ABSTRACT

Transit systems require a safety case to operate; this is true for both Greenfield and Brownfield systems. These safety cases should be based upon, or supported by, a properly executed hazard analysis. Hazard analysis, however, is not a single activity but a series of analyses each of which fulfill a specific role in the overall safety process. These analyses need to address design, operations and occupational health and safety issues. Common problems with hazard analyses relate to unclear hazard definition, poor integration, incomplete mitigations/controls and a lack of associated verifications. This is further complicated by the frequent misapplication of the various types of analyses and unclear expectations as to what information the hazard analysis should contain. As a minimum, the hazard analyses should identify the hazard, its cause, its effect, recommended controls, verification of controls and an estimate of its associated risk. Properly performed, the analyses provide not only an understanding of the hazards associated with the system's design and operation, but they also identify the controls necessary to ensure safety is maintained. This paper presents a post mortem of recent hazard analyses for a North American transit system and provides examples of common issues that should be avoided. A simple framework for conducting a hazard analysis shall be provided and an explanation of the process in a transit setting shall be presented.

INTRODUCTION

Safety on a transit system project is managed through the creation of a System Safety Program Plan (SSPP) [7]. The SSPP provides the framework to prove the system is safe prior to it being certified for revenue service. This is true for a new system or major upgrades such as fleet procurement, addition of a new line or construction of a new station. The activity that forms the basis for the safety case is the hazard analysis. The hazard analysis is provided to the Authority Having Jurisdiction (AHJ) who determines whether the risk associated with the project is at an acceptable level. The AHJ may be a regulatory body, an oversight committee or an owner.

Despite the importance of the hazard analysis activity, it is usually one of the poorest performed activities. The following are some of the main shortcomings of many hazard analyses:

- Misapplication of analyses;
- Unclear hazard definition;
- Poor risk assessment;
- Scarcity of data;
- Confusing hazards with mitigations;
- Inadequate mitigations;
- Missing verifications;
- Inadequate/missing mitigations;
- Incorrect usage of reliability analyses, and
- Unrealistic probability targets.

ABBREVIATIONS AND ACRONYMS

When used in this paper the abbreviations and acronyms have the following meaning:

- AHJ Authority Having Jurisdiction
- CA Criticality Analysis
- CIL Certifiable Items List
- FMEA Failure Mode Effects Analysis
- FMECA Failure Mode, Effects and Criticality Analysis
- FTA Fault Tree Analysis
- LOTO Lock-Out/Tag-Out
- O&SHA Operating and Support Hazard Analysis
- OHS Occupational Health and Safety
- IHA Interface Hazard Analysis
- MSDS Material Safety Data Sheets
- PHA Preliminary Hazard Analysis
- PHL Preliminary Hazard List
- SHA System Hazard Analysis
- SSHA Subsystem Hazard Analysis
DEFINITIONS

One of the first problems that a safety person encounters is that the terms used in the field are not universally defined or agreed upon. The following terms shall be used throughout the discussion and shall have the meaning presented hereunder:

Brownfield – An established system.
Fail safe - A design feature that ensures that the system remains safe or in the event of a failure will cause the system to revert to a state which will not cause a mishap.
Greenfield – A new system (where none previously existed).
Hazard - A condition that is prerequisite to a mishap.
Hazard Log – A repository for hazards identified on the project.
Hazard probability - The aggregate probability of occurrence of the individual events that create a specific hazard – Frequency.
Hazard severity - An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.
Mishap - An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment - Accident.
Mitigation – Measures taken to reduce adverse impacts on the environment or workplace [2, 6].
Risk - An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability.
Safety critical - (A) A term applied to a system or function, the correct performance of which is critical to safety of personnel and/or equipment.
(B) A term applied to a system or function, the incorrect performance of which may result in a hazard.
NOTE - Vital functions are a subset of safety-critical functions [8].
Single failure point - The failure of an item which would result in failure of the system and is not compensated for by redundancy or alternative operational procedure [9].
System safety manager (SSM) - A person responsible to program management for setting up and managing the system safety program.

NOTE - for the purposes of this paper the SSM refers to the person responsible for the development of the safety case for certification (typically the contractor).
Vital function - A function in a safety critical system that is required to be implemented in a fail-safe manner.

