A Structured Approach to Risk Assessment and Design Safety Analysis of Urban Maglev System

No. 8
Chinnarao Mokkapati
Ansaldo STS Union Switch & Signal, Inc., 1000 Technology Drive, Pittsburgh, PA 15219, USA
cmokkapati@switch.com

ABSTRACT: This paper presents a structured approach for quantitative risk assessment and subsequent safety analysis of the General Atomics urban maglev system that is under development. This approach, broadly based upon industry standards such as U.S. Military Standard 882C, AREMA Communications & Signals Manual Section 17, and CENELEC Norm EN50129, is applicable to any safety-critical system, and has been used specifically for signaling and train control systems.

1 INTRODUCTION

Risk assessment of a safety-critical system and the subsequent anlaysis of the system's design to verify that it meets the safety requirements derived from the risk assessment process typically consist of the following steps (U.S. DoD. 1993), (AREMA 2004), (CENELEC 2002), (CENELEC 1999), also shown in Figure 1:

1. Define the system adequately.
2. Identify key operational hazards.
3. Determine the tolerable hazard rate for each hazard by analyzing the consequences of the hazards (taking into account the operational parameters).
4. For each hazard: Analyze the causes down to a functional level taking into account the system definition and architecture.
5. Apportion the tolerable hazard rates (THRs) to various subsystems and functions. Also, translate the THRs into safety integrity levels (SILs). This step provides a detailed safety requirements specification for each subsystem and its functions.
6. Design the subsystems and the overall system with suitable techniques that help achieve the THR and SIL goals, and validate through safety analyses and testing that they meet the specified requirements.

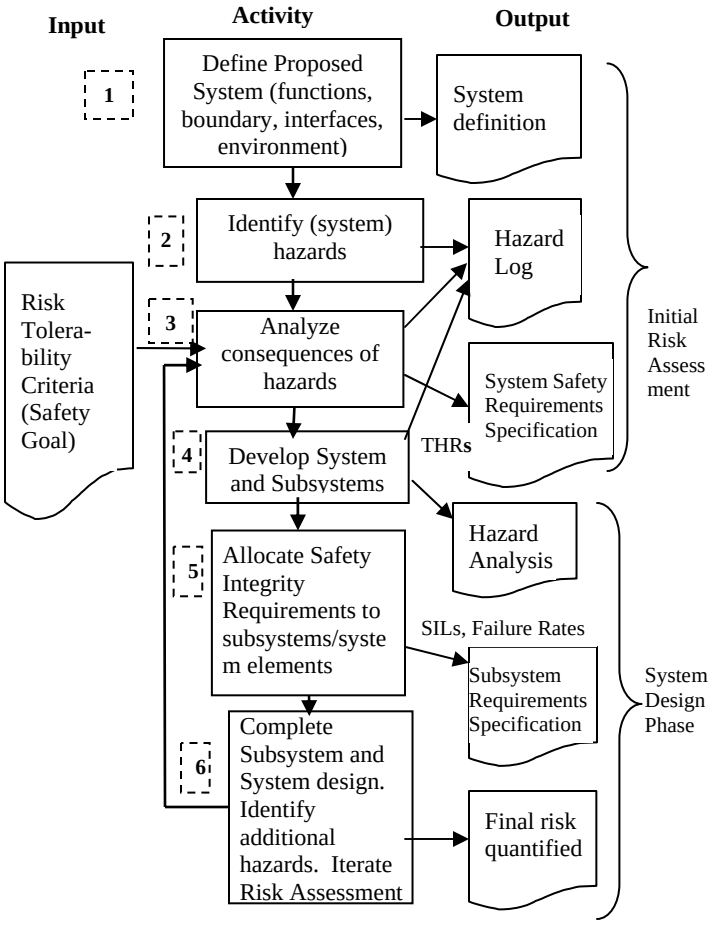

Figure 1. Risk Assessment and System Design Phases

Steps 1 through 3 are the initial risk assessment phase and the remaining steps are the system design phase. The overall effort involves an *iterative* process as shown in Figure 1. The risk assessment steps are described in Section 2, with an example application (at a high level) to the General Atomics urban maglev system. The system design safety analysis process as applied to one of the subsystems of the urban maglev system is outlined in Section 3, without going into details since these details can be found in text books on System Safety Engineering.

