[7] Automotive companies that have been using STPA with support from the MIT STPA team are: GM, Nissan, Ford, Toyota, FCA, Zenuity, Mercedes-Benz, Renesas, Continental.[8]
- MIL-STD-882E *Department of Defence Standard Practice*, *System Safety* – STPA was used to assess compliance of the system with safety requirement.[9]

Research, knowledge transfer from other disciplines, and regulations will encourage the improvement of current practices and the development of new best practices.

Many evaluations and comparisons of STPA to more traditional hazard analysis methods have been done, including fault-tree analysis (FTA), failure modes and effects criticality analysis (FMECA), event tree analysis (ETA), and hazard and operability analysis (HAZOP).[10] In these evaluations, STPA found all the causal scenarios found by the more traditional analyses but it also identified many more, often software-related and non-failure scenarios. In addition, STPA turned out to be less costly in terms of time and resources than the traditional methods.

[3] "Road vehicles – Safety of the intended functionality," International Organization for Standardization, 2019

[4] New Guide for Application of Systems-Theoretic Process Analysis to Aircraft, WK60748, November 2017

[5] Using STPA During Development and Safety Assessment of Civil Aircraft," AIR6913, SAE International, January 2012

[6] Airworthiness Security Methods and Considerations, RTCA DO-356, September 2014

[7] Mark A. Vernacchia, Recommended Practice for STPA in Automotive Safety Critical Systems, March 2018

[8] John P. Thomas, MIT's STAMP Research and STPA Applications, March 2018

[9] Department of Defense, Standard Practice, "System Safety," May 2012

[10] Information about some of these were presented at past MIT STAMP/STPA workshops. Presentations can be found at http://psas.scripts.mit.edu/home/

Figure 1 shows that hazard analysis techniques, such as FMEA, FTA and HAZOP (Sections A and C), examine failure scenarios in an attempt to prevent component and functional failures. Unsafe but not unreliable scenarios (Section B) are not handled with traditional hazard analysis techniques derived from reductionism.

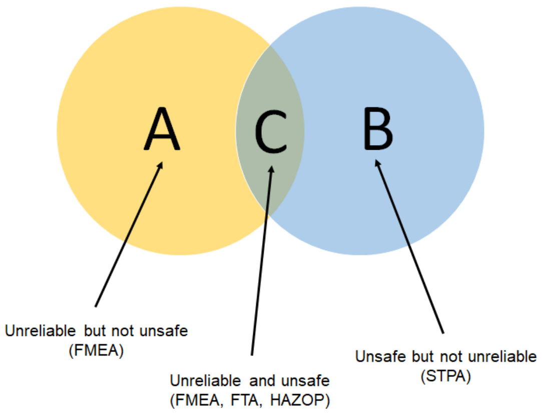
A
C
B
Unreliable but not unsafe (FMEA)
Unreliable and unsafe (FMEA, FTA, HAZOP)
Unsafe but not unreliable (STPA)

Figure 1- Safety vs. Reliability

STPA is a top-down systems engineering technique that can be used to generate high-level safety requirements and constraints. In fact, it does not generate a probability number related to a hazard, as the only way to generate such a probability of an accident for complex systems is to omit important causal factors that are not stochastic or for which probabilistic information does not exist. A typical example of such a causal factor is software failures, which are more and more common in projects involving digital technologies. Contrariwise, STPA is a rigorous technique that identifies inadequate control actions and aims to examine scenarios or paths to accidents.

STPA also considers those factors not included or poorly handled by the traditional hazard analysis methods, such as software requirements errors, component interaction accidents, complex human decision-making errors, inadequate coordination among multiple controllers, and flawed management and regulatory decision-making. Safety is thusly treated as a dynamic control problem.

The more complex the system, the more powerful STPA will be.

To get the most from STPA, we should choose systems with the following characteristics:

- Opportunity to be surprised
- Potential for unexpected behaviour or unanticipated interactions
- Systems with many interactions, where systems of positive synergies are being created
- Different decision-makers trying to work together: computers, humans, organizations, etc.

STPA considers the above-mentioned factors and can be used in a proactive way to help guide the design and system development, rather than as simply a hazard analysis technique on an existing design. STPA depends on accident causality models and functional control diagrams. Its main feature is its ability to cope with system complexity and help to identify all hazards related to software, technical components, human operators and users, and the interactions between them.

From Complex Questions to a Straightforward Solution

Projects will often use different techniques and tools to identify hazards, analyze risk and develop safety requirements. STPA can shift our attention from hardware and reliability-focused techniques to more intangible factors, such as human behaviour in complex systems, that could have an impact on the safety of the system, as accidents have shown.

Using STPA in the application of the CSM-RA, or any other safety method, can form a powerful process of safety assessment, bring value for money through efficient use of time and resources, promote a systems-thinking approach to safety in the rail sector, and help answer two crucial questions: *How can we be confident that we understand what our safety requirements should be? Are we really sure that all reasonably foreseeable hazards have been identified?*

WSP's SI:D^3 embeds safety in the DNA of each program by applying cutting-edge engineering practices and techniques to bring about positive synergy between the increasingly complex individual parts of rail system projects.

To put safety into a wider perspective, by improving the way we provide for safety in rail megaprojects, we can partially answer the big question: How do we improve project and program delivery? It is not a sustainable solution to keep applying traditional safety techniques to new software-intensive systems where engineers must—in addition to focusing on technical issues—consider the social, managerial, and even political factors that impact safety. The solution lies in adopting or creating systems approaches to safety and risk management based on modern systems thinking and systems theory.

Authors

Dr. Mikela Chatzimichailidou
Systems Assurance Engineer,
United Kingdom
Mikela.Chatzimichailidou@wsp.com

Ross Dunsford
Systems Assurance Engineer,
United Kingdom
Ross.Dunsford@wsp.com

About WSP

As one of the world's leading professional services firms, WSP provides engineering and design services to clients in the Transportation & Infrastructure, Property & Buildings, Environment, Power & Energy, Resources and Industry sectors, as well as offering strategic advisory services. Our experts include engineers, advisors, technicians, scientists, architects, planners, surveyors and environmental specialists, as well as other design, program and construction management professionals. With approximately 49,000 talented people globally, we are uniquely positioned to deliver successful and sustainable projects, wherever our clients need us. wsp.com