MISAPPLICATION OF ANALYSES

The hazard analysis activity encompasses several related analyses that cover a wide range of data that progress from the general to the specific depending on the phase of the project for which it is intended. These analyses have different purposes and should not be used interchangeably. Once identified the hazards should be entered into a hazard log so that they can be tracked and updated.

The following types of hazard analysis should be used on transit projects:
• Preliminary Hazard List;
• Preliminary Hazard Analysis;
• Subsystem Hazard Analysis;
• System Hazard Analysis, and
• Operating and Support Hazard Analysis.

It should be noted that the hazard analyses are designed to represent the risks associated with revenue operation, as this is the goal of the project certification. Installation and Testing and Commissioning are not dealt with in this paper.

Preliminary Hazard List

The first step in the hazard analysis process is to develop a Preliminary Hazard List (PHL). The PHL should present the hazards that exist on the project. The System Safety Manager (SSM) is responsible for creating the PHL based upon the technology (train, track, electrification, etc.) as well as the type of operation (Elevated, grade separated, streetcar, etc.) that will form the project. Checklists are available to assist in the generation of a PHL [1, 3].

PHL – Common Issues

Frequently a PHL is not developed and thus little direction is provided to the subcontractors. This can result in significant confusion, as subcontractors are unable to meet the SSM’s expectations or they are required to perform integration without sufficient perspective.
PLH – Recommended Approach

The Preliminary Hazard Analysis (PHA) is one of two analyses, the other being the Operating and Support Hazard Analysis (O&SHA), required by most contracts. The PHA builds on PHL by providing common hazards related to the overall project. The PHA should be produced by the SSM and should contain hazards that relate to general system configuration. This is a good venue for presenting Occupational Health and Safety (OHS) hazards (electrocution, hazardous materials, fall hazards, etc.), and operational hazards (collisions, derailments, incursions into work zones).

PHA – Common Issues

Frequently the PHA is a subcontractor deliverable. If a subcontractor is required to produce a PHA, there will be substantial duplication in the hazard log.

PHA – Recommended Approach

The PHA should be produced by the SSM and present the general hazards that apply to most equipment and subsystems. The PHA should be produced early in the project and can be used to as a check to verify if guidance documents (OHS, operating procedures) are available or need to be created.

Subsystem Hazard Analysis

The next step in the hazard analyses process is the Subsystem Hazard Analysis (SSHA). The SSHA is the subcontractor’s analysis that presents the hazards related to their scope of supply. The SSM should review each subcontractor’s SSHA and provide integration by ensuring all relevant design features of the overall system and the system operating, maintenance and safety procedures are referenced, where appropriate, as mitigation.

Subsystem Hazard Analysis – Common Issues

The SSHA is sometimes treated as an over the wall analysis, it is the subcontractor’s document and it is not scrutinized by the SSM. This means that there may be little in the way of integration of the subcontractor hazards into the overall system. In most cases, the subcontractor lacks the ‘big picture’ needed to ensure that the SSHA properly reflects how the system is operated. Consider an HVAC supplier’s SSHA, the supplier is not aware of the Owners operating procedures hence he/she is not able to integrate these hazards into the system. If the HVACs are linked to the smoke detection capabilities, the failure of the HVAC may lead to an impairment of the vehicle and be cause for removal from service.

Another problem with SSHAs is that each subcontractor identifies PHA style hazards in the SSHA. For instance, most subcontractors’ analyses include hazards related to: sharp edges, heavy lifting, falls, electric shock, etc. These hazards are not specific to their product and do little to improve the safety case. The SSM should cross reference these hazards to the PHA hazards to prevent duplication.

SSHA – Recommended Approach

It would be impractical for each subcontractor to be provided with the system operating and OHS procedures. In most cases they would not know how the procedures applied to their product. The SSM, during the review of the SSHAs, should integrate the subsystem hazards into the hazard log by entering the system level mitigations. Identical hazards should be cross referenced to prevent duplication.

System Hazard Analysis

The System Hazard Analysis (SHA) provides the linkage between the various subsystems and is often referred to as an Interface Hazard Analysis (IHA). As an example, a brake supplier will understand the hazards associated with its product, but may not know how the track work on the project is configured and how the train will be operated on the system. The SSM should review each SSHA and ensure that any hazards arising from the subsystems interaction are identified.