2 RISK ASSESSMENT

Risk assessment begins with the definition of the proposed system and identification of the hazards associated with that system, and continues throughout the design phase until the final risk associated with the system is shown to be acceptable. Each of the risk assessment steps of the proposed methodology is described in more detail below.

2.1 System Definition

The system under investigation must be defined completely. This is typically done via the following documents:

- *System Requirements Specification*, which lays out the functional, physical, and performance requirements of the system, giving consideration to the signaling principles to be satisfied and the operational parameters to be met (e.g., train schedules, speeds, traffic densities, etc.)
- *System Architecture Description*, which specifies the primary system components or subsystems and defines the interfaces between them and between the overall system and its environment
- *System Design Description*, which outlines the system design for meeting the requirements.

These documents are part of every system development process or system application.

2.2 Hazard Identification

This second step of the Risk Assessment process involves identification (and documentation in a Hazard Log) of the potential hazards associated with the intended operation of the system in its normal operating environment. This is accomplished through a structured Hazard Identification Study using techniques such as Brainstorming, HAZOPS (Hazard and Operability Study), and FMECA (Failure Modes, Effects and Criticality Analysis), as described in (AREMA 2004).

To illustrate the methodology, we will assume that there are n hazards associated with a particular system, which result from its failure modes (or those of its subsystems). Each hazard, H_j, j = 1,…., n, will have a hazard rate, HR_j, measured in failures/hour. Any of these hazards could already be present in the system when an individual starts using the system, or it could occur while the individual is using the system (examples of an individual using a railway system are a train journey, passing through a grade crossing, etc.). In either case, a hazard exposure time E_j can be defined. Thus we can express the probability that an individual using the system is exposed to hazard H_j as the term HR_j x E_j.

2.3 Identification of Accidents

Upon identification of the significant hazards, a systematic and objective Consequence and Loss Analysis is required in order to forecast safety risks, taking into account the operational environment. The aim is to systematically arrive at a THR value for each hazard. This will in turn assist with a credible determination of Safety Integrity Requirements for the system.

Each hazard may result in one or more types of accidents. For hazard H_j let there be m possible types of accidents $A_{jk,}$ k = 1,….., m. We will also define C_{jk} as the probability of occurrence of accident A_{jk}. The values of these probabilities are determined by performing an *event tree analysis* of the kinds of mishaps that can occur when a hazardous situation is encountered. Consequently, a set of accident rates, $AR_{jk,}$ associated with accident types A_{jk} can be specified as:

$$AR_{jk} = N \times (HR_j \times E_j) \times C_{jk} \quad \textit{accidents/hour} \qquad (1)$$

where N is the number of times the individual uses the system per hour; j = 1,….., n; and k = 1,……,m.

2.4 Collective Risk Estimation

In order to come up with a tolerable level of each hazard rate, the impact of all accident types that could occur due to each hazard must be determined, since a greater impact, say in terms of lives lost, will necessitate a lower tolerable hazard rate. The impact of an accident is typically specified in terms of a severity level, which is expressed in terms of an *adjusted* number of fatalities. The adjusted number of fatalities, S_{jk}, associated with accident type A_{jk} is expressed as:

S_{jk} = Actual number of fatalities + actual number of injuries converted to an equivalent number of fatalities + all financial losses converted to an equivalent number of fatalities.

In general, multiple individuals are affected by each accident, such as two crew members on a locomotive, several passengers on a train, or the occupants of a vehicle at a grade crossing. Consequently, there is a collective risk associated with every accident. If CR_{jk} is defined as the collective risk of fatality associated with accident type A_{jk}, then the set of collective risks of fatality associated with accident type A_{jk} are:

$$CR_{jk} = AR_{jk} \times S_{jk} \quad \textit{fatalities/hour} \qquad (2)$$

Each collective risk of fatality thus represents the *rate* of (adjusted) fatalities for a particular type of accident that results from the occurrence of a hazard for the system in question.

2.5 Calculation of Individual Risks

Since safety is usually expressed in terms of a Tolerable Individual Risk (TIR), the collective risks calculated in the previous step should be converted to individual risks so that they can be compared to the TIR, which represents the risk to an individual using the system of being killed because the system fails in an unsafe manner. The TIR in a transportation system is generally defined in terms of fatalities per passenger-mile, and it must be compared against all the hazards that are possible for that system.

