Safety Analysis from Bottom to Top and Top to Bottom

Kerim Çakmak

Rational Software
International Business Machines (IBM)
Systems and Software Engineering Solutions
Cinnah Cad. No3: Kavaklidere, 06686, Ankara TR

ABSTRACT

When it comes to functional safety, there are several ways to handle. Failure Mode Effects Analysis (FMEA) is an analysis method, generally for testing reliability which is considered as a bottom to up approach. The idea is to identify all the possible faults of the system and analyse their effects. The safety point of view is added to this method when "criticality" is introduced. This is called Failure Mode Effects and Criticality Analysis. The idea is to identify the probability of failure modes against the severity of their consequences in addition to FMEA studies. On the other hand, Fault Tree Analysis (FTA) is a top down approach to identify safety related risks of the system. In this paper, we would like to present how it would be possible to use both methods to verify each other in terms of completeness and validity. We will use a conceptual approach and try to implement these concepts in analysis tools for automation and reporting.

Keywords: Safety Assessment, FMECA, Hazard, FTA, Safety Goals, Requirements, Traceability

INTRODUCTION

Today, more complex products or systems interfere with humans directly. Ranging from automobiles, medical health care devices, planes, cell phones, trains, energy generation facilities etc. The more functionality these systems provide via a software controlled unit, the importance of safety in these systems grows. There are certain standards of course, that these systems has to comply with, regarding their industry. In a system development point of view staying compliant with these standards is an issue, regarding the cost overhead it brings. But what is more important than this is, does a system 100% compliant with the relevant standards is 100% safe to use?

In this paper, we will be focusing how different safety analysis techniques can be used to verify the coverage of hazards and their mitigation scenarios were incorporated in the design.

The first section will underline our understanding of safety. In the second section, we will discuss about the techniques of safety assessment. Third section will be about the process of deriving safety requirements and incorporating those into further analysis. In the last section, we will try to present how this process can be realized on a set of tools.

WHAT IS SAFETY

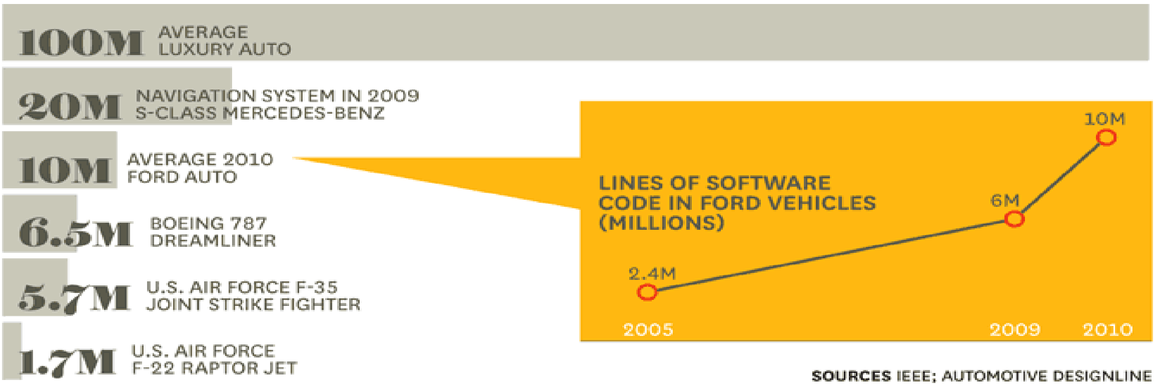
Very briefly, safety can be considered as the freedom from accidents and losses. Several definitions can be found for the term “safety”, some of which have already been confused with reliability and / or security. Where, “reliability” is again briefly the probability the system will perform its intended function satisfactorily and “security” to be the protection against outside world, like attacks, interference or espionage. Sometimes we easily confuse security with safety because both has threads but in the former threads are coming from another consciousness out of the system. This consciousness can be considered as an actor to the system. However on the latter, threads are due to the nature of the system or to the environment the system is deployed.

In this paper, we will be focusing on two analysis methods on the threads from the safety point of view and how we can use each, to verify the results of the other.

Complex Systems and Safety

Today we are surrounded with complex products, which supposed to make our lives easier. Nowadays, nearly no car is produced without an ECU as it were in 60’s or 50’s. Even though both today’s cars or the cars in the 50’s serve the same purpose (they carry us from point A to point B) why do we want to increase costs so much and make the systems more complex than every day?

One of the possible answers to this question can be found under the safety compliance issues. For instance the figure below (see Figure1) can draw us a picture about how the complexity rises with the emerging requirements of safety.



SOURCES IEEE; AUTOMOTIVE DESIGNLINE

More Complex Than a Fighter Jet: Safety regulations and consumer demand for performance and convenience have led to an exponential spike in cars’ software complexity.

