



HAL
open science

Organisational resilience at the limit: projects integrating new technologies in complex operational systems

Stéphanie Tillement, Thomas Reverdy, Céline Cholez

► To cite this version:

Stéphanie Tillement, Thomas Reverdy, Céline Cholez. Organisational resilience at the limit: projects integrating new technologies in complex operational systems. *New Institutionalism. European Group on Organization Studies (EGOS) Workshop, Jul 2008, Amsterdam, Netherlands.* halshs-00347767

HAL Id: halshs-00347767

<https://shs.hal.science/halshs-00347767>

Submitted on 16 Dec 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Organisational resilience at the limit: projects integrating new technologies in complex operational systems

Sub-theme 29: Risky Organizations and the Organization of Risk Management
24th EGOS colloquium

Authors:

Stéphanie Tillement
PhD Student, PACTE
stillement@yahoo.fr

Thomas Reverdy
Assistant Prof. PACTE
thomas.reverdy@upmf-grenoble.fr

Céline Cholez
Assistant Prof. PACTE
Celine.cholez@upmf-grenoble.fr

*This research was supported by the **Foundation for an Industrial Safety Culture (FonCSI)**.*

Introduction

The concept of “organisational resilience” stirs real interest amongst risk management researchers. It is derived from the generalisation of the concept of resilience in psychology, referring to “a fundamental quality of individuals, groups, organizations and systems as a whole to respond productively to a significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behaviour” (Horne and Orr, 1998).

The concept of “organisational resilience” recognises that risk control depends on the capacity of an organisation to take account of “irregular variations, disruptions and degradation of expected working conditions” (Hollnagel, Leveson and Woods, 2005, Woods 2005), or the organisation’s skills in « managing the unexpected » (Weick and Sutcliff, 2001). Thus, “a high reliability organization is one that exhibits resilience, among other qualities, in the face of unanticipated occurrences” (Kendra and Wachtendorf, 2003). The “resilient organisation” works a bit like a reed in bad weather: it bends but doesn’t break, whilst a tree, which is more rigid, would have broken. It is possible to register several degrees of resilience according to the definition that we give to “unexpected occurrences”: they may be unforeseen aspects of the activity (Hollnagel, Leveson and Woods, 2005), unexpected situations or a major crisis affecting the organisation, including an element of trauma (Kendra and Wachtendorf, 2003). Capacities which count for resilience are generally those associated with forward planning, perception and reaction to variations (Hollnagel, Leveson and Woods, 2005), the ability to interpret events, manage complexities, improvise, redefine roles, immediately correct errors and learn from them (Weick and Sutcliff, 2001). Resilience also uses redundant resources, “organisational slack” (Woods, 2005) and the redistribution

of technical competences within the organisation on account, amongst other things, of the mobility of its people (Kendra and Wachtendorf, 2003).

Our paper proposes discussion of organisational resilience in the case of a project to add a new automation system to highly reliable, complex operational systems. Adding new technology to an existing system generally poses unexpected interface and technical complexity problems which can have different types of impacts which can disorganise a project. Furthermore, the automation introduced new tight couplings (Perrow, 1986), bringing unexpected sequences and interactions, potential sources of major dysfunction (Perrow, 1999, Wolf and Berniker, 1999).

The combination of technologies introduces numerous unforeseen technical outcomes into the design activity. These technical outcomes and their resolution can take on unexpected proportions, both in terms of complexity and number and, in turn, lead to a variety of uncertainties. Atkinson et al. (2006) categorise uncertainties in projects into three groups: "uncertainty associated with estimating" (lack of experience in a given area, unclear specifications, interdependency between activities, unexpected occurrences during the project), "uncertainty associated with projects parties" (motivation of different parties, perception of objectives and risks, the skills of each party), "uncertainty associated with the stages in the project life-cycle" (design changes, planning changes). The more complex the system combining existing and new technologies, the more complex the design and development work will be: designers realise that there are incompatibilities between their design choices once the project has begun, trials show that the expected level of performance is not being achieved, unexpected outcomes will propagate from team to team in an unexpected manner (Aggeri, Segrestin, 2002).

The coordination of tasks and project members is subject to permanent readjustments "because the numerous interconnected and sequential tasks involved in the project will not automatically organise themselves into appropriate action and time sequences" (Strauss, 1985). Unexpected outcomes disrupt the work of teams (Atkinson et al, 2006) and provoke work overloads which are difficult to manage safely within the project's deadline and resource limitations.