SHA – Common Issues

The main issue with the SHA is that it is sometimes not performed. The lack of an SHA means that hazards at the interface of subsystems can go unidentified. When it is performed, it is often assigned to the subcontractor who does not possess the perspective to perform the analyses.

SHA – Recommended Approach

The SSM is the only one who can review the various subsystem analyses and ensure that interface hazards are identified. The SSM should provide the integration of the hazard analyses by producing the SHA.
Operating and Support Hazard Analysis

The Operating and Support Hazard Analysis (O&SHA) is one of the most important, yet least understood of the hazard analyses. The O&SHA’s main purpose is to ensure that operations and maintenance procedures do not introduce hazards into the system when they are used [1, 8]. Since the O&SHA is performed on the procedures it is necessarily performed later in the project than the other analyses.

O&SHA – Common Issues

The O&SHA is sometimes performed with a view to how many ways a person can injure themselves in maintenance. Most hazards related to maintenance are mitigated through OHS procedures that are mandated by regulation. In simple terms, if a person is injured because a procedure lacks a warning or its steps are out of sequence then it is a valid O&SHA hazard whose resolution is accomplished by editing the procedure.

Another issue is that the O&SHA is often confused with human factors engineering, a design activity that tries to prevent human errors through designing for the human machine interface [10]. This is understandable in that some guidelines emphasize the requirement to examine acts of omission and commission as well as human errors [3]. This preceding approach is difficult as the number of permutations would quickly become unmanageable.

O&SHA – Recommended Approach

During most projects there will be a period of manufacture, installation or testing and commissioning. During these periods the assembly of the equipment should be monitored to verify that the manuals provide proper instructions. Any procedures that are found to be incorrect or missing a safety warning should have an O&SHA hazard created and analyzed as discussed below. The mitigation would be that the procedure was adjusted or warnings placed in the instructions.

HAZARD DEFINITION

Now that the various types of hazard analyses have been presented, it is time to discuss how a hazard should be written. In order to control a hazard it needs to be defined so that it can be understood. Standards and guidelines present diverse templates with many suitable fields, but they usually recommend two text fields to describe the hazard.

Hazard Description

The goal of the hazard description is to clearly explain the hazard so that mitigations can be instituted to prevent or lessen their impact. Many analyses use only two fields to state the hazard. If we consider that any mishap is likely to have several contributors and the correct identification of them will permit action to be taken to prevent or eliminate the hazard, then perhaps it would be reasonable to populate more than two fields to increase clarity.

The following fields are recommended for hazard identification and description:
- Description;
- Condition or cause;
- Mishap, and
- Effect.

Description

The description should be a one word explanation that describes what could happen (collision, derailment, fire etc.). The hazard descriptions should be drawn from the PHL.

Description - Common Issues

In many instances, hazards are identified in terms of a loss of equipment function. A hazard analysis is not concerned with the equipment ceasing to function, but is concerned with what happens when the equipment ceases to function. Consider the loss of a pump, in reality it is what occurs when the pump stops working that is of interest (does something flood, overheat?). In other instances multiple events are listed in the same hazard description (for example: head-on, rear-end, sideswipe collisions, and derailment). Clearly these hazards occur differently and their amalgamation prohibits clarity.

Another issue related to hazard description is the practice of subdividing hazards. For instance, adding qualifying terms to hazards is not recommended (i.e. minor electrocution, small fire, etc.). This practice adds ambiguity to the process and is not beneficial.

Description – Recommended Solutions

Complicated explanations of functionality should be avoided. The description should be one or two words, it should directly relate to the effect (consider electric shock for a severe injury vs. electrocution for a fatality).

Condition or Cause

This field should clearly indicate what contributed to the hazard and this should be accomplished through a short textual explanation. This field explains what causes the hazard or what hazardous condition exists (maintainer failed to Lock-Out/Tag-Out (LOTO) equipment and it was energized while it was being maintained).
**Condition or Cause - Common Issues**

The difference between a condition and a cause is not well understood. A condition exists; it does not necessarily require anything to precipitate it. For example, a fall hazard exists due to working at height. Contrast this with an electrocution hazard in maintenance that would be caused by a failure to de-energize equipment.

