SUCCESSFUL INTERFACE RISK MANAGEMENT – FROM BLAME CULTURE TO JOINT ACTION

Axel Kappeler, Principal

James Catmur, Director

Arthur D. Little

SUMMARY

Interfaces are important because they are everywhere. However, interfaces can be a problem, for example because responsibilities are not clearly defined, the exchange of information is not smooth or different parties have different incentives affecting their behaviour towards managing interface risks. Current approaches for managing safety risks at interfaces often only consider technical aspects, especially the interaction between systems or sub-systems. Some include considerations of man-machine interfaces but few consider non-technical (e.g. organisational) interfaces.

This paper examines a new approach to systematically identifying, assessing and managing non-technical interface risks.

The emphasis of the approach is on bringing both parties together to work jointly to manage the interface risks. As a result there is a far better understanding and agreement on:

1. What the interface is.
2. What the risks at the interface are.
3. How big the risks are.
4. What actions need to be taken by each party to manage each risk.

The approach has been applied successfully by a number of clients in the UK and abroad including a high speed rail project, the Highways Agency and a multinational manufacturing company.

INTRODUCTION

The Oxford Dictionaries define interface as *"a point where two systems, subjects, organizations, etc. meet and interact."* [1] We can, for example, think of interfaces in terms of:

- A system (e.g. ETCS[1]) is formed of a number of sub-systems (e.g. Radio Block Centre (RBC), Eurobalise, GSM-R, on-board computer, cab display), each of which is made from a number of components.
- User interface or man-machine interface, where a person interacts with a machine or piece of equipment.
- Different departments in an organisation, for example operation, maintenance, safety, human resources, finance, procurement etc.
- A project that is made up of a number of sub-projects or workstreams, for example hardware development and software development or civil engineering and structures, tunnelling, signalling, electricity supply and distribution.
- A corporate centre and individual business units or markets.
- A company with its customers, suppliers, owners (e.g. shareholders) and regulators.

[1] European Train Control System

Interfaces are important because they are everywhere. However, interfaces can be a problem, for example because responsibilities are not clearly defined, the exchange of information is not smooth or different parties have different incentives affecting their behaviour towards managing interface risks.

Current approaches for managing safety risks at interfaces often only consider technical aspects especially the interaction between systems or sub-systems. Some include considerations of man-machine interfaces but few consider organisational interfaces.

For example, MIL Standard 882 requires the creation of a System Safety Programme Plan (SSPP). This requires defining "*the safety interfaces between each associate contractor and subcontractor (and suppliers and vendors as applicable), e.g. integrating hazard analyses"*. Preliminary Hazard Analysis (PHA), carried out as part of the safety analysis, *"shall identify hazards by considering the potential contribution to subsystem or system mishaps from"* … *"Interface considerations to other systems when in a network or System-of-Systems (SoS) architecture."* System Hazard Analysis (SHA) is carried out *"to identify previously unidentified hazards associated with the subsystem interfaces and faults"* … *"including software and subsystem and human interfaces."* [2]

The terms of reference for the NATO Research and Technology Organisation (NATO RTO) report 'Validation, verification and certification of embedded systems' states as one of its specific goals: Interface testing techniques for embedded systems which could include both specialized and Commercial-Off-The-Shelf (COTS) components. In addition chapter 4.5 of the report considers Man Machine Interfaces. [3]

The Common Safety Method (CSM) on risk evaluation and assessment states that *"particular attention should be paid to risk management at the interfaces between the actors which are involved in the application of this Regulation."* Interfaces are defined as *"all points of interaction during a system or subsystem life-cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks."* Annex I of the regulation states that *"for each interface relevant to the system under assessment … the rail-sector actors concerned shall cooperate in order to identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces".* [4]

The NASA Risk Management Handbook describes two complementary processes, integrated into a single coherent framework, in order to foster proactive risk management - Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM). *"The RIDM process addresses the risk-informed selection of decision alternatives to assure effective approaches to achieving objectives." "The CRM process addresses implementation of the selected alternative to assure that requirements are met."*

"Throughout the RIDM process, interactions take place between the stakeholders, the risk analysts, the Subject Matter Experts (SMEs), the Technical Authorities, and the decision-maker to ensure that objectives, values, and knowledge are properly integrated and communicated into the deliberations that inform the decision."