This coordination is based on formal mechanisms but also on informal exchanges which allow the work to be organised (Strauss, 1985). During the project, the different actors negotiate, persuade, make arrangements and more or less "tacit understandings" in order to rank priorities, resolve time-related conflicts and finally construct a "negotiated order" (Strauss, 1988). Negotiations will encompass the meanings of actors, their tasks, responsibilities, obligations, commitments, conceptual structures and time-related issues (Hampson and Junor, 2005). This is not decided in advance and in a vast project organisation, coordination can be severely affected by the division of work, the tendency to depersonalise relationships as well as physical distance or competition between occupational groups. Ethnographic studies (Star, 1989; Wenger, 1998; Strauss, 1988) have clearly shown the extent to which cooperation between members belonging to different "social worlds" or "communities of practice" can be difficult and will substantially influence the direction a project takes.

Several of the origins of these tensions and “misunderstandings” have been identified: a high degree of bureaucratic partitioning; highly specialised knowledge which is difficult to transfer (Carlile, 2004); spatial difference (Metiu, 2004); the lack of shared objectives and meanings (Star, 1989); the existence of divergent interests (Metiu, 2004); identity-related issues (Wenger, 2003; Mork and ali. 2008). A substantial body of literature has advanced ways in which differences can be overcome, notably through the construction of artefacts or boundary objects (Star, 1989; Carlile, 2004). But as Mork and ali (2008) emphasise, the analysis of “discontinuities between occupational communities” and their impact on projects still has a lot to teach us. Technological innovation projects can lead to redefinitions of occupational territories (Abbott, 1988; Mork and ali, 2008; Bechky, 2002) questioning roles, identities and statuses of certain groups within the organisation (Metiu, 2004), leading to deliberate obstacles to cooperation (development of opacity, intra-organisational competition), obstacles in the management of unforeseen outcomes and absence of formal and informal regulation between the different teams.

We have carried out an in-depth analysis of several major incidents caused by errors made during technical modifications to a operating rail system as part of a major modernisation project. An ethnographical study at the heart of this project organisation has allowed us to consolidate our analysis of organisational factors which degrade reliability. The situations are particularly critical because the modernisation project – and in this case, automation – concerns infrastructures which are used each day for passenger transport.

Modifications are progressively introduced during operational downtime, in other words at night, and the infrastructure has to be working again next morning, with maximum reliability.

Guaranteeing the reliability of a given project organisation would require increasing that organisation’s ability to adapt to unforeseen outcomes, in other words, its capacity for resilience. But, referring to the notion of resilience for project organisation carries with it a high degree of ambiguity. Indeed, this notion encourages adaptation capacities: “by making critical adjustments in a timely manner, business organizations are better able to manage the unexpected” (Weick, 2001). However, it does not really question the limits to adaptation and the maximum pressure of unforeseen outcomes that a project or team can handle without degrading reliability. We might ask the question as to whether there is not an acceptable level of unforeseen outcomes beyond which resilience is no longer present, exposing the project to risks of error or technical dysfunctions which result in deviation from reliability objectives. What is true for a project is even more so for the different teams working within it. To what extent is the flexibility shared and negotiated? Is it based on regular re-framing exchanges between the teams? Insisting too much on reactivity within a project brings with it the risk of encouraging certain teams to accept an excessive workload and short-circuiting formal or informal redundancies which, until now, allowed them to guarantee the high level of security required. Guaranteeing the reliability of a project organisation would therefore mean preventing, limiting or regulating unforeseen outcomes that each team within the project would be required and able to absorb and thus avoiding deviances (Vaughan, 1999) towards an excessive acceptance of unforeseen outcomes that it would not be able to manage.

The context: a project for the automation of existing equipment

The rail transport company where this research was carried out is currently undergoing a major equipment renewal phase. The equipment has aged, in particular on account of much heavier traffic than planned and, in some cases, even become obsolete. In some cases, very substantial modernisation works have been decided. Also, a serious accident - a derailment 10 or so years ago - showed the urgency of pushing ahead with renewal.

This gave rise to a concomitant launch of several major projects affecting more than half of the network's lines, designed to provide a safer but also more efficient transport system, whilst reducing the intervals between trains to increase transport capacity.

These projects target primarily the automation of train-driving systems. This means replacing old automation systems by new, computerised ones. In order to ensure efficient, completely safe services, these new automation systems are interfaced with large amounts of older equipment, such as electro-mechanical signalling equipment (detection of trains and information from the control room and from other drivers, etc....).