**Condition or Cause – Recommended Solutions**

There should be a clear link between the hazard and its condition/cause.

**Mishap**

This field states how the accident actually happened; this may require a sentence to describe (train traversed a misaligned switch, technician contacted live electrical equipment, etc.).

**Mishap - Common Issues**

The issue that is most commonly observed with identifying the mishap is that it becomes a technical explanation that does not explain the accident.

**Mishap – Recommended Solutions**

Simply state what happened to the person or equipment involved in the accident. There is no need to explain what caused the mishap; this is covered by the condition/cause field. Consider stating a mishap as follows: Worker contacted live circuit, passenger fell striking stanchion, etc.

**Effect**

What resulted from the mishap; a credible outcome of the hazard manifesting. It is recommended that this field directly reflect the severity categories (death, severe injury, major damage, etc.).

**Effect - Common Issues**

The issue that is most commonly observed with the hazard effect is the aggregation of effects, (for example death, major injury, injury). Clearly of the three effects listed, death would effectively supersede the other types.

**Effect – Recommended Solutions**

The hazard effect should be expressed in terms of the severity categories identified in the SSPP. The advantage of describing the effect in terms of the severity is that they are simple, well known concepts that are easily understood.

---

**RISK ASSESSMENT**

A critical component of a hazard analysis is the risk assessment. The goal of this portion of the analysis is to provide a means of ranking hazards so that critical issues can be identified and tracked to closure. The two elements of the hazard that must be identified in the risk assessment are the severity of the potential mishap and the probability with which the hazard may manifest.

**Hazard Severity**

There are a variety of scales used to categorize severity, but a I-IV ranking is commonly used, see Table I. The identification of what effects relate to which severity can be problematic. In general, three types of effects are considered:

- Injury to people;
- Damage to equipment, and
- Impact on the environment.

NOTE: In some cases occupational illness has been added, but these are often long term effects that may not be easy to detect or quantify.

<table>
<thead>
<tr>
<th>Description</th>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>I</td>
<td>Fatality, system loss or severe environmental damage.</td>
</tr>
<tr>
<td>Critical</td>
<td>II</td>
<td>Severe injury, severe occupational illness, major system or environmental damage.</td>
</tr>
<tr>
<td>Marginal</td>
<td>III</td>
<td>Minor injury, minor occupational illness, minor system or environmental damage.</td>
</tr>
<tr>
<td>Negligible</td>
<td>IV</td>
<td>Less than minor injury, occupational illness, or less than system or environmental damage.</td>
</tr>
</tbody>
</table>

*Table 1 - Severity Description*

**Hazard Severity – Common Issues**

The severity is an examination or expression of the worst credible effect of a hazard. For instance, assigning an electrocution hazard a II or III severity does not match the human experience. While an electric shock may result in a severity II, electrocution is always considered fatal. Some analysts believe that assigning every hazard a severity of ‘I’ means that they consider the hazards important and that they have identified the risk. In actual fact, this practice of over estimating the severity prevents a prioritization of the risk associated with the project.

Modifying the severity categories to be very specific is also problematic. Hazard analyses are very specific in nature, hence general categories are sufficient to allow the analysis to proceed.
Transit System Hazard Analyses – A Post Mortem

Hazard Frequency

Frequency is usually defined on an A-E scale as shown in Table 2. In some standards this scale is extended to A-F or further [11]. The frequency is often related to a probability range or value that the hazard will manifest. These ranges can be quite broad, but this is acceptable as the hazard process is qualitative in nature.

<table>
<thead>
<tr>
<th>Description</th>
<th>Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>A</td>
<td>Likely to occur frequently.</td>
</tr>
<tr>
<td>Probable</td>
<td>B</td>
<td>Will occur several times in the life of an item.</td>
</tr>
<tr>
<td>Occasional</td>
<td>C</td>
<td>Likely to occur some time in the life of an item.</td>
</tr>
<tr>
<td>Remote</td>
<td>D</td>
<td>Unlikely, but possible to occur in the life of an item.</td>
</tr>
<tr>
<td>Improbable</td>
<td>E</td>
<td>So unlikely, it can be assumed occurrence may not be experienced.</td>
</tr>
</tbody>
</table>

Table 2 - Frequency Description

Hazard Frequency – Common Issues

The frequency is supposed to represent how often a hazard may occur; unlike failures, whose rates are listed in industry libraries, there is usually no data on hazard frequencies. This is especially true of transit systems that may not report all incidents or hazards to a central repository.