Figure 1: Lines of code used in complex systems

As a functional safety standard for road vehicles, ISO 26262 is released on 11 November 2011. This standard is a customization of the IEC 61508 standard. It is obvious that increasing safety requirements and regulations put additional complexity in to the system design and definition. Today, we cannot manage to stay safe only by using checklists. We need to implement some additional (safety) requirements into our smart products driven by standards and regulations.

SAFETY ANALYSIS TECHNIQUES

While considering safety, several approaches can be discussed. It is necessary to mention the Hazard Theory, which is represented by the hazard triangle (see Figure 2).

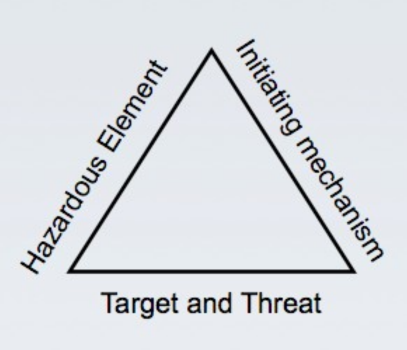
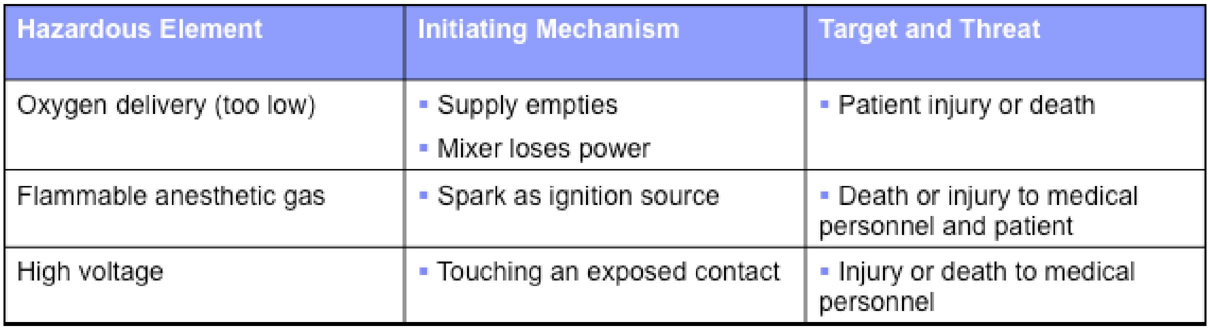


Figure 2: The Hazard

In this theory, a hazardous element is a source of harm. Possible causes of this hazard are defined in the initiating mechanism. In the target and threat section, the person or thing that is vulnerable to harm is identified. It is a common understanding to conduct the hazard analysis throughout the development lifecycle. A sample is illustrated below (see Figure 3).



Hazardous Element	Initiating Mechanism	Target and Threat
Oxygen delivery (too low)	▪ Supply empties ▪ Mixer loses power	▪ Patient injury or death
Flammable anesthetic gas	▪ Spark as ignition source	▪ Death or injury to medical personnel and patient
High voltage	▪ Touching an exposed contact	▪ Injury or death to medical personnel

Figure 3: Hazard Triangle

Specifically in the phases like, concept and preliminary design, subsystem design, system integration etc.

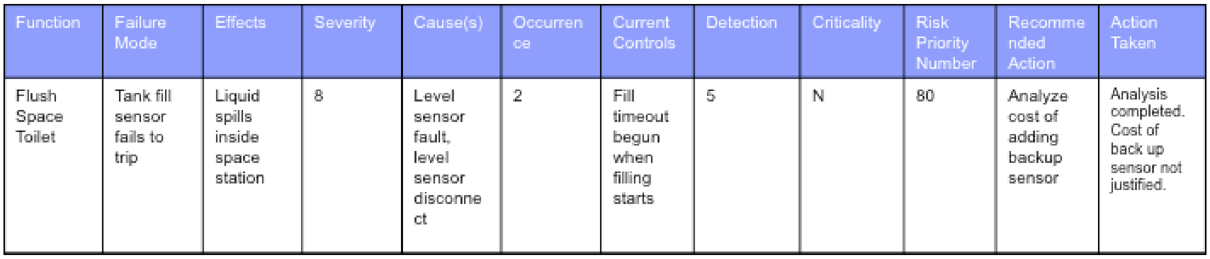
A hazard analysis is a central repository for information around system hazards, risks, and control measures. This includes the following categories of information:

- The nature of the hazard.
  What can happen? What faults can lead to the potential accident?
- The quantification of risk.
  How severe? How likely?
- The timeframe of concern.
  How long can the fault be tolerated? How long to detect it? How long to handle it?
- The control measure.
  What design features or procedures will be put into place to address the hazard and/or fault condition?