A very large diversity of technical skills in play

The need to manage numerous automation projects at once led to the creation of a new engineering unit bringing together skill sets which, until then, had been dispersed: automation engineers, signalling engineers and railway engineers. Project teams were created, made up solely of automation engineers; they took over project management, including budgets and the deadlines, piloting sub-contractors and development of the project and work with signalling engineering and rail engineering departments. These departments are structured by functions which correspond to the different project phases: specification design, testing and implementation. Thus, the project organisation is required to work with a dual segmentation of tasks; segmentation by technical field (automation, electro-mechanics, etc...) and functional segmentation within.

The project is divided up into different stages which can run sequentially or in concomitantly. This temporal organisation is included in the schedule formalised by the project team.

Considerable economic, technical and safety issues

These projects include many challenges for the company investigated: they represent major budgets and it is difficult to extend deadlines beyond the dates initially fixed. They engage new technologies which have not always yet been designed and have never previously been in operation. The project team cannot really depend on any real past experience, and not all can be defined or planned beforehand, which makes scheduling very difficult.

However, modifying equipment dedicated to safety presents two key risks: technical incoherence and error. There is a risk of technical incoherence on account of the technical interfaces involved: between signalling and automation or between signalling engineering and contractors. It is important to ensure that the modifications are inter-compatible and that a modification to one part of the system will not compromise the operation of another. Coordination between technical specialities is therefore crucial in order to prevent this sort of risk. There is also a risk of errors, both in terms of design (an error which has slipped into the drawings) and implementation (cabling errors, for example).

The conditions under which these modifications are implemented increase the risks associated with those operations. In this case, work on existing installations which are actually in operation. The phasing of operations is therefore very important: throughout the period of the project (several years), partial modifications will be made almost nightly, to very tight deadlines (between 3 and 4 hours), tested and checked before services start up again at 5 o'clock in the morning. After the works, the system must therefore be perfectly safe, but also ready for operation. Several technical configurations (old and new) will coexist during relatively long periods and that must not impact operations: the trains continue to carry passengers.

Incidents

In the night of February 14th to 15th 2006¹, modification works to signalling equipment were carried out at station "X" on the red line. The objective was to run installation tests on a new switching system, involving a change in the signalling logic: it meant checking that the signals matched with the position of the switch (left or right) i.e. that they pointed the train in the right direction. During the whole of the night, the workers had to deal with different dysfunctions which they managed to solve. At 4.35am the trials were completed. At 4.55am the equipment and workers returned to the station: no-one was now on the tracks. At 5.10am, the final tests were carried out remotely, from the station: the situation was considered normal. At 5.45am, the workers, who were still in the station, were informed of a problem with the switch signal: the signal was green and therefore the driver was authorised to go through it, even though he would be going in the wrong direction. The workers return immediately to the signal and observed an oversight in the reopening of the electrical supply controlling the signal, i.e. the system was still in project configuration. After corrective work, a further test was carried out: the situation was now normal, and the workers left the station. The green signal authorised the driver to go onto a track where another train was stationary. A train crash was narrowly avoided !

In the night of April 17th to 18th, works and tests were carried out at station "Y" on the red line. Only sub-contractors were present and the modifications carried out were considered minor and without any operational incidence. This work was completed during the night of April 18th to 19th. At 6am, after the test passage of two trains (to ensure that no anomalies occurred), as required by the regulations, the sub-contractors called the company to inform them of the post-work situation. The conclusion was clear: "nothing to report". At 11.16am, the signalling engineering group was informed of a signalling anomaly at station "Y", which suggested an "absence": the train at the station disappeared, virtually: it was no longer electrically detected and therefore the signals intended to protect it stayed green and the central control tower did not see them. There was nothing to stop a train positioned behind it from moving forward ... and hitting the "ghost train". The seriousness of the situation was assessed immediately and all traffic was stopped. The work carried out on the previous nights was thought to be the root cause. The signalling project manager responsible for this operation went to the area in which the dysfunction happened and informed the sub-contractor of the situation, who also turned up at the site. Together, they checked all the

¹ For reasons of confidentiality, the dates of the incidents as well as their locations have been modified. However, the intervals between these incidents have been respected.

plans concerning the modification carried out the previous nights: they then realise that this modification had a functional impact on signalling logic which was not spotted at the time of the design and verification process. They therefore made modifications to the equipment to secure zone temporarily. At 3.25pm, the situation was back to normal: traffic could re-start. The signalling workers had to review all the designs in order to secure this zone on a permanent basis. Once again, a train crash was only just averted, and traffic was stopped for 4 hours.

These two incidents were particularly serious and occurred just several months apart. The signalling engineering team was shaken by the sequence of events and questioned its capacity to control the risks linked to modifications being carried out on a very large number of points on the network. The fallout went