Hazard Risk Matrix

The severity and frequency are usually combined into a hazard risk matrix, see Table 3. The risk matrix provides a quick guide for the classification of hazards into categories that relate to acceptability.

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: Catastrophic</td>
<td>I-A</td>
<td>Permitted, Owner to review</td>
</tr>
<tr>
<td>B: Critical</td>
<td>II-A</td>
<td>Permitted</td>
</tr>
<tr>
<td>C: Minor</td>
<td>III-A</td>
<td>Permitted</td>
</tr>
<tr>
<td>D: Negligible</td>
<td>IV-A</td>
<td>Permitted</td>
</tr>
<tr>
<td>E: Improbable</td>
<td>I-E</td>
<td>Are not permitted in the design/operating System</td>
</tr>
</tbody>
</table>

Table 3 - Hazard Risk Matrix

It should be noted that the hazard analyses are designed to represent the risks associated with revenue operation as this is the goal of the project certification. Installation and Testing and Commissioning are not dealt with in this paper.

Initial Vs. Final Risk

The risk assessment exercise needs to be performed twice; once to estimate the risk associated with the hazard before mitigation and another to estimate the risk after the mitigations have been identified and put in place. It should be noted that this process is generally qualitative in nature, i.e. there is no magic way of determining exactly how much of a decrease in frequency any given mitigation will provide.

SCARCITY OF DATA

A potential stumbling point related to system upgrades or new fleet procurements is the integration of a new analysis into the existing system. On a Greenfield project it is understood that the contractor is responsible for developing the safety case with little data from the Owner. On a Brownfield project there tends to be an expectation on the contractor’s part that the owner/operator will have data related to hazard occurrence probabilities. These are usually related to the human element and can include the number of slip, trips and falls, assaults, acts of vandalism, etc.

Potential Issues

Asking for hazard data seems like a reasonable request, but there are several issues with this approach. The owner/operator may not have statistics related to the hazards of interest. Requesting hazard, or accident data, is not a standard approach as it attempts to obligate the owner to provide information that is not required by the contract. The request for this type of information will create delays in the contractor submittal process; this can be contentious and lead to finger-pointing.

Recommended Approach

The contractor is responsible for their scope of supply, the certification relates to the hazards they have identified with the frequencies they have defined. With respect to a Brownfield system, the frequencies of hazards related to human activities (i.e. intrusion, assault, vandalism) should be considered to be the same on the new equipment as it is on the old. The provision of the new equipment should not change the probabilities related to the passengers or public actions. This being the case, there is no need to agonize over such data.

HAZARDS VS. MITIGATIONS

Hazards are prerequisites to mishaps while mitigations are measures that are taken to lessen the frequency of the hazard. The objective of hazard analyses is to determine what hazards are related to the system and
transit system hazard analyses – a post mortem

To try and prevent the hazard from manifesting by putting mitigations in place.

Potential Issues

Some analysts try to create hazards by stating that the non-existent of a mitigation actually is, in and of itself, a hazard. For example, if maintenance is a mitigation, then not performing maintenance must be a hazard. This seems logical, but the logic is circular in that the hazard cannot exist unless the mitigation does not and vice versa. As an example, the hazard is that the equipment failed, rather than a lack of maintenance. After all, a failure can occur whether or not maintenance is being performed and a failure may not occur even if maintenance is not performed.

Using this logic with procedures is a major problem with how the O&SHA is performed. Many O&SHA hazards state that the procedure is incorrect; the hazard should state what would happen if the procedure were followed. For example, suppose there was no instruction to de-energize equipment prior to beginning maintenance. The hazard would be electrocution (not incorrect procedure) and the cause would be failure to de-energize equipment. The mitigation should indicate how the procedure was modified to prevent the hazard (i.e. warning added indicating electrocution hazard).

These poorly identified hazards increase the size of the hazard log, but provide no value.

MITIGATIONS

Once the hazard has been defined, mitigations must be developed to decrease the hazard frequency. It is important to note that one hazard may have many mitigations. The SSM’s job is to identify the mitigations for each hazard and to ensure that any subcontractor’s hazards have system level (integration) mitigations added.