Two methods are effectively used in hazard theory. The Failure Modes Effect and Criticality Analysis (FMECA) and Fault Tree Analysis (FTA).

Briefly, FMECA can be considered as a bottom up approach, which is an extension to the FMEA (Failure Mode Effects Analysis) method. The latter, is a method of analyzing reliability. By extending this to criticality of the system under development, the method may become a safety analysis one.

In FMECA, all the possible failures of the system are tried to be determined according to the functionality of the system or to the process step. Its possible effects and the analysis of these effects are determined in a sheet which lead to a management plan to identify the risks, and their mitigation and contingency actions.



Function	Failure Mode	Effects	Severity	Cause(s)	Occurrence	Current Controls	Detection	Criticality	Risk Priority Number	Recommended Action	Action Taken
Flush Space Toilet	Tank fill sensor fails to trip	Liquid spills inside space station	8	Level sensor fault, level sensor disconnect	2	Fill timeout begun when filling starts	5	N	80	Analyze cost of adding backup sensor	Analysis completed. Cost of back up sensor not justified.

Figure 4: Sample FMECA Analysis

Another method mentioned is the FTA, which can be described as a deductive, analytical technique, such as an undesired state (a top-level event (TLE)) is specified, and the system is analyzed for the possible chains of basic events (typically, system faults) that may cause the top event to occur. A Fault Tree (FT) is a systematic representation of such chains of events, which makes use of logical gates, corresponding to logical connectives such as AND and OR, to depict the logical interrelationships linking the basic events with the top event. An AND gate relates events that are both required to occur to cause the hazard, whereas an OR gate represents alternative causes. The basic events are the leaves of the FT, whereas events that appear in between the root and the leaves are called intermediate events. The tree is typically drawn with the TLE at the top of the diagram.

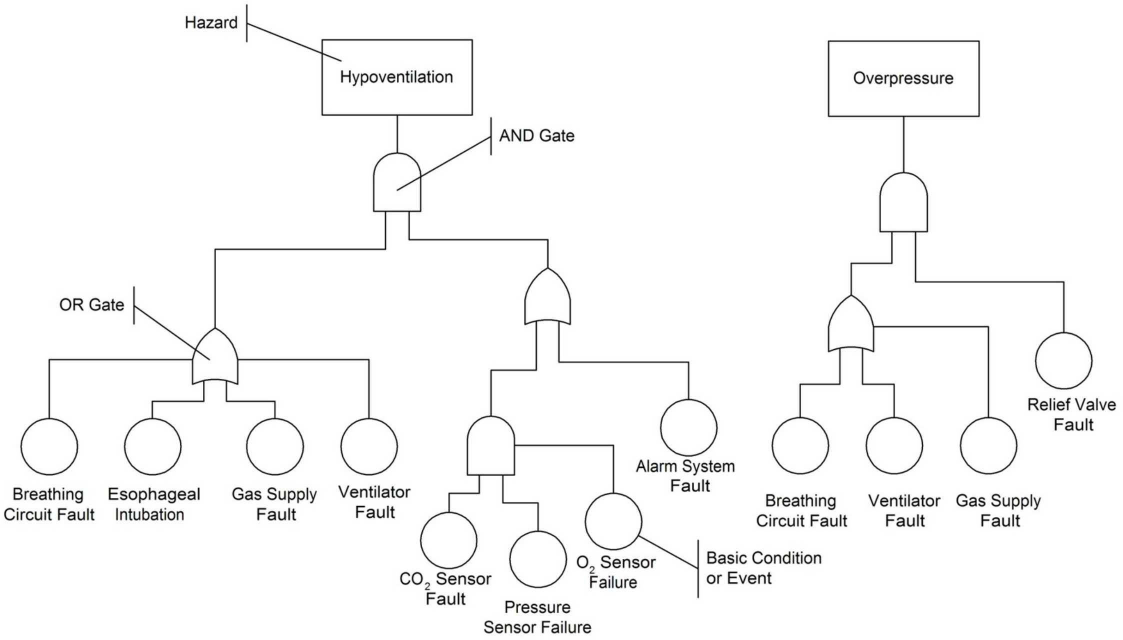


Figure 5: Sample FTA Diagram

There are other analysis models for safety assessment, other than the hazard theory. Risk analysis and risk measures are two of them. But these are out of the scope of this paper.

THE PROCESS FOR CONFORMANCE OF SAFETY IN COMPLEX SYSTEMS

In a systems engineering process, the V-model can be represented to include safety actions within the whole engineering lifecycle. Since the given set of requirements are not expected to include the requirements and specifications about safety a process is required to derive them.