The RIDM process requires that within each unit the interfaces with the unit(s) at the next higher and lower levels in the organizational hierarchy are considered (e.g. when negotiating objectives and establishing performance requirements), as well as with its own unit's CRM process. [5]

Non-technical interfaces, such as those between two organisations, different departments within an organisation, two projects or a number of workstreams within a project are often not systematically analysed for their safety risks. Therefore, risk management approaches need to be extended to these non-technical interfaces.

But current risk management approaches, as well as the attitudes and behaviours of key players at such interfaces, are often not well suited to identify, assess and manage safety risks at interfaces. Each party is typically only looking at their own 'patch' and, more often than not, blaming the other side if something goes wrong.

This paper examines a new approach to systematically identifying, assessing and managing non-technical interface risks. The approach has been applied successfully by a number of clients in the UK and abroad including a high speed rail project, the Highways Agency and a multinational manufacturing company.

AN APPROACH TO MANAGING INTERFACE RISKS

The aim of the approach is to turn a typical attitude and behaviour of 'blame the other side' when something goes wrong into a culture of taking joint responsibility for understanding and successfully managing safety risks at interfaces. The emphasis of the approach is on bringing both parties together to work jointly to manage the interface risks. As a result there is a far better understanding and agreement on:

1. What the interface is.
2. What the risks at the interface are.
3. How big the risks are.
4. What actions need to be taken by each party to manage each risk.

1. Understanding the interface

The first step of the approach is to clearly define and describe the interface between two parties. This sounds obvious but is often not done or done poorly. This first step is therefore not only important in terms of forming the basis for a sound risk assessment but also in terms of developing a culture of shared understanding and action between the parties. It can provide an important turning point in the relationship of the two parties and the behaviours and attitudes of individuals on both sides. Finger-pointing and blaming each other for problems that occur (such as accidents, quality problems, delays or cost overruns) make way for jointly identifying potential risks that may occur and how to best address them (before they become problems).

Interfaces can be of many types, for example hardware, software, requirements, specifications, Validation & Verification (V&V) plans etc. There are many ways of describing the interfaces between two (or more) parties and the parties need to decide the most suitable representation on a case-by-case basis. The interfaces could be described in form of a list or table that lists the key flows or deliveries going across the interface or it could be a flow diagram or other graphical representation. Below is an example from an interface between two projects that is structured around already existing meetings that take place between the two projects.

Engineering meetings interface	Coordination meetings interface	Planning meetings interface	Other interface
■ Technical solutions for feature fulfillment ■ Software (SW) ■ Hardware (HW) ■ V&V plan fulfillment – Uptime – Material deliveries (maturity of the material as one parameter) – Reliability growth rate (Problem solving speed, verification fulfillment) – Changes on Engine side --> leading to changes vehicle side	■ Feature fulfillment ■ Feature balancing ■ Business impact	■ Vehicle to Powertrain: Material order from vehicle project of Engine/transmission deliveries ■ Priority of vehicles in the common plan ■ Vehicle to Powertrain: SW status on the truck to the engine ■ SW delivery plan, who is developing the SW? – Right SW in the right time for the right purpose is a key interface. The people working with the planning are stuck in short term firefighting ■ V&V for different engine types	Define the interface in terms of: ■ Quality & Features (technical aspects) ■ Delivery (timing) ■ Costs (product/project) ■ Managerial (control)

Figure 1: Example interface definition based on existing meeting structure between two projects

2. Identifying interface risks

There are two main approaches that can be taken to identify interface risks:

1. Bringing the parties together to identify the risks at their interface jointly.
2. Working with each party separately.

In the first approach the parties that share an interface are brought together either physically in one meeting room or virtually via conference call and net-meeting.