If the system collective usage (or throughput) is PM passenger-miles per hour, then it can be seen that the individual risk of fatality, IR_{jk}, associated with accident A_{jk} is:

$$IR_{jk} = \frac{CR_{jk}}{PM} \quad \textit{fatalities/passenger-mile} \qquad (3)$$

These are the fatality rates for individuals using the system for each accident A_{jk}. In general, risks, whether collective or individual, are specified as rates.

2.6 Determination of Tolerable Hazard Rates

If the sum of the individual risks resulting from the hazards as calculated in Section 2.5 is smaller than or equal to the TIR, then the hazard rates are tolerable, and the system must be designed to meet these THRs. Also, new hazards may be found during the system design phase, in which case the risk assessment process must be repeated to obtain a new set of THRs. If realization of the final set of THRs turns out to be too costly or too demanding, then the Railway Authority may have to introduce additional procedural or physical barriers into the operation of the system, to ensure that the TIR goal is always met.

2.7 Determination of Risk Assessment Input Parameters

2.7.1 Risk Tolerability Criteria and TIR Determination

Different sources are available to determine the tolerable level of individual risk, TIR. For mass transit systems such as heavy rail/light rail metros and automated people movers, the Federal Transit Administration (FTA) may set the value of TIR. For railroads operating long-distance passenger trains and/or freight trains, the Base Case risk assessment conducted per the requirements of FRA Rule 236 Subpart H (FRA 2005) may provide the value of TIR. In Europe, the GAMAB (Globalment Au Moins Aussi Bon, which means '*globally* at least as good') principle, the ALARP (As Low As Reasonably Possible) principle, and the MEM (Minimum Endogenous Mortality) principle are used for this purpose. A report (Schäbe 2001) of the Institute for Software, Electronics, Railroad Technology, TÜV InterTraffic GmbH, provides a useful treatment of GAMAB, ALARP and MEM principles.

The GAMAB principle requires the risk of the new system to be no higher than that associated with the system being replaced. An upper and a lower bound on TIR (individual fatality rate in fatalities per year)

can be derived from the ALARP principle. And a single value for TIR can be derived from the MEM principle.

2.7.2 Estimation of C_{jk}, S_{jk} and PM

The accident probabilities C_{jk} are estimated using techniques such as Cause-Consequence Analysis conducted using the Event Tree Analysis method, supported by historical data on human reliability and effectiveness of circumstantial barriers that prevent hazards from translating into accidents.

The accident severity parameters S_{jk} can be obtained from historical data maintained by various sources such as government agencies, transit authorities and operating railroads on accidents/incidents that happened in operating scenarios similar to those in which the proposed system will be used. Caution must be used in applying or extrapolating limited historical data to future scenarios applicable to the proposed system.

The parameter PM (passenger-miles per hour) can be computed based upon the planned operation of the proposed system.

2.8 *Example Risk Assessment*

Step 1: Define the system

The urban maglev system being developed by a General Atomics (GA) Consortium (UCSD, 2008a), shown in Figure 2, is used here as an example to help clarify each of the steps involved in the risk assessment process.

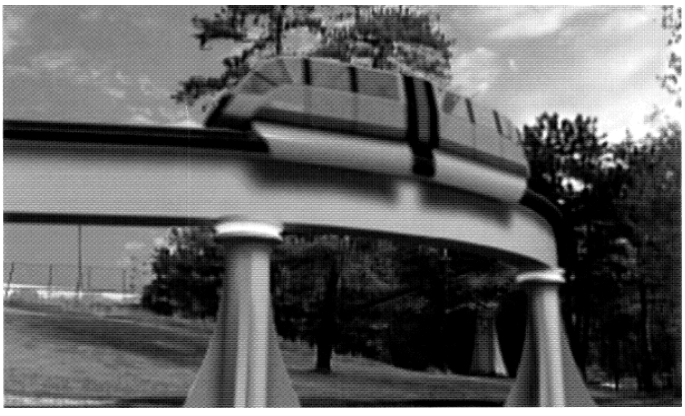

Figure 2. Envisioned GA Urban Maglev System

The urban maglev system is intended to operate magnetically-levitated trains carrying up to 100 passengers at speeds up to 50 mph, (average speed of 40 mph) in urban settings such as university campuses and downtown business districts. The system will use a passive, permanent magnet levitation method with a linear synchronous motor (LSM) powering the guideway to provide propulsion and guidance for the vehicle. The articulated vehicle (or a set of vehicles configured as a train) will be driverless and can operate in all-weather conditions, and have no on-board power electronics and control systems for levitation or propulsion. All power, control, and train protection systems will be in wayside control room(s).