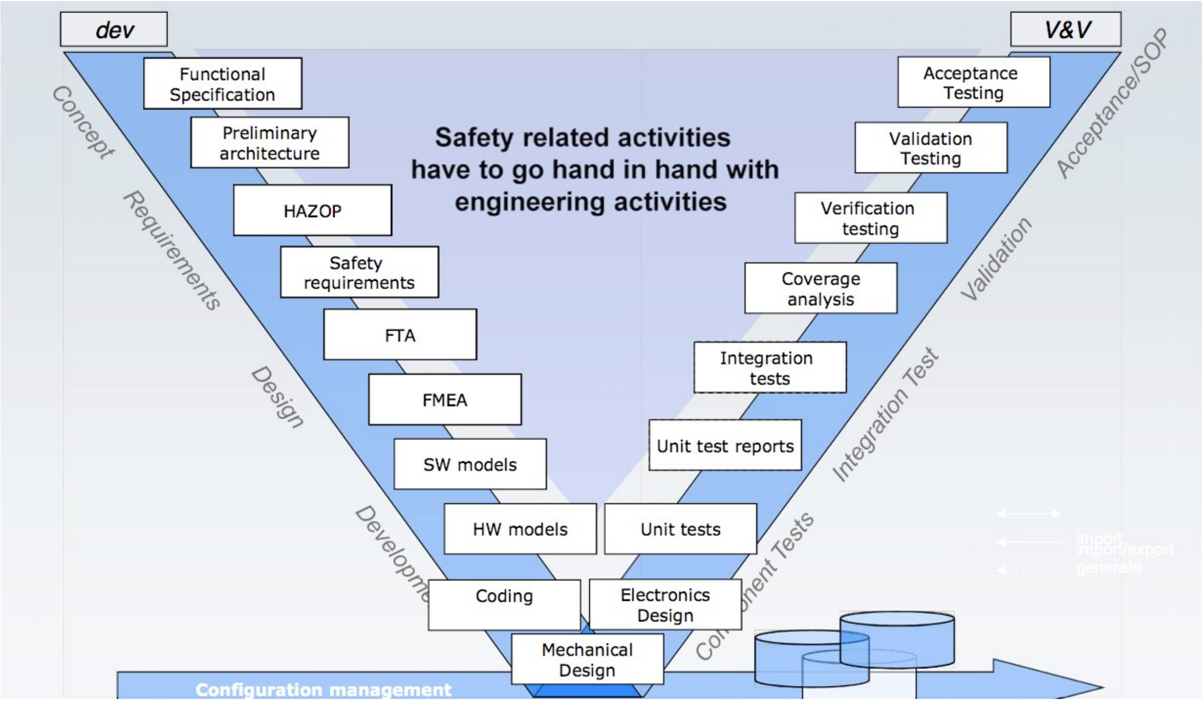


Figure 6: The V-model with safety actions

The hazard theory and the above-mentioned hazard triangle are incorporated in the “Requirements” stage here (see Figure 6).

Each hazardous element in the hazard triangle can result in one or more failure modes. Each failure mode is analyzed carefully to create a proper mitigation action, which can result into a high level safety requirement.

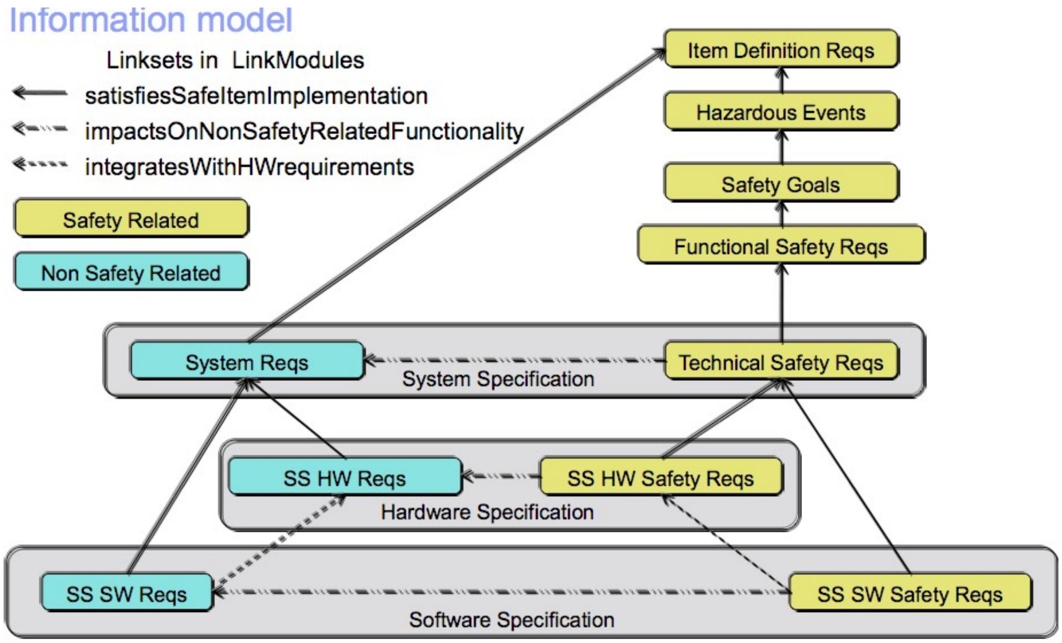


Figure 7: The Information Model for Safety Analysis in System Design

To put this in other words, refer to the figure below where safety analysis is done to derive new requirements and these requirements are used in the further analysis of the safety of the lower levels.