System level mitigations would include OHS procedures, operating procedures and associated failure management procedures that the subcontractors may not be aware of.

Occupational Health and Safety

Many hazards involving maintenance personnel are mitigated by OHS procedures. The contractor should possess a working knowledge of OHS principles and provide direction as to which mitigations related to OHS is appropriate. In addition, the contractor has the obligation to instruct the Owner/Operator regarding any OHS issues that their product creates.

If a project involves provision of new equipment, the contractor is responsible for LOTO procedures for their equipment. If the project involves usage or provision of chemicals, Material Safety Data Sheets (MSDS) must be provided to the owner/operator.

Mitigations – Common Issues

There is a belief that a mitigation can change the severity of a hazard. It is not a good idea to decrease the severity of a hazard based upon a mitigation. The only time the severity of a hazard should change is when the hazard has been eliminated or a design change has been made that fundamentally changes the nature of the hazard.

Failing to identify mitigations is common, sometimes this is due to error, but in other cases it is believed that sufficient mitigations have been developed. In the latter case the identification of mitigations is viewed as a quantitative exercise, i.e. only identify the number of mitigations to make the risk acceptable. As stated earlier, hazard analysis is a qualitative exercise and there is no way of determining how much reduction in risk is related to a mitigation.

Mitigations – Recommended Approach

It is recommended that any mitigation that relates to a hazard be identified. Mitigations covering design, operations, training, testing should be referenced. Any mitigation that references a procedure needs to include a review under the O&SHA.

HAZARD VERIFICATIONS

The existence of mitigations has to be proven; this is usually accomplished by listing the documents (design, testing, and/or procedures) that verify the mitigation. Once complete this list of verifications also comprises the Certifiable Items List (CIL) [4].

Verifications – Common Issues

The recommended mitigation must be developed through reference to the verification. It is imperative that the verification (test procedure, design document, etc.) be listed with the mitigation when it is prepared so that rework is minimized. Ideally this activity will occur once the design is frozen; else the hazard may have to be revised. In addition, operational and procedural documents are often prepared late in the project so this could lead to rework.

Verification – Recommended Approach

Linking a mitigation with a verification is an important step in that it ensures that the underlying documentation has been referenced. This forces the SSM to review the documentation for the project and thereby gain increased knowledge of the system. The linkage also serves to create the Certifiable Items List
RELIABILITY ANALYSES

Reliability and safety analyses are intricately linked in the transit business. They are discussed and used interchangeably despite the fact that they have different applications and these are not always compatible. In general, reliability analyses are quantitative while safety analyses are qualitative in nature. The two reliability analyses that are usually linked to safety are the Failure Mode, Effects and Criticality Analysis (FMECA) and the Fault Tree Analysis.

Failure Mode, Effects and Criticality Analysis

The FMECA is a bottom-up analysis, which considers one failure at a time, and is composed of two distinct parts the Failure Mode Effects Analysis (FMEA) and the Criticality Analysis (CA). The FMECA is primarily a reliability analysis, but it does have application in other areas [9]. A FMECA examines one failure at a time and its purpose is to examine failure effects of equipment and identify single failure points [5]. Failures that result in catastrophic or critical effects are of particular importance.

FMECA – Common Issues

A FMECA is not a hazard analysis although it is often identified as one in contracts. In reality, very few single failures result in catastrophic or critical effects. The ones that do are usually structure related and are addressed through safety factors; it is realized that should these items fail there could be a safety impact, but this does not change how the safety is assured.

Consider the number of components that make up a modern transit system, since each item may have more than one failure mode, there would be thousands of hazards just related to failures. Properly completed, however, the FMECA does provide operational data in the form of failure management that is useful for operations.

Fault Tree Analysis

A Fault Tree Analysis (FTA) is a top-down analysis that examines an event of interest and determines what contributors need to happen for the event to occur. If the top event is identified as a hazard, say collision, the FTA can allow for a mapping of events that have to occur for the top event to manifest. The FTA allows for an event related to operational decisions to be created. It can demonstrate the chain of events or decisions that would have to occur before the event manifests.