The urban maglev system intends to use a communications-based automatic train control (ATC) system to ensure safe operation of the maglev vehicles. A high-level architecture of the proposed ATC system (Pascoe 2008) is shown in Figures 3(a)-(d). This system will perform the basic functions of automatic train protection (ATP), automatic train operation (ATO), and automatic train supervision (ATS), with the help of a central control office segment, vehicle-borne ATP equipment (VATP), and wayside equipment.

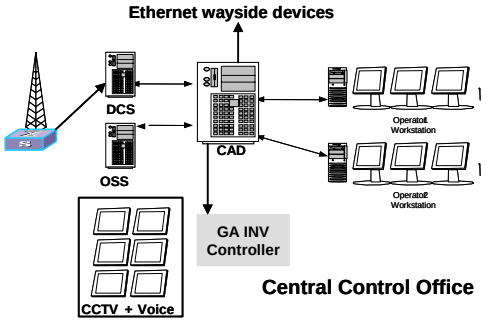

Figure 3(a). CAD, OSS and DCS at Central Control Office

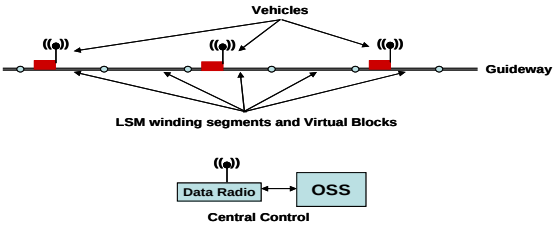

Figure 3(b). Virtual Block Control via OSS

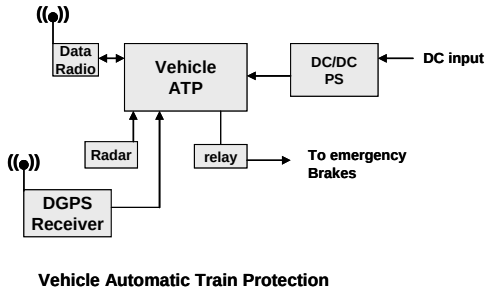

Figure 3(c). VATP and Peripheral Equipment On-board a Vehicle

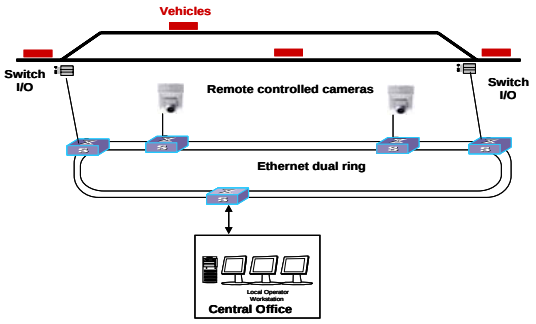

Figure 3(d). Wayside Equipment

The ATP functions are performed by the office safety server (OSS) and the VATP equipment. The VATP equipment determines the train's location on the guideway (using differential GPS and Doppler radar) and transmits the location data to the OSS. The OSS uses virtual block control principle to generate a movement authority limit (MAL) for the vehicle and communicates the MAL (via the data communication system) to the VATP. The VATP then generates a safe speed-distance profile to the end of its MAL, and calls for emergency brake (EB) application if the profile is violated. The EB application commands the applicable inverter to be shut down, resulting in safe stopping of the train.

The ATO functions of vehicle speed regulation between stations and programmed station stopping are performed by the inverter control system.

The ATS functions of automatic train routing, schedule-keeping, and headway control, are performed by the computer-aided dispatch (CAD) subsystem located at the central control office. This subsystem also performs surveillance of stations and vehicles, and voice communications between the dispatcher and passengers. In emergency situations, the CAD subsystem can initiate EB application via the OSS and the vehicle's data radio if the dispatcher determines the need to stop all vehicles in a specific area of the guideway.

The wayside equipment will consist of a dual-ring Ethernet wired network, remotely controlled cameras, and safety processors that monitor and control the guideway switches.

Step 2: Hazard Identification

By using a Hazard Identification process, let's say a set of initial hazards shown in Table 1 have been identified for the system described in Step 1.

Each hazard should be assigned an initial hazard rate for the subsequent steps of risk assessment. Also, additional data as described below are required for completing the initial risk assessment.

Table 1. Hazards in Urban Maglev System

Hazard #	Hazard Description
H1	OSS declares wrong occupancy status of virtual blocks, which results in an incorrect MAL to a vehicle, which in turn could lead to a collision
H2	VATP determines its location on the guideway incorrectly, which in turn could lead to a collision
H3	VATP fails to call for EB application when the vehicle's speed-distance profile is violated, which in turn could lead to a collision
H4	Inverter subsystem fails to shut down when commanded via the VATP, which in turn could lead to a collision
H5	Wayside safety processor indicates/communicates wrong guideway switch position, which in turn could result in collision or derailment

A report (UCSD, 2008b) on the GA urban maglev system stated the Safety Goal for the system as: < 0.1 unsafe incidents/million passenger-miles, < 0.1 injuries/100 million passenger-miles, and zero fatalities.

Though the goal of zero fatalities may be unrealistic, the stated goals of unsafe incidents and injuries can be converted into a single goal in terms of a limit on an adjusted number of fatalities per passenger-mile. Assuming that 10 unsafe incidents equate to 1 fatality and 5 injuries equate to 1 fatality, the Safety Goal can be stated as ≤1.02 fatalities per 100 million passenger-miles. This can be considered as the TIR for the system.

Also, from the design and operational data for the proposed system, let's assume that:

- N = Number of times an individual uses the maglev train = 2 per hour (typical usage by a student in a university campus);
- Exposure time to any hazard in the system = average duration of each trip = 6 minutes;
- PM = System usage or throughput = 1,150 passenger-miles per hour, based upon an average number of 50 passengers in each 2.3-mile trip, at 10 trips/hour;
- Guideway Cost = $40 M/mile; and
- Maglev Vehicle Cost = $3 M each.

Step 3: Consequences Determination

In general, in the event of a wrong-side equipment failure in one part of a system that remains undetected or non-negated (reflected as the hazard rate that needs to be quantified), the consequences (incidents/accidents) depend upon how the other parts of the system, including any humans involved, react to such failure. The system design features and human actions provide physical, procedural, or circumstantial barriers that prevent the hazards from translating into incidents/accidents, most of the time. It's the failure of these barriers that results in incidents/accidents. The probabilities of such failure are to be used in the quantitative derivation of the final outcomes of hazards.

However, as a simple and conservative cause-consequence analysis of the example urban maglev system, assume that each of the hazards listed in Table 1 could result in a collision at ≥40 mph with a probability of 0.1 and an adjusted number of fatalities of 60, or a collision at <40 mph with a probability of 0.9 and an adjusted number of fatalities of 20.

Using the above information, the Individual Risk values shown in Table 2 are obtained.

Table 2. Individual Risks Associated with Hazards

Hazard	Initial Hazard Rate (Failures per hour)	Possible Consequences	Individual Risk (Fatalities per 100 million passenger miles)
H_1	10^{-7}	A_{11} = Collision at ≥40 mph	IR_{11} = 0.01
		A_{12} = Collision at <40 mph	IR_{12} = 0.03
H_2	10^{-6}	A_{21} = Collision at ≥40 mph	IR_{21} = 0.1
		A_{22} = Collision at <40 mph	IR_{22} = 0.3
H_3	10^{-7}	A_{31}= Collision at ≥40 mph	IR_{31} = 0.01
		A_{32}= Collision at <40 mph	IR_{32}= 0.03
H_4	10^{-7}	A_{41} = Collision at ≥40 mph	IR_{41} = 0.01
		A_{42} = Collision at <40 mph	IR_{42}= 0.03
H_5	10^{-6}	A_{51} = Collision at ≥40 mph	IR_{51} = 0.1
		A_{52} = Collision at <40 mph	IR_{52} = 0.3
		Sum of Individual Risks =	0.92

From Table 2, it can be seen that the sum of Individual Risks from all accidents is below the Safety Goal. Hence, the hazard rates shown in the second column of the Table are a set of tolerable hazard rates. The supplier of the system should design the system to meet these THRs, if it can be done at a reasonable cost. An iterative process needs to be employed to determine the THRs if the Safety Goal is not met on the initial round, or if additional hazards are found during the design of the system.

If it turns out that the system design is too expensive to meet the THRs, some of hazard rates may be re-evaluated and additional procedural barriers may be placed by the Owner of the system.

3 SYSTEM DESIGN SAFETY ANALYSIS

Safety analysis process (CENELEC 2002) (CENELEC 2001) typically used during the system design phase (steps 4 through 6 in Figure 1) is outlined in Figure 4. It essentially consists of developing the architecture of each subsystem that can be used to satisfy the THRs, apportioning the THRs to various functions of the subsystems through a structured hazard analysis process such as Functional Fault Tree (FFT) Analysis (IEEE 2000), assigning SILs to the functions, implementing the

functions in the defined architectures, and finally analyzing the implementation to validate compliance with the safety requirements.

The purpose of assigning SILs as shown in Table 4 is to ensure that techniques and measures for design, verification & validation, safety assurance, and quality assurance that are mandated or highly recommended by industry guidelines (CENELEC 2001) (CENELEC 2002) for the required SIL are used in order to ensure Systematic Failure Integrity of the system.

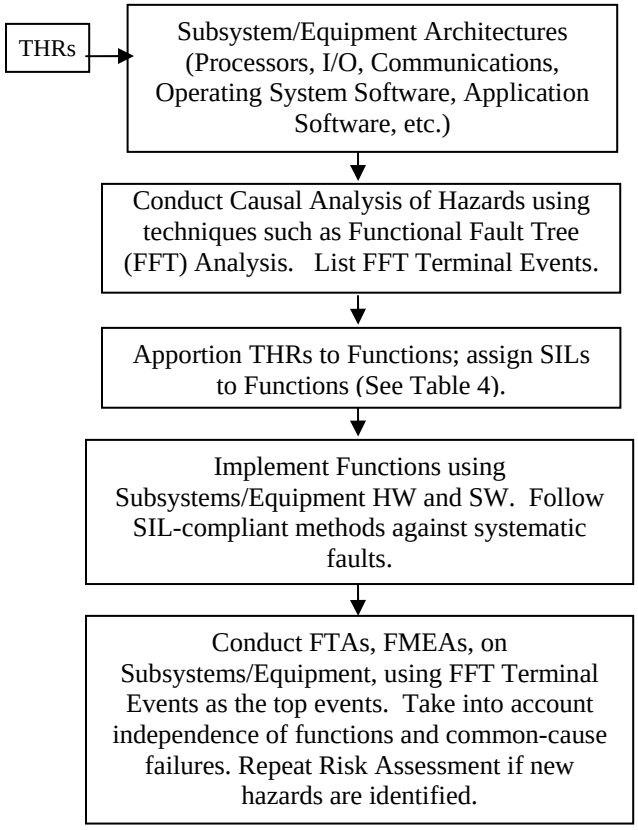

Figure 4. System Design and Analysis Steps

Table 4. THR- SIL Relationship

Tolerable Hazard Rate per Hour and per Function	Safety Integrity Level
THR < 10^{-8}	4
10^{-8} < THR < 10^{-7}	3
10^{-7} < THR < 10^{-6}	2
10^{-6} < THR < 10^{-5}	1

Application of the above process to the OSS subsystem is described here as an example. The OSS can be implemented with equipment such as Union Switch & Signal's MICROLOK® II vital programmable controller.

The architecture of the OSS is shown in Figure 5 below.

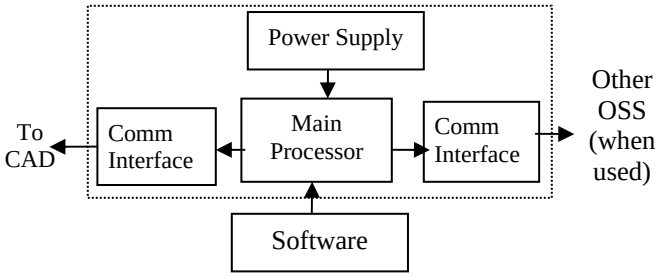

Figure 5. OSS Architecture

The OSS hardware platform consists of the main processor, communications interface with the CAD network and with other OSS units (when more than one OSS is required depending upon the size of the system), and a power supply, all mounted in a cardfile with a suitable backplane. The OSS software consists of the following components:

- Executive software that does all the system diagnostics, task scheduling and execution, system timing functions, reset processing, vital processing support functions, event logging, vital and non-vital communications, etc.
- Communications interface software that handles all message transmission and reception between the OSS and CAD, and with other OSS units when used.
- Application processing software consisting of a message director, message processors, and rules processors.
- Vital database consisting of static and dynamic data on maglev system guideway segments and paths, and movement authorities.
- Maintenance mode software for planned maintenance upgrades, troubleshooting, database updating, etc.

Through a hazard analysis using the FFT approach, Hazard H1 (See Table 1) can be shown to be the result of following functional faults (FFT Terminal Events):

1. System Executive software processing errors result in generating an incorrect MAL

2. System Executive software diagnostics fail to detect an unsafe hardware failure that results in generating an incorrect MAL
3. Communication software errors result in transmitting incorrect MAL
4. Communication protocol fails to detect corruption of MAL message due to hardware faults or external influences
5. Application processing software errors result in creating incorrect MAL
6. Vital database errors or corruption result in creating incorrect MAL.

The THR of 10^{-7} failures per passenger-mile as determined during the risk assessment phase (see Table 2) can be apportioned equally to the above six Terminal Events under the assumption that they are all independent and equally likely to occur. That is, each of the functions has to be designed to a hazard rate no higher than 1.67×10^{-8} failures per passenger-mile. They should be designed using at least SIL3 methods and techniques.

After the implementation of the above OSS functions, each Terminal Event should be analyzed further with the help of FTA and FMEA techniques to verify that the apportioned hazard rates are not exceeded. The results of the application of SIL3 methods should be documented to show that systematic failure integrity consistent with the apportioned hazard rates is achieved.

The other subsystems of the proposed maglev system shown in Figure 3 should be analyzed in a similar manner.

4. CONCLUSIONS

Quantitative risk assessment of a safety-critical system along the lines presented in this paper allows the derivation of tolerable hazard rates for the major functions of the system, using a stated safety goal as the reference. These hazard rates are then apportioned to various functions of the subsystems and equipment comprising the system, using techniques such as Functional Fault Tree Analysis. The functions are then assigned safety integrity levels consistent with the apportioned hazard rates. Design, safety analysis, and verification & validation of the functions then proceed, using methods and techniques consistent with their SILs, to ensure systematic failure integrity. Safety analyses such as FTAs and FMEAs are conducted on all the functions to show that apportioned THRs have been met, for ensuring random failure integrity. This paper has presented the application of these processes to the General Atomics urban maglev system at a high-level only. Detailed implementation and documentation of these processes is a significant task, and should be conducted on contract(s) awarded for installation and use of the system.

5. REFERENCES

AREMA. 2004. Communications & Signals Manual, *Section 17: Quality Principles. Parts 17.3.1, 17.3.3, and 17.3.5*.

CENELEC. 1999. Report prR009-004: *Railway Applications – Systematic Allocation of Safety Integrity Requirements.*

CENELEC. 2001. *Standard EN 50128: Railway Applications-Communications, signaling and processing systems – Software for railway control and protection applications.*

CENELEC. 2002. Standard EN 50129: *Railway Applications-Communications, signaling and processing systems - Safety related electronic systems for signaling.*

FRA. 2005. Rule 236 Subpart H: *Standards for Processor-Based Signal and Train Control Systems, March 7, 2005*.

IEEE. 2000. IEEE Standard 1483-2000 for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control.

Pascoe, R. D. 2008. Command, Control and Communications – Automatic Train Control System, Paper No. 6, *Maglev 2008 Conference, San Diego, CA, Dec 15-18, 2008*.

Schäbe, Dr. H. 2001. Different Approaches For Determination of Tolerable Hazard Rates**,** *Institute for Software, Electronics, Railroad Technology, TÜV InterTraffic GmbH, 51105 Köln* (2001).

UCSD. 2008a. University of California, San Diego Maglev Program Plan, GACP20000335, 28 July 2008

UCSD. 2008b. General Atomics Low-Speed Maglev Technology Development Program – Requirements for UCSD, UCSDs-OO-001, July 28, 2008

U.S. DoD. 1993. Military Standard: MIL-STD-882C - System Safety Program Requirements.