Considering the process under a flow,

We incorporate the hazard identification action in the early stages like system conceptual design or preliminary design.

- The causes and effects to possible hazardous elements identified.
- Effects are analyzed, classified and prioritized.
- Mitigation actions identified.
- Functional Safety Requirements out of these actions are derived.

Since this is a high level analysis of the hazards, which may cause harm, a mode detailed assessment of safety would be required when considering a detailed design phase. FTA can be used at this stage of assessment to derive technical safety requirements from the basic conditions.

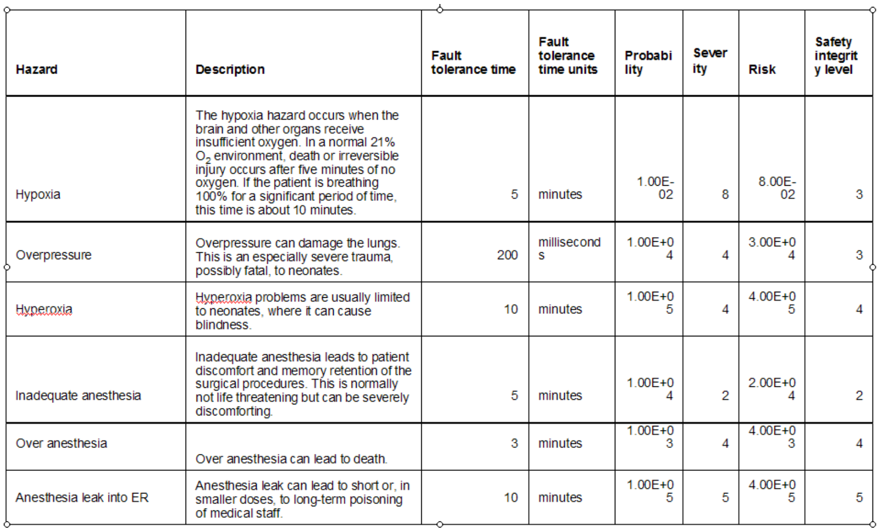
For complex systems, it is very difficult to guarantee that a specific safety goal or requirement is satisfied 100% in the design. Since, they may not be functional and may not appear in the functional allocation in the preliminary design. Moreover, system design and engineering involves trade-offs between cost and reliability, such that, a given requirement can generally be implemented in many different ways, some safer and more reliable than others.

An important concern in this process would be the coverage of the functional safety requirements in the further phase like FTA done in the design phase (see Figure 6). That should guarantee to make sure every functional safety requirement has a satisfaction from a technical safety requirement that would be derived from the FTA. To support these ideas with a technological background a tool support can be made use of.

An important component of the human systems integration plan should be a verification and validation process that provides a clear way to evaluate the success of human systems integration. The human systems integration team should develop a test plan that can easily be incorporated into the systems engineering test plan. The effectiveness and performance of the human in the system needs to be validated as part of the overall system. It may seem more attractive to have stand-alone testing for human systems integration to show how the user interacts with controls or displays, how the user performs on a specific task. This methodology can address the performance of the human operator or maintainer with respect to the overall system. The most important thing is to develop a close relationship between human systems integration and systems engineering.