FTA – Common Issues

The FTA requires significant knowledge of the system in order to develop the Boolean logic that is required for quantifying the analysis. This can lead to an analysis where some events are quantified while others are not. In general, once an FTA progresses past three levels, a software program is required to calculate the probabilities. These programs are expensive and require training to be used effectively.

Another problem with FTAs is that the person performing the analysis must understand what the results mean. For example, fail-safe equipment should achieve $10^8$ operating hours without a wrong side failure. If the probabilities being generated by the FTA exceed this figure, and are not of a fail-safe design, there is likely something wrong with the FTA structure (i.e. an “AND” gate was used in place of an “OR” gate).

A common mistake in FTAs is that quantities are not considered when constructing the fault tree. For example if you are trying to determine the probability of a train departing with a door open, you would need to know the failure rate for the door monitoring circuit and the number of trains. When quantity is not considered the result will be an underestimation of the risk.

Table 4 provides a quick reference as to what numbers mean in terms of probability or mean time to occurrence. The first italicized line is the usual fail-safe requirement. When a quantitative analysis is reviewed, it is a good idea to have on hand a table like this to interpret the numbers.

<table>
<thead>
<tr>
<th>n</th>
<th>$X^n$</th>
<th>Hours</th>
<th>Time/ys</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0.1</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.01</td>
<td>100</td>
<td>4 days</td>
</tr>
<tr>
<td>3</td>
<td>0.001</td>
<td>1000</td>
<td>1.5 months</td>
</tr>
<tr>
<td>4</td>
<td>0.0001</td>
<td>10000</td>
<td>1.14</td>
</tr>
<tr>
<td>5</td>
<td>0.00001</td>
<td>100000</td>
<td>11.4</td>
</tr>
<tr>
<td>6</td>
<td>0.000001</td>
<td>1000000</td>
<td>114</td>
</tr>
<tr>
<td>7</td>
<td>0.00000001</td>
<td>10000000</td>
<td>11400</td>
</tr>
<tr>
<td>8</td>
<td>0.000000001</td>
<td>1000000000</td>
<td>114000</td>
</tr>
<tr>
<td>9</td>
<td>$1E-10$</td>
<td>$1E+10$</td>
<td>$1,140,000$</td>
</tr>
<tr>
<td>10</td>
<td>$1E-11$</td>
<td>$1E+11$</td>
<td>$11,400,000$</td>
</tr>
<tr>
<td>11</td>
<td>$1E-12$</td>
<td>$1E+12$</td>
<td>$114,000,000$</td>
</tr>
<tr>
<td>12</td>
<td>$1E-13$</td>
<td>$1E+13$</td>
<td>$1.14E+09$</td>
</tr>
<tr>
<td>13</td>
<td>$1E-14$</td>
<td>$1E+14$</td>
<td>$1.14E+10$</td>
</tr>
</tbody>
</table>

Table 4 - What Numbers Mean
**FMECA/FTA – Recommended Approach**

A useful approach is to combine data from the FMECA using an FTA structure to create a quantitative hazard analysis [5]. Failure rate data used in an FTA can be cross checked against industry databases or the FMECA. This type of analysis would be difficult to perform, but it could provide insight into system hazards.

**UNREALISTIC PROBABILITY TARGETS**

Most contracts define frequency or probabilities targets related to hazards. In many cases an ‘E’ frequency is assigned a $10^{-9}$ probability of occurrence (similar to fail-safe equipment). Care should be taken, in consideration of Table 4, that the target is acceptable for the system. Consider that a system with a larger quantity of trains and passengers will accrue operating hours much quicker than a smaller system.

While the targets are usually based on operating hours they will have different practical implications. The same target on a small system might mean that a hazard happens once a year, but once a week on a larger system.

Many hazards deal with human errors, it is not realistic for a probability target for fail-safe equipment to be used as a target for human error. When dealing with hazards involving humans it is important to account for other factors such as supervision, testing and design mitigations that can lower the probability.

**CONCLUSION**

Transit systems all rely on hazard analyses to provide assurance that the system is safe. Selection of the correct analysis, coupled with clearly identifying the hazard, permits the System Safety Manager to demonstrate that the risk associated with the system is acceptable and able to be certified for revenue service. This paper has presented some simple guidelines to improve the overall quality of the hazard log.

**REFERENCES**

The following documents were referenced in the creation of this paper:


