Paper 160 – RAMS analyses for the next generation of waterways

PASCUAL, X.; VILA, P.S.; CASTRO, J.A.
SENER Ingeniería y Sistemas, S.A. (Avda.Zugazarte 56 Las Arenas), Vizcaya, Spain

Email (1st author): xavier.pascual@sener.es

ABSTRACT: *Methodologies and standards from other transport infrastructures like highways and port terminals are being increasingly adapted to the special waterways' features but any common and standardized body of knowledge seems to have been stablished. In this sense, this paper states an initial basis for RAMS analyses implementation under the scope of operational management and maintenance of waterways activities considering the introduction of the new River Information Systems (RIS) that will drive the achievement of the Safety and Availability Requirements*

1 INTRODUCTION

SENER experience in the design of complete transportation systems (railways, urban transport, airports, etc.) is transferred from other transport infrastructures to the special waterways' features.

The requirements of these transport infrastructures in terms of: integration of different systems, assessment of safety and improvement of the level of service, requires a systematic approach to be applied during the entire life-cycle of the project, considering the project as a complete and complex Transportation System, so specific methodologies shall be followed to deal with the complexity and to assure the safety and the service level requirements.

In this paper we present an initial approach to the relevant aspects of these methodologies with an emphasis in the Functional Safety due to its criticality in the future key objectives of the waterways.

2 RIVER INFORMATION SYSTEMS

The foreseen projects of Waterways will introduce support systems to enhance the operational procedures and competitiveness in the supply chain, including passenger transportation.

The key objectives of this River Information Systems (RIS) are ():

- Enhance of inland navigation safety
- Provide traffic information for safety and logistics
- Enhance efficiency of the navigation, exchanging information between vessels, locks, bridges, terminals and ports
- Increase efficiency of the use of inland waterways
- Environmental protection
- Integrating existing legacy navigation systems into the new RIS framework

When designing the future waterways including the River Information Systems it is important to distinguish between Services and Key Technologies.

2.1 *Services*

According the Guidelines and recommendations for River Information Services (PIANC Report nº 125), the main services to be provided to inland waterways' user would be the ones listed below:

- Fairway Information Services (FIS)
- Traffic Information (TI)
  - Tactical Traffic Information (TTI)
  - Strategic Traffic Information (STI)
- Traffic Management (TM)
  - Local Traffic Management (Vessel Traffic Services - VTS)
  - Lock and Bridge Management (LBM)
  - Traffic Planning (TP)
- Calamity Abatement Support (CAS)
- Information for Transport Logistics (ITL)
  - Voyage Planning (VP)
  - Transport Management (TPM)
  - Intermodal Port and Terminal Management (PTM)

Cargo and Fleet Management (CFM)
- Information for Law Enforcement (ILE)
- Statistics (ST)
- Waterway Charges and Harbour Dues (CHD)

2.2 *Involved Key Technologies*

According the same Guidelines, indicated services would be provided through the use of some key technologies like the ones listed below:
- Inland Electronic Chart Display & Information System (ECDIS)
- Inland Automatic Identification System (AIS)
- Electronic Reporting
- Notices to Skippers
- Radiotelephone Service
- Radar and Additional Location Devices

Additional Technologies such as enhanced communications systems (high-performance radio systems or satellite communications and location systems) plays crucial role in the deployment of the above identified technologies and services.

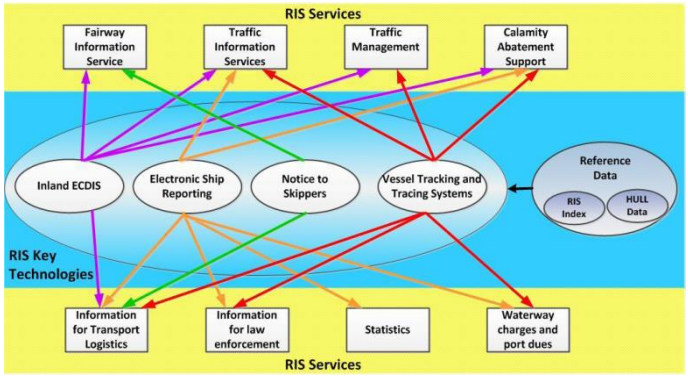


Figure 1: Relationship between RIS services and Key Technologies. (Source: PIANC)

On the operational side, a state-of-the art of TIC services will be required to deal with huge data management and storage, automatic decision making algorithms to improve the operations in real time.

All these technologies shall be designed and integrated into the civil infrastructure of the waterway and the port and shall manage low-tech devices such as lockage gates, mechanical equipment, etc.

It is important to manage this kind of projects with a system wide approach based in the mentioned objectives for the entire infrastructure:
- Guarantee Certain Level of Service
- Improve the Operations
- Assure the Safety for people and assets
- Be integrated into the environment with low environmental impact
- Be integrated with adjacent modes of transport when available.

3 SYSTEMS ENGINEERING APPROACH

Systems engineering is a methodical, disciplined approach for the design, realization, technical management, operations, and retirement of a system. Here "system" is a Waterway Transportation Infrastructure (e.g. civil structures, mechanical elements) together with a collection of different equipment for process and control that together produce results not obtainable by the elements alone.

Systems engineering is a holistic, integrative discipline, wherein the contributions of structural engineers, electrical engineers, mechanism designers, power engineers, human factors engineers, and many more disciplines are evaluated and balanced, one against another, to produce a coherent whole that is not dominated by the perspective of a single discipline.

We can consider Waterways Projects to consist of two main stages; the development of an engineering solution in the form of a detailed design and the delivery of the design solution through a procurement and build process.

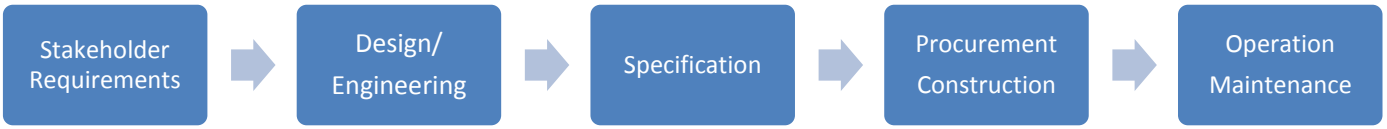


Figure 1: Waterway Infrastructure Life Cycle

The design processes Waterways Infrastructures is, to a large extent, circumscribed by standards and codes; the technical solutions will be similar to those of recent projects, and the cost of the design will be a fraction of that of the implementation, which in this case is the construction stage. Due to these factors, the design processes tend to be relatively well established and reasonably optimized and any

complexity to be addressed lies more in issues of interfaces, procurement and constructability.

In the Waterways Projects there are many complexities. There may be a number of outcomes required by a variety of stakeholders, some seemingly contrary to each other, and many alternative ways to satisfy the requirements all competing for priority and for the same resources and finances.

For projects that have a long time span, construction will often begin before engineering is complete. Situations such as these require a systematic approach in order to keep the project aligned. These circumstances add significant complexity to otherwise straightforward processes. For example, design change analysis will require not just consideration of the affected system/sub-system designs but also of the procurement and construction status of all interacting systems and facilities.

A common model used within infrastructure projects is the 'V' Model. This model serves as a guidance for Systematic Approach to Integration in order to coordinates the activities between design and construction parties in terms of technical responsibilities and shared interfaces. Systems Integration avoids gaps and unclear scope definitions between technical disciplines: civil structures, mechanical components, lockage mechanisms, vessel information system, communications, etc.

There are several systems engineering practices that are involved in the Systems Approach for design and construction of Waterways Projects and in this paper we propose to focus in: requirements management, interface management, Safety and Availability Engineering, as part of the RAMS Discipline.

The application of systems engineering to the Waterways Design and construction is essential to support client's expectations for the timely and cost-effective delivery of the project.

This approach to systems engineering will avoid over-engineering and its associated higher costs and unnecessary complexities.

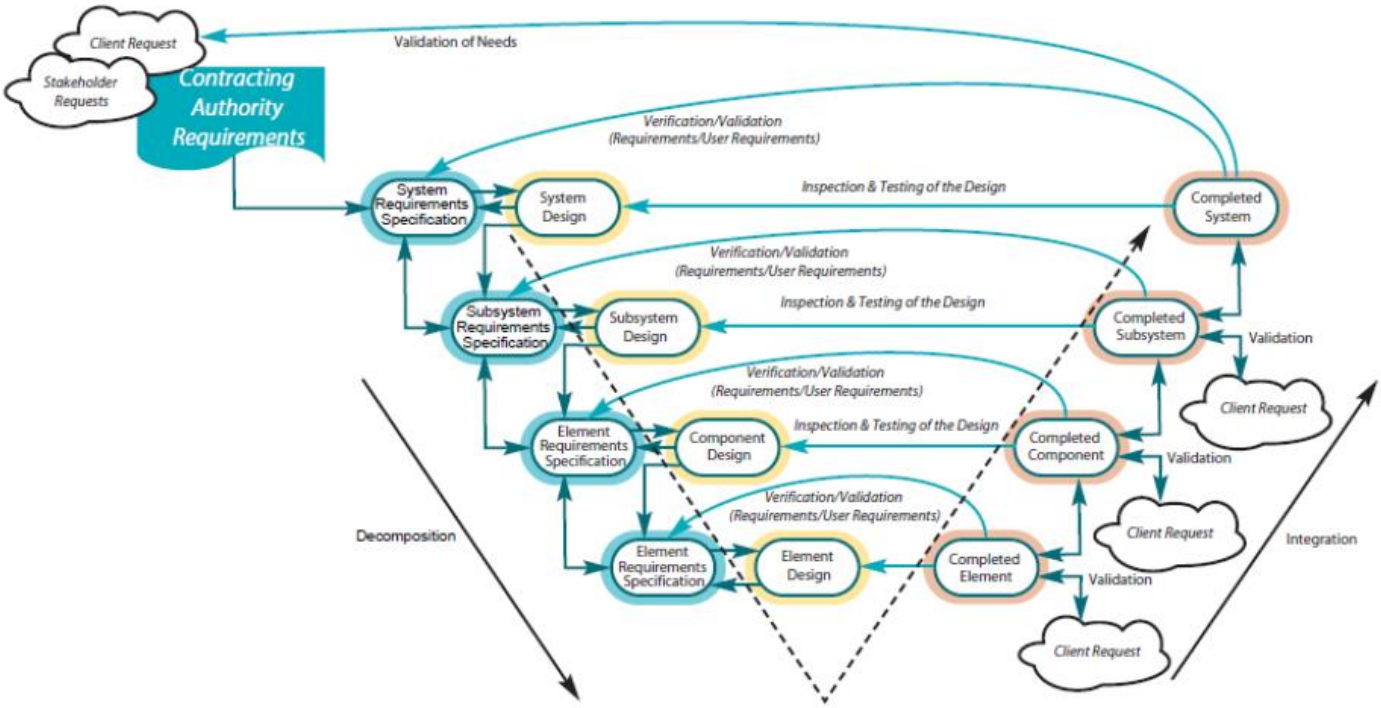


Figure 2: Systems Approach V-Model (source Dutch Ministry of Public Works)

From this model it is clear that a comprehensive Requirements Management activity is crucial for the following reasons:

- Specify since the very beginning the scope of works clearly.
- Include the Clients expectations and needs into a single framework as other inputs to the project-
- Include non-technical issues to the project life-cycle such as RAMS and environmental constraints.
- Allow a systematic procedure to follow the design and define the verification and validation processes once the design and construction stages are completed.

- Allow a systematic procedure for change management during project execution.

On the other hand, The goal of interface management is to identify, coordinate and perform design integration with adjacent contracts, third parties and other entities in cooperation with the Client. The interface management will assure that the work (design and construction) is being designed and executed in a way that facilities and subsystems are being accommodated without functional or physical constraints.

3.1 *Requirements Management*

Requirements management activities apply to the management of all stakeholder expectations, customer requirements, and technical product requirements down to the lowest level component requirements.

There are several fundamental inputs to the Requirements Management Process:

- Requirements and stakeholder expectations are identified during the system design processes
- The Requirements Management Process must be prepared to deal with requirement change requests that can be generated at any time during the project life cycle or as a result of reviews and assessments
- System Verification and Validation results from the Verification and Validation Processes are mapped into the requirements database with the goal of verifying and validating all requirements.

The Requirements Management Process involves managing all changes to expectations and requirements baselines over the life of the project and maintaining bidirectional traceability between stakeholder expectations, customer requirements, technical requirements, component requirements, design documents, and test plans and procedures. The successful management of requirements involves several key activities:

- Establish a plan for executing requirements management.
- Receive requirements from the system design processes and organize them in a hierarchical tree structure.
- Establish bidirectional traceability between requirements.
- Validate requirements against the stakeholder expectations, the mission objectives and constraints, the operational objectives, and the project success criteria.
- Define a verification method for each requirement.
- Evaluate all change requests to the requirements baseline over the life of the project and make changes if approved

As each requirement is documented, its bidirectional traceability should be recorded. Each requirement should be traced back to a parent/source requirement or expectation in a baselined document or identify the requirement as self-derived and seek concurrence on it from the next higher level requirements sources.

An important part of requirements management is the validation of the requirements against the client expectations, the project objectives and constraints, the operational objectives, and the project success criteria.

3.2 *Interface Management*

There shall be four (4) phases in the Interface Management process:

- Interface Identification

  Although interfaces can be initiated throughout the life of the project, the initial identification of inter-faces shall be a structured process which shall be carried out by all involved parties.

  Interfaces shall be identified on the Interface Matrix (IM), and for each of the entries, a list of interfaces and their descriptions shall be elaborated in the Interface Register (IR).

- Interface Definition:

  This definition will allocate responsibilities to define the path forward to resolve the interface by means of the design activities.

  Interface definitions shall include one or more of the following categories of information: Functional and technical definition, Demarcation points between works and/or systems, Limits of work scope between the parties, Construction/Installation requirements, Validation Requirements

  The aim of the definition phase shall be to fully agree and baseline the interfaces to a point where interfacing parties are able to carry on with their own designs on the basis of the agreed interface.

- Interface Resolution

  Resolution of an Interface may occur during various stages of the project as follows: at the same time that the interface definition is reached, once both interfacing parties have completed and are satisfied with their own design on the basis of the agreed interface definition.

  Interface resolution shall be achieved directly by the interface parties defining the agreed actions, responsibilities and target dates.

The information recorded for each interface will include: Interface description, Interface location, Interface status, indicating whether the interface is closed (design complete and mutually agreed) or in progress

- Interface Validation

  Following the resolution of an interface which has a functional aspect, the correctness of its design and implementation shall be validated.

  The validation of interfaces will generally be achieved through specific activities as specified in the cor-responding plans (e.g. Validation Plans or Test, Commissioning and System Integration Plan). These activities will encompass formal verification through test, specific analysis, review of design, etc.

4 SAFETY ENGINEERING

The Waterway Projects are intended to provide a means of transportation both for freight and passengers and the design shall consider also additional operational aspects that may influence in the final performance. One of this issues that is becoming a guiding constraint in other transportation systems (e.g. railways, urban transport, etc.) is the Functional Safety.

Safety Engineering encompasses a set of norms and methodologies to consider the safety as an input requirements since the beginning of the design of the Waterways system, including the client needs and expectations in terms of mitigation of accidents and hazards to avoid; not only casualties, even unexpected economic impacts, etc.

RAMS (Reliability, Availability, Maintainability and Safety) is a major contributor to the Quality of Service provided by the Waterway Project.

RAMS engineering is of utmost importance in the development of a waterway line, because the correct application and development of the RAMS engineering, methods, and tools shall drive the behaviour of the system, and determine whether the system will:

- Be able to achieve a defined level of rail traffic in a given time
- Be reliable and available to perform its given function
- Upon occasional failures, be repairable, and maintainable, with an acceptable restoration time
- Be safe for the lives of users, maintainers, and operators

RAMS engineering has a clear influence on the cost of the system during the whole life-cycle of the project (i.e. from design and development, through to operation and maintenance phases), because RAMS engineering will determine:

- The level of redundancy required to achieve a specific availability
- The complexity and cost of development of the subsystems (i.e. the development cost of subsystems with safety requirements, soars as the required level of safety increases)
- The numbers of spare parts, spare equipment, and spare trains to achieve a specific avail-ability and restoration time

RAMS is a characteristic of a system's long term operation and is achieved by the application of established engineering concepts, methods, tools and techniques throughout the lifecycle of the system.

The global process consists of risk analysis and hazard control. The risk analysis produces tolerable hazard rates which are the input to the hazard control.

In order to guarantee the required levels of safety a systematic approach shall be performed using the guidance of industry standards and similar practices from other transportation infrastructures, such as railways or process industry.

This methodology will avoid by design the occurrence of hazardous situations during operations.

All these techniques and tools are also described in in the norms listed in section 7:

This Safety or Risk Assessment Study comprises "every process control system considering each device and facility that have electrical and/or electronic and/or programmable electronic (E/E/PE) technologies.

The risk assessment study shall determine all required safety functions and safety integrity requirements for the project to be sufficiently reliable in order to prevent major hazards: flooding lower levels of locks facilities, dry-docking a ship, collisions with structural elements, collisions between vessels, etc.

The level of depth for the Risk Assessment Study and will be consistent with the level of procurement (replaceable items) as long as functionally independent items can be found.

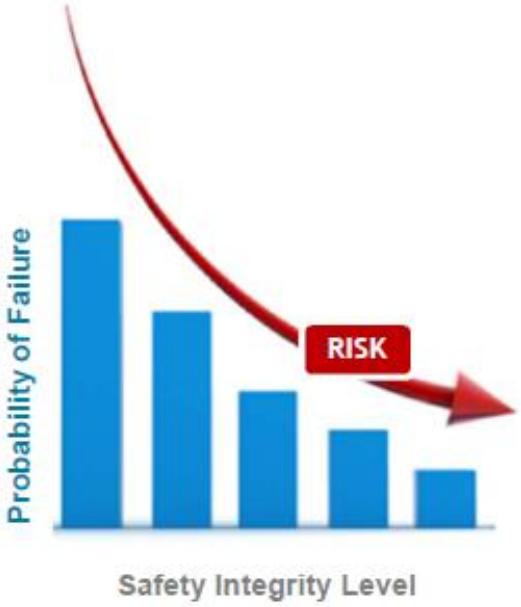
If one replaceable item provides on its own a single safety function, then the replaceable item will be the lowest level the analysis will reach.

If for instance two or more replaceable items are located into an equipment or subsystem, and they together collaborate to provide a single safety

function, then the analysis will be kept at a the equipment or subsystem level.

A clear definition Safety Integrity can be found in IEC 61508: "Probability of an safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time", that is:

- The higher the level of safety integrity, the lower the probability of failure of the safety-related system.
- Safety integrity comprises hardware safety integrity and systematic safety integrity.
- Random hardware failures, may be quantified using such measures as the average frequency of failure.
- Systematic failures cannot be accurately quantified but can only be considered qualitatively.
- SIL is allocated to Functional Safety Requirements, not to system elements.



The Safety Engineering comprises ten (10) stages that are introduced in the following sections.

4.1 *System Definition*

On this phase we will define with a high-level of detail a functional description of the Waterways Infrastructures, with all the Operational Systems, including those in charge of the Operation and Control that may involve an impact in the functional safety of the infrastructure, as defined above.

The definition of the System shall be based and supported by the Owner requirements already identified where will be defined the operational principle, the safety policy to be followed and guidelines that will define required level of services.

The core activities that will be performed during this phase will be:

- Definition of the system boundaries
- Performance of a functional analysis along with identification of functional safety requirements
- Identification of safety related technical and operational requirements (at system level)

4.2 *Hazard Identification at System Level*

In this stage it is crucial to involve both the final Operator (if it is identified) together with the Employer or the Owner currently in charge of the Project. A set of brainstorming or similar meetings shall be conducted in order to list the relevant accidents (including estimations of levels of consequences) for the envisaged Waterway Infrastructure. These accident descriptions must include field data (if available from similar infrastructures).

With these inputs the activity during this phase will focus on:

- Sort out the relevant top-level hazards
- identify hazards at system boundary (i.e. the system contribution in the disasters sequences)

The objective will be to produce a list of hazards for the Waterways Infrastructure aligned with the Project boundaries, in order to identify clearly what is out of the scope of the project and cannot be managed by Infrastructure (e.g. natural disasters, vandalism, etc.)

As an example of the above identification, the top level hazard (i.e. disaster) may be the "structural damage to a vessel" if locks are included into the project scope of works, but the hazard at the System Level boundary is that "a lock gate closes unexpectedly".

4.3 *Consequence Analysis*

After a clear identification of the Hazards described at System Level boundaries, that is, considering the scope of works in a waterways project, we will have a unique list of "System Level Hazards". Considering also operational procedures, and other knowledge of the project including modes of operation, technical and operational aspects contributing as factors or mitigations in the hazard sequences, the activities during this stage of analysis will be:

- Analyze the possible consequences of each hazard, as identified in stage 2 (identify the sequences of events /conditions leading to a disaster).

- The following techniques will be used: Event Tree Analysis, and Fault Tree Analysis (Cause-Consequence Diagrams)

So, we will be able to develop a Cause-Consequence model, including quantified estimates for the probability of occurrence of each accident sequence initiated by each hazard.

Considering again the above example, with the Top Level Hazard (TLH) , "structural damage to a vessel" the objective is to estimate the occurrence probability of this TLH once the System Level Hazard (e.g Lock Gate closes unexpectedly) is triggered.

As mentioned, one technique is to evaluate this probability with the Event Tree Analysis tool, as shown in the following figure:

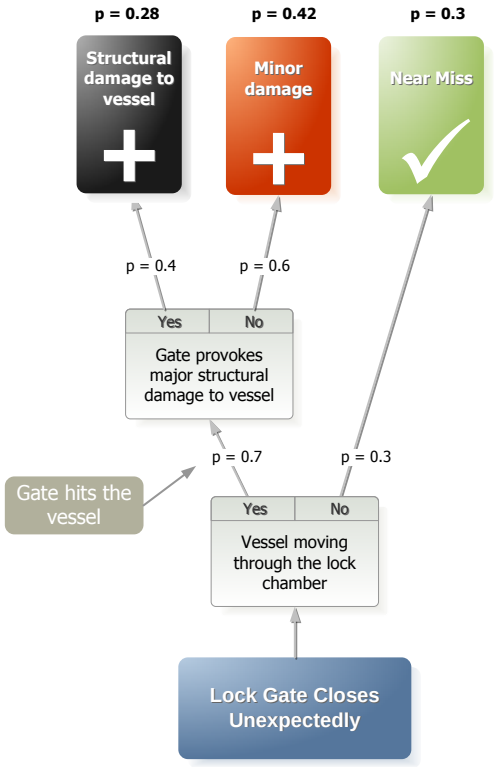


Figure 3: Event-Tree Analysis

4.4 *Risk Tolerability Assessment at System Level*

The next step is to define for each of the System Level Hazards a numerical value of tolerable risk. This value will be the occurrence probability of the hazard that the system is assuming that can occur to achieve the overall safety targets. These targets are defined or derived from the first two stages of this process and shall be agreed with the Infrastructure Owner, Operator, etc.

Considering the Cause-Consequence Models for each of the System Level Hazards and the agreed Safety Citeria, we will develop a risk acceptability criteria that will be depicted into a risk matrix.

The following figure shows an example of Risk Matrix applicable to a waterway infrastructure with a Operational Life-Cycle (until retirement of the Infrastructure) of 100 years. It is very important to highlight that this matrix and especially the values for frequency and severity shall be agreed with all the stakeholders of the project.

Severity				3	2	1	0
Consequences	Personal Safety			Catastrophic	Critical	Marginal	Negligible
	Environment			Massive effect	Major effect	Localized effect	Slight effect
	Investment			Extensive damage	Major damage	Localized damage	Slight damage
	Reputation			International impact	National impact	Considerable impact	Slight impact
Frequency (Events / year)	A	Frequent	F > 1	Intolerable	Intolerable	Intolerable	Undesirable
	B	Probable	1 > F > 1/10	Intolerable	Intolerable	Undesirable	Tolerable
	C	Occasional	1/10 > F > 1/100	Intolerable	Undesirable	Tolerable	Tolerable
	D	Improbable	1/100 > F > 1/1000	Undesirable	Tolerable	Tolerable	Negligible
	E	Incredible	F <1/1000	Tolerable	Tolerable	Negligible	Negligible

Figure 4: Risk Tolerability Matrix

For each of the identified Hazards and considering the tolerability criteria of the matrix, the Tolerable Hazard Rate (THR) is assigned, that is, the tolerable frequency (in events/year) that is acceptable for this hazard to keep the entire System (i.e, the Waterways Project) safe.

Note that for similar infrastructures and projects, this THRs may also be derived from comparison with existing systems or from acknowledged rules of technology, either by analytical or statistical methods.

So the output of this stage will be the List of System Hazards (as identified in stage 2) and the associated THR.

Back to the example that we are using as a guide for this explanation, from the event tree of stage 3 and, the system hazard has two relevant consequences:

- Structural Damage to a Vessel, with a tolerable frequency less than F<0,01 events/year (Critical)
- Minor Damage to a Vessel, with a tolerable frequency less than F<0,1 events/year (Marginal)

From the consequence analysis we select the most restrictive THR for the same System Harzard:

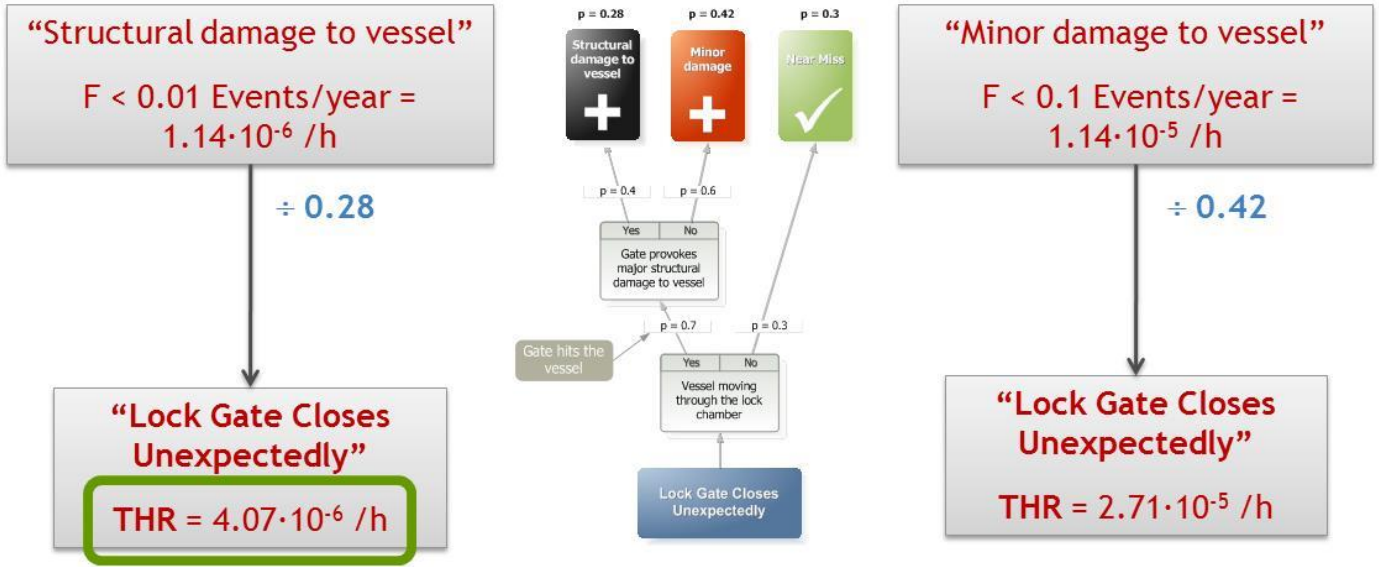


Figure 5: Tolerable Hazard Rate (THR) Assignation

4.5 *System/Subsystem Level Safety Requirements*

Once we have the System Hazards identified and quantified with the required THR value the objectives of this stage are:

- Translate system hazards into functional safety requirements
- Refine / complement the identification of safety related technical and operational requirements.

The above activities will allow establishing:

- A list of system functional safety requirements
- A quantified qualification of the tolerable frequency of system failure to meet each requirement (derived from the THR)
- List of system safety requirement (of technical or operational origin), which may not have been expressed as functional requirements.

Considering again the above example we have to translate system hazards into functional safety requirements with a quantified qualification of the tolerable frequency of system failure, for instance; the safety function will be:

"The gate shall operate from fully open to fully closed after the operator activates the close operation. The lock gates shall not close without a prior operator order." The tolerable frequency of system failure of this safety function is THR = 4.07·E-6 /h.

4.6 *System Design*

In this stage it is crucial that the safety engineering activities evolves aligned with the detailed design of the Waterways to:

- Breakdown the system into subsystems, and elements.
- Develop a structured functional analysis, and identify safety related technical and operational requirements down to subsystems and elements level.

Then subsystems and elements specifications traceable to the system specification will be available.

4.7 *Causal Analysis*

The critical objectives of this stage is to identify hazards at lower levels and to allocate them a THR, to elements/equipment/functions.

It includes two major activities:

- Fault tree Analysis (FTA)
- Common Cause Failure -CCF- analysis to justify independence of items.

To obtain:

- List of subsystem/element hazards.
- Description of the sequences of events linking subsystem/element hazards to system level hazards.
- Apportionment of THR to subsystem/element hazards

Considering again the example for a locking devices into a waterways, the following figure contains an example of a Fault Tree Analysis of the "Lock Gate Closes Unexpectedly" hazard. In this hazard, several subsystem/elements may participate: Local Machinery Control, Variable Frequency Drive, Motor Control, etc.

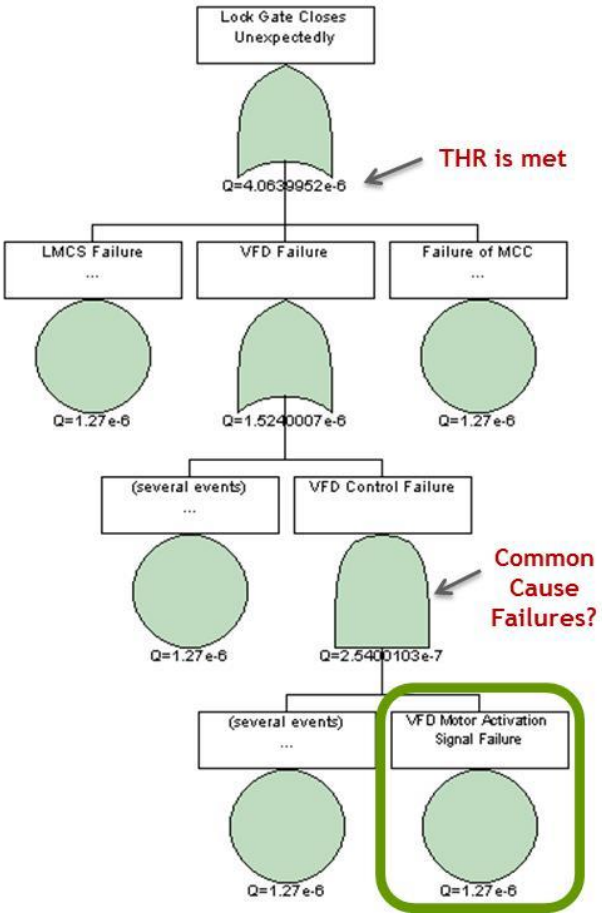


Figure 6: Fault Tree Analysis Assignation

Top event for the FTA is the system hazard, and most basic events are subsystem/element hazards at its boundary.

At the end of the tree, the following event is reached: "VFD Motor Activation Signal Failure"

A tolerable hazard rate THR = 1.27·E-6/h has been apportioned to the VFD hazard "VFD Motor Activation Signal Failure".

Now we are near to our objective, that is to identify those physical requirements for equipments and devices that guarantees that our overall design is safe, from a top-down and structured analysis.

4.8 *Safety Requirements Specification*

The objective of this stage is to translate subsystem/ element hazards into subsystem/ element level functional safety requirements and refine/complement the identification of safety related technical and operational requirements.

So we will obtain a list of subsystem/element functional safety requirements and a quantified qualification of the tolerable frequency of subsystem failure to meet each requirement (derived from the THR).

So, again with the same example, the Safety Function will be:

"The VFD shall drive the gates operating motor mechanism. The VFD shall not start the motors without a prior order from the control system"

"The tolerable frequency of failure of this safety function is THR = 1.27·E-6/h"

The above requirement is quantifiable and allows the design team to include in the detailed design the required element with this specification as an input for the procurement team. Providers shall be able to demonstrate (again using the same approach and standard) that the equipment or component has the required failure probability, based in manufacturers data, performing records, etc.

4.9 *Safety Integrity Categorization*

One common framework that has becoming very popular in other engineering disciplines such as railways systems engineering or space and aeronautics industry is a cathegorisation of the safety functions using the Safety Integrity Levels (SIL) based in the operational conditions of the safety function, that is: if the function is performing continously (e.g. valve control, location system for a vessel, etc.) or if this function is designed to be operated under demand (e.g. emergency stop button, manual procedures to operate a device, etc.)

There is a consensus in the engineering practives to assign a correspondence between THRs and these Safety Integrity Levels (SIL) following the next table:

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function	Average frequency of a dangerous failure of the safety function [h^{-1}]
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 7: Safety Integrity Levels Assignation

Note that the values of THR (failures probabilities per year or per hour) are different if the Safety Function operates continously or on-demand, because the number of events /year will be completely different.

With our example, we will have a Safety Function: "The VFD shall drive the gates operating motor mechanism. The VFD shall not start the motors without a prior order from the control system" The Safety Integrity Level of this Safety Function is SIL1.

4.10 *Consolidation of SIL Allocations*

In complex systems, the same function will participate into several System Hazards mitigations, to will be analyses with different points of view and within different scenarios and considerations.

Each of these analysis will give different values of tolerable hazard rate, that is, the same element will be required to have different probability of failires, so the final stage of this process is to consolidate the SIL Allocations and Failure probabilities to the safest and most restrictive case:

4.11 *Implications of different SIL Levels*

After the above description step-by-step of the overall process it is important to give an overview of the expected impact of the SIL levles into the design processes:

SIL 1: is relatively easy to achieve especially with proven quality management practices apply throughout the design providing that Functional Safety Capability is demonstrated.

SIL 2: is not dramatically harder than SIL 1 to achieve although clearly involving more review and test and hence more cost.

SIL 3: however, involves a significantly more substantial increment of effort and competence than is the case from SIL 1 to SIL 2. Specific examples are the need to revalidate the system following change and the increased need for training of operators. Cost and time will be a significant factor and the choice of vendors will be more limited by lack of ability to provide SIL 3 designs.

SIL 4: involves state of the art practices including 'formal methods' in design. Cost will be extremely high and competence in all the techniques required is not easy to find. There is a considerable body of opinion that SIL 4 should be avoided and that additional levels of protection should be preferred.

Finally, it is important to appoint some typical misunderstanding in the concept of the SIL in the Systems Design:

SILs should be assigned only after a top-down analysis starting from the highest system level. It is meaningless to assign SILs prior to completing such an analysis.

SIL assignment should be undertaken down to a level where functionally independent items can no longer be found.

SILs are allocated to safety-related functions and consequently the subsystem/element implementing these functions, but no further. SIL for an element (and for some elements), which are part of a subsystem (or system), is the same as for the equipment, unless functional independence can be demonstrated between elements within the equipment/element.

Functions with SIL0 exist and they may still make a significant contribution to safety. In such cases, no specific Safety Integrity requirements are defined. This does not mean that these functions are superfluous or that they need not be implemented. It only means that no Safety requirements need to be specified.

5 AVAILABILITY ENGINEERING

Systems Assurance is the application of management methods and analysis techniques to assure that a design meets Reliability, Availability, Maintainability and Safety (RAMS) criteria. Hence, Systems Assurance is often referred to as RAMS Assurance. System safety has been introduced in the previous section.

The RAM approach as described by CLC/TR 50126-2:2007 (see section 7) is achieved by the application of established engineering concepts, methods, tools and techniques throughout the life cycle of the Waterways System, and can be characterized as a qualitative and quantitative indicator of the degree that the system, can be relied upon to function as specified and be both available and reliable.

Note that the referred standard deals with the application of RAMS to Railways; as mentioned earlier, the application of an industry proven methodologies with a holistic and system-wide sense guarantees the successful achievement of the project objectives: a transportation system (in this case, a waterway with systems to control the operation).

RAM management is an important discipline that contributes to a number of other engineering processes: Design by equipment and system topology selection guided by probabilistic reliability modeling and reliability demonstration through observed failure data; Operational & maintenance by guiding the operational and maintenance procedures, Continual improvement through a reliability growth program.

The goal of the Waterway system is to achieve a defined level of service in a given time. Railway RAM describes the confidence with which the system can guarantee the achievement of this goal. As such it is a major contributor to the Quality of Service required by the Client or Owner of the Infrastructure.

6 CONCLUSION

The future development of the Waterways Infrastructures will require the introduction of additional systems to achieve operational objectives and guarantee the safety of the operations. Among these new systems to be included the River Information Systems (RIS) plays a crucial role and require that their design evolves aligned with the other engineering disciplines, typically focused in infrastructures and mechanical devices.

This paper presents a holistic approach to deal with the complexity of these projects from a System-Wide point of view with an especial emphasis on some of the critical aspects that typically drive the Project Life-cycle activities: requirements, management or safety management.

7 REFERENCES

- IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems. Parts 1-7.

- IEC 61511-1:2003 Functional safety - Safety instrumented systems for the process industry sector.
- ISA-84: "Safety Instrumented Functions(SIF) - Safety Integrity Level(SIL) Evaluation Techniques" (ISA–TR84.00.02–2002).
- IEC 62061:2005 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- IEC 61025:2006 Fault tree analysis (FTA).
- CLC/TR 50451:2007 Railway applications - Systematic allocation of safety integrity requirements.
- CLC/TR 50126-2:2007 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the application of EN 50126-1 for safety