TOOLS; TO SUPPORT THE PROCESS

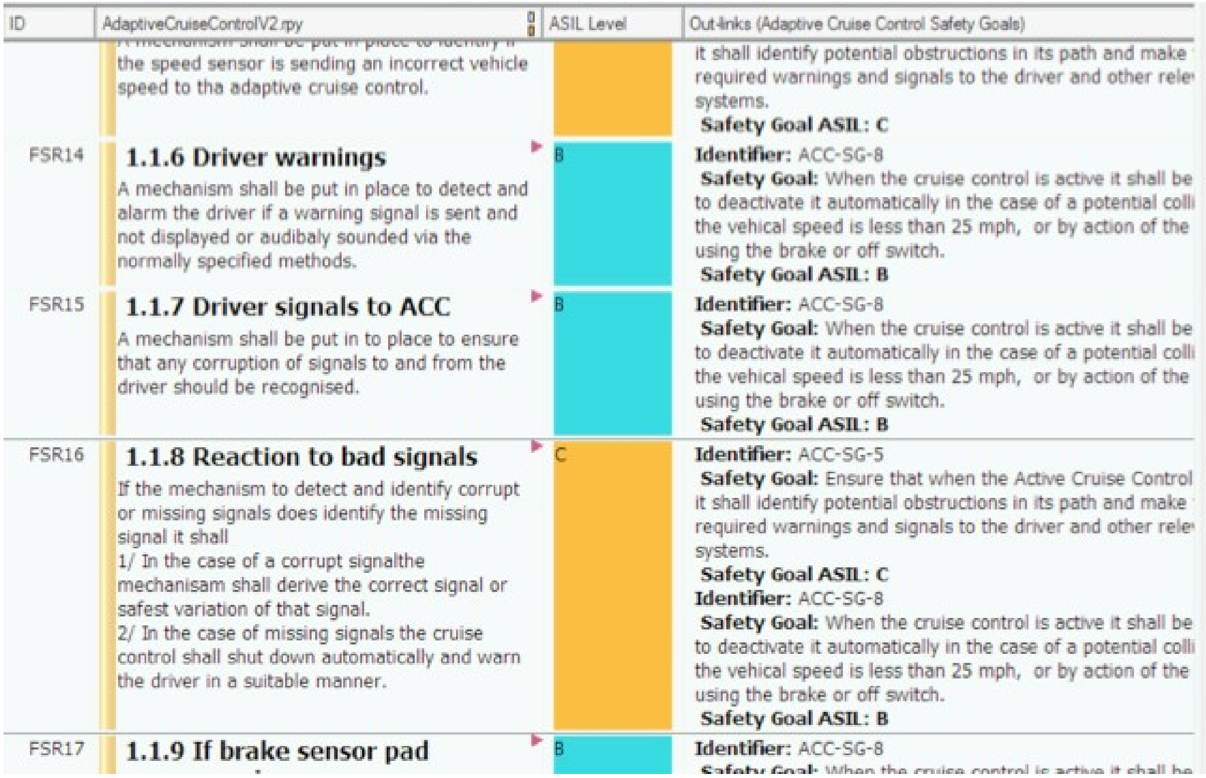
Starting with a basic sheet of hazardous elements as shown in the figure below, one can capture the functional safety requirements in a requirements management tool.



Hazard	Description	Fault tolerance time	Fault tolerance time units	Probability	Severity	Risk	Safety integrity level
Hypoxia	The hypoxia hazard occurs when the brain and other organs receive insufficient oxygen. In a normal 21% O_2 environment, death or irreversible injury occurs after five minutes of no oxygen. If the patient is breathing 100% for a significant period of time, this time is about 10 minutes.	5	minutes	1.00E-02	8	8.00E-02	3
Overpressure	Overpressure can damage the lungs. This is an especially severe trauma, possibly fatal, to neonates.	200	milliseconds	1.00E+04	4	3.00E+04	3
Hyperoxia	Hyperoxia problems are usually limited to neonates, where it can cause blindness.	10	minutes	1.00E+05	4	4.00E+05	4
Inadequate anesthesia	Inadequate anesthesia leads to patient discomfort and memory retention of the surgical procedures. This is normally not life threatening but can be severely discomforting.	5	minutes	1.00E+04	2	2.00E+04	2
Over anesthesia	Over anesthesia can lead to death.	3	minutes	1.00E+03	4	4.00E+03	4
Anesthesia leak into ER	Anesthesia leak can lead to short or, in smaller doses, to long-term poisoning of medical staff.	10	minutes	1.00E+05	5	4.00E+05	5

Figure 8: Sample Initial Hazard Assessment

It would be good practice to document all the safety goals and lower level functional safety requirements and link them together to keep track of changes. The tool would help in prioritizing the safety goals and requirements as well as managing them effectively (see Figure 9).