The approach used for identifying interface risks is based the HAZOP[2] study technique and using Guidewords. HAZOP is an especially powerful technique for analysing interfaces. [6,7,8,9]

The approach consists of:

- Defining a set of guidewords to identify interface risks.
- Applying the guidewords systematically to the interface (as defined in the first step) to identify potential risks at the interface.
- Recording the risks in a risk register.

[2] Hazard and Operability

Guidewords used in the approach cover, for example, timing, information, material, activity:

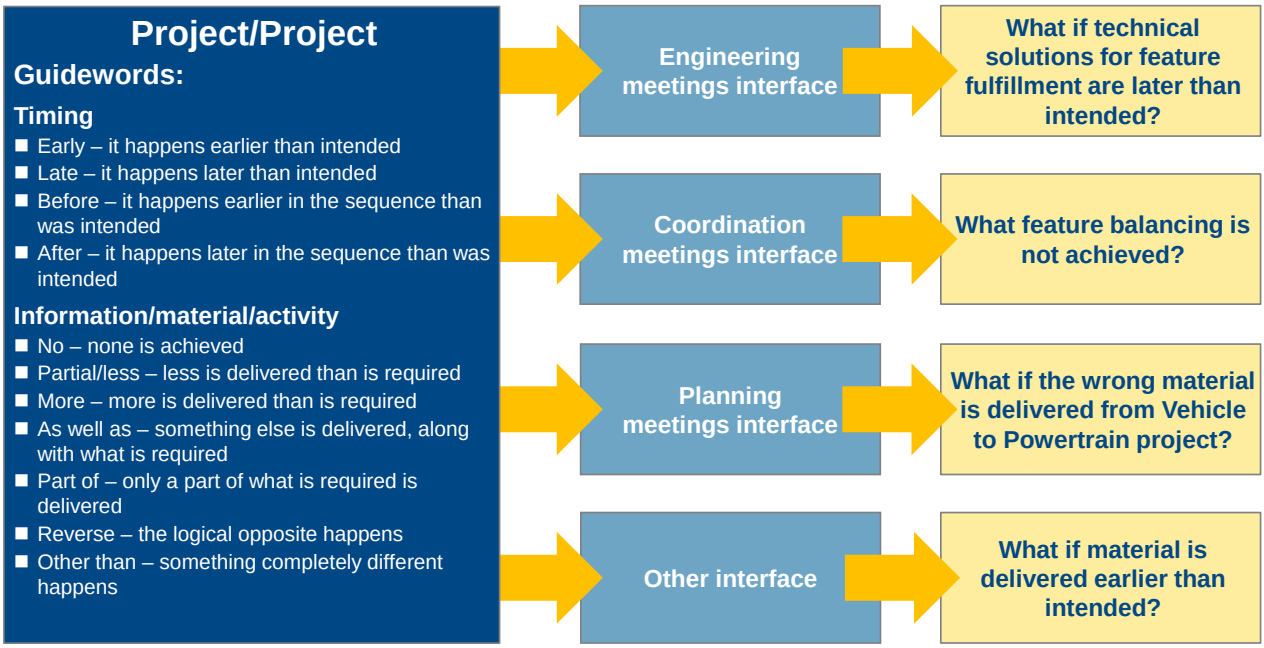

Figure 2: Example guidewords for interface risk analysis

If we identify 'Software' as a delivery at the interface between two projects, applying the guidewords we would, for example, ask:

Timing:

- What risks can we identify if the software is delivered early?
- What risks can we identify if the software is delivered late?
- What risks can we identify if the software is delivered in a different sequence than planned, e.g. package Y is delivered before package X?

Information/material/activity:

- What is the risk if the software is not delivered?
- What is the risk if only part of the software is delivered?
- What if more functionality is delivered than was expected?
- What is the software delivered has features that are not required?
- What is the risk of the software delivered is completely different from that planned?

It should be noted that not every guide word will make sense for each element of the interface, but the guidewords have been developed over many years to represent a good list of the failure modes of an interface so can be used to trigger thoughts about possible interface risks.

For one project we identified forty risks during a workshop using this approach. Thirty of the risks were new and were not already listed in the existing risk registers of either party involved at the interface.

The second approach is appropriate if there is a danger that the parties would not work openly and constructively together, particularly where three or more parties are involved. This is something we experienced on another project where in a first joint workshop the parties would either not mention risks they knew existed or they would engage in blaming and accusing each other for things that had already happened or could happen.

In these circumstances, it is best to talk to each party separately. Each party is asked separately about the risks they see at the interface – the risks that their activities could cause others and the risks they think others are causing them. The identified risks are consolidated and entered into a risk register. In this approach it is important to preserve anonymity, i.e. you don't tell party A which risks were brought up by party B, which by C and which by D. The focus should be on agreeing that there is a risk and that it needs to be managed.

3. Assessing interface risks

In the third step the identified interface risks are assessed. Typical methods for assessing the likelihood and impact can be used, for example risk ranking matrices.

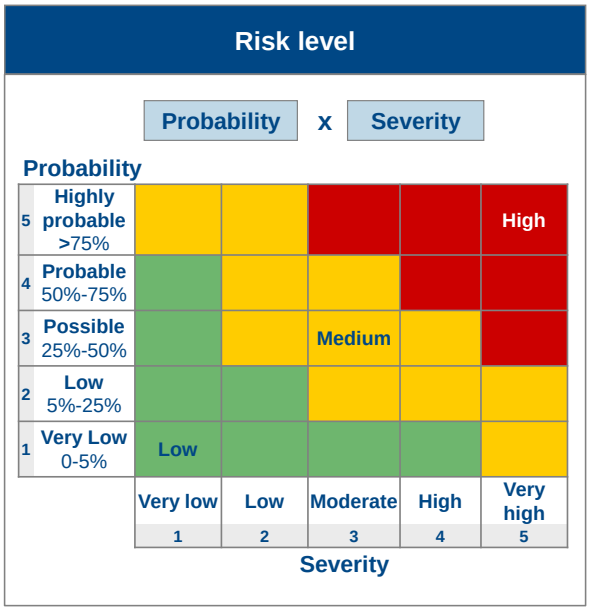

Figure 3: Example risk ranking matrix

4. Taking action to manage interface risks

In the fourth step action plans are developed to mitigate the risks. One of the main challenges with interface risks is that the direct control of a risk can often not be attributed to one party alone or the party affected by the consequences of the risk is not the same party that causes (and often controls) the risk.

Therefore, actions to mitigate the identified risks need to be developed jointly by the parties and agreed. Each action should be conducted by the party that is best placed to take it. For each risk and action a Single Point of Accountability (SPA) should be nominated. The risk SPA is accountable that the risk is effectively managed – through one or several actions. The risk SPA does not need to be accountable for, or indeed carry out, all the actions, but he needs to make sure that the agreed actions are completed on time. The SPA should typically be a senior person, such as a department head, to provide sufficient focus and visibility. For actions the SPA can delegate responsibility for completing the action (e.g. to a person in his department or team) but remains accountable that the action is completed.

This approach provides clarity and accountability for all sides as to who needs to do what by when to mitigate a specific risk.

Note that for one risk more than one action may be identified or that one action may mitigate two or more risks.

Finally, the implementation of the actions needs to be monitored to check that they are being done and have the desired effect in mitigating the risk.