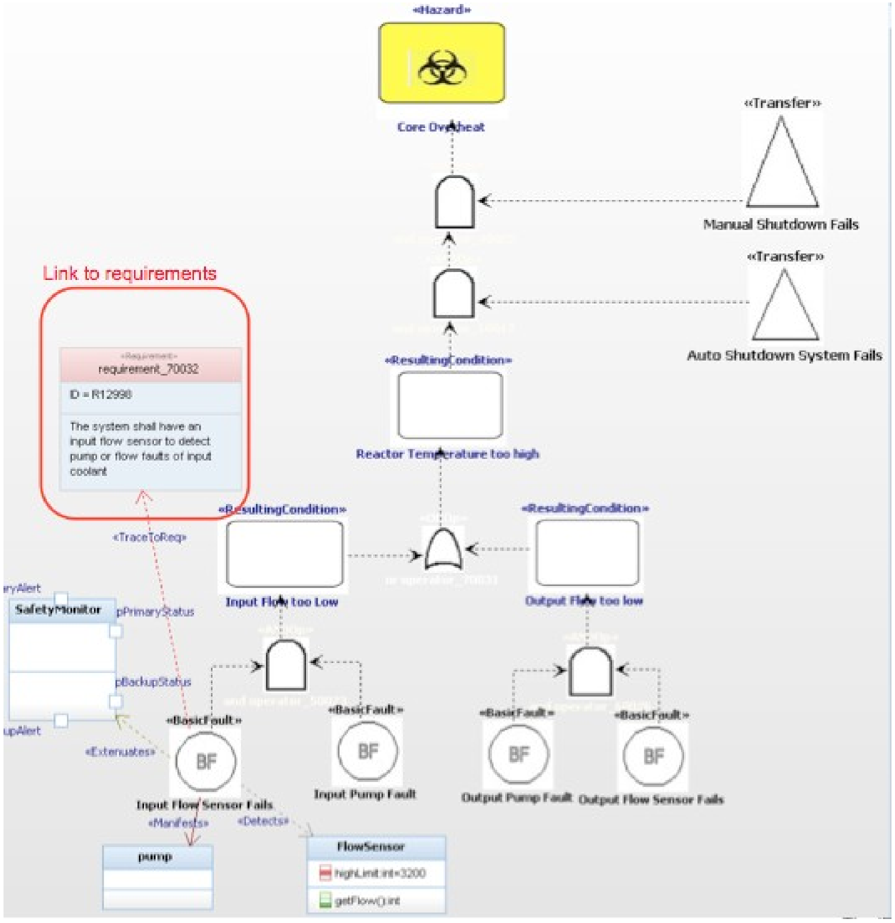
ID	AdaptiveCruiseControlV2.rpy	ASIL Level	Out-links (Adaptive Cruise Control Safety Goals)
	A mechanism shall be put in place to identify if the speed sensor is sending an incorrect vehicle speed to tha adaptive cruise control.		it shall identify potential obstructions in its path and make required warnings and signals to the driver and other rele systems. **Safety Goal ASIL: C**
FSR14	**1.1.6 Driver warnings** A mechanism shall be put in place to detect and alarm the driver if a warning signal is sent and not displayed or audibaly sounded via the normally specified methods.	B	**Identifier:** ACC-SG-8 **Safety Goal:** When the cruise control is active it shall be to deactivate it automatically in the case of a potential colli the vehical speed is less than 25 mph, or by action of the using the brake or off switch. **Safety Goal ASIL: B**
FSR15	**1.1.7 Driver signals to ACC** A mechanism shall be put in to place to ensure that any corruption of signals to and from the driver should be recognised.	B	**Identifier:** ACC-SG-8 **Safety Goal:** When the cruise control is active it shall be to deactivate it automatically in the case of a potential colli the vehical speed is less than 25 mph, or by action of the using the brake or off switch. **Safety Goal ASIL: B**
FSR16	**1.1.8 Reaction to bad signals** If the mechanism to detect and identify corrupt or missing signals does identify the missing signal it shall 1/ In the case of a corrupt signalthe mechanisam shall derive the correct signal or safest variation of that signal. 2/ In the case of missing signals the cruise control shall shut down automatically and warn the driver in a suitable manner.	C	**Identifier:** ACC-SG-5 **Safety Goal:** Ensure that when the Active Cruise Control it shall identify potential obstructions in its path and make required warnings and signals to the driver and other rele systems. **Safety Goal ASIL: C** **Identifier:** ACC-SG-8 **Safety Goal:** When the cruise control is active it shall be to deactivate it automatically in the case of a potential colli the vehical speed is less than 25 mph, or by action of the using the brake or off switch. **Safety Goal ASIL: B**
FSR17	**1.1.9 If brake sensor pad**	B	**Identifier:** ACC-SG-8 **Safety Goal:** When the cruise control is active it shall be

Figure 9: Safety goals and requirements defined

In the preliminary design phase a more detailed analysis on the hazards from top to bottom can be done as FTA. Expected result from FTA would be the technical safety requirements. Aligning these technical safety requirements with the system requirements is a way to express the safety coverage.

However, from the highest level, it is a good practice to ensure all functional safety requirements are incorporated into FTA.

Generally FTA requires a tool to draw visual diagrams. The textual representations of the functional safety requirements derived from previous hazard assessments as safety goals can be mapped to the resulting conditions or basic faults of the FT (Fault Tree) to ensure coverage (see Figure 10) .



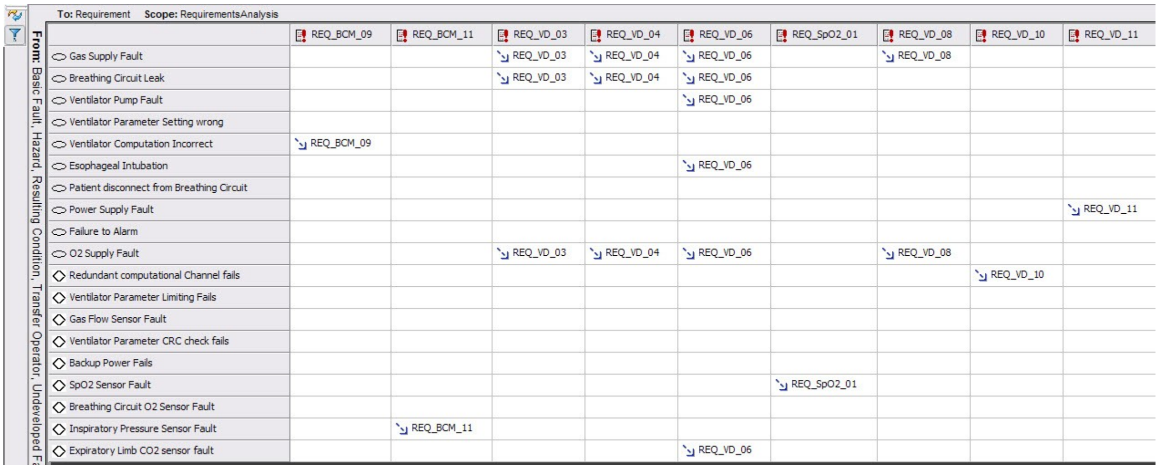
«Requirement»
requirement_70032

ID = R12998

The system shall have an input flow sensor to detect pump or flow faults of input coolant

Figure 10: Sample FTA Diagram

A linkage report can be generated based on the analysis of one or more hazards, identifying the relations between basic failures or resulting conditions and safety goals or functional safety requirements.



To: Requirement Scope: RequirementsAnalysis

From: Basic Fault, Hazard, Resulting Condition, Transfer Operator, Undeveloped Fa

	REQ_BCM_09	REQ_BCM_11	REQ_VD_03	REQ_VD_04	REQ_VD_06	REQ_SpO2_01	REQ_VD_08	REQ_VD_10	REQ_VD_11
Gas Supply Fault			REQ_VD_03	REQ_VD_04	REQ_VD_06		REQ_VD_08		
Breathing Circuit Leak			REQ_VD_03	REQ_VD_04	REQ_VD_06				
Ventilator Pump Fault					REQ_VD_06				
Ventilator Parameter Setting wrong									
Ventilator Computation Incorrect	REQ_BCM_09								
Esophageal Intubation					REQ_VD_06				
Patient disconnect from Breathing Circuit									
Power Supply Fault									REQ_VD_11
Failure to Alarm									
O2 Supply Fault			REQ_VD_03	REQ_VD_04	REQ_VD_06		REQ_VD_08		
Redundant computational Channel fails								REQ_VD_10	
Ventilator Parameter Limiting Fails									
Gas Flow Sensor Fault									
Ventilator Parameter CRC check fails									
Backup Power Fails									
SpO2 Sensor Fault						REQ_SpO2_01			
Breathing Circuit O2 Sensor Fault									
Inspiratory Pressure Sensor Fault		REQ_BCM_11							
Expiratory Limb CO2 sensor fault					REQ_VD_06				

Figure 11: Link report

All technical safety requirements derived from such analysis will already cover the linked safety goals and / or functional safety requirements.

CONCLUSIONS

Safety is a critical piece in complex systems and generally a factor that increases the complexity even further. The safety compliance is generally ensured by standards like IEC 61508 or its industry variations like ISO 26262. In this paper we tried to focus on a process that incorporates safety actions into the system analysis and design. Within this process, derivation of safety requirements and safety goals is a key element. An important point that has been missing generally in the industry is ensuring the coverage of the safety analysis in the design. To satisfy the coverage, it is beneficial to apply for a tool support. But the main concern remains, which is not to miss a single requirement that may cause a harm. The safety assessment can be employed at any stage of the design. But it is important and very beneficial to use the outputs of the former in the latter to ensure the coverage.

REFERENCES

Bozzano, Marco, and Adolfo Villafiorita. *Design and Safety Assessment of Critical Systems*. Auerbach Publications. © 2011. ISBN:9781439803318

Douglass, B.P. (2009). “Build Safety Critical Designs with UML-based Fault Tree Analysis – The basics”, Embedded.com, April 27, 2009.

Ericson, C.A. (2005), “Hazard Analysis Techniques for System Safety”, John Wiley & Sons. ©2005 ISBN-9780471720195

Lindsay, P.A., McDermid J.A, Tombs, J.D. (2000). “Deriving Quantified Safety Requirements in Complex Systems”, Computer Safety, Reliability and Security Lecture Notes in Computer Science Volume 1943, 2000. pp. 117-130