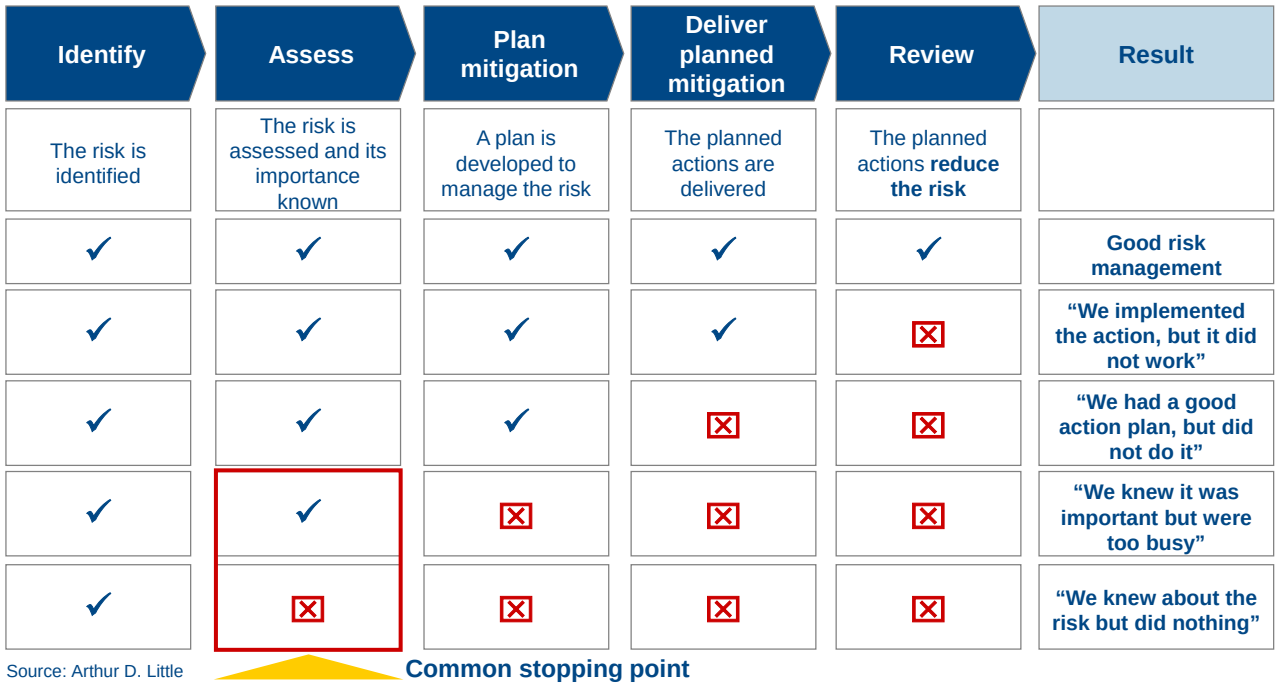

Figure 4: Good risk management does not stop once risks have been identified and assessed – it makes sure risks are managed

CONCLUSION

Interfaces are important because they are everywhere. However, current approaches for managing safety risks at interfaces often only consider technical aspects and whilst some include considerations of man-machine interfaces few consider non-technical (e.g. organisational) interfaces.

This paper proposes a new approach to systematically identifying, assessing and managing non-technical interface risks. The emphasis of the approach is on bringing both parties together to work jointly to manage the interface risks. As a result there is a far better understanding and agreement on:

1. What the interface is.
2. What the risks at the interface are.
3. How big the risks are.
4. What actions need to be taken by each party to manage each risk.

Core to the approach used for identifying interface risks is a HAZOP style assessment using Guidewords. HAZOP is an especially powerful technique for analysing interfaces. The paper also proposes a framework for managing the identified risks to make sure they actually reduce risk – an area often overlooked or conducted poorly in many organisations.

The approach outlined in this paper has been applied successfully by a number of clients in the UK and abroad including a high speed rail project, the Highways Agency and a multinational manufacturing company.

REFERENCES

[1] http://oxforddictionaries.com/

[2] Department of Defence standard practice system safety, MIL-STD-882E, 11 May 2012

[3] North Atlantic Treaty Organisation, RTO technical report TR-IST-027, Validation, verification and certification, of embedded systems, published October 2005

[4] Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council

[5] NASA Risk management handbook pre-decisional first draft, NASA/SP-2011-XXX, Version 1.0, XXXXX 2011

[6] Catmur J, Chudleigh M, Redmill F, System safety: HAZOP and software HAZOP (Hardback, 1999)

[7] Kletz T, Hazop and Hazan – Identifying and assessing process industry hazards, 4th edition, IChemE, 1999

[8] Chemical Industries Association, A guide to hazard and operability studies, 1990

[9] Kletz T, Hazop and Hazan, Notes on the identification and assessment of hazards, loss prevention, The Institution of Chemical Engineers Information Exchange Scheme, Hazard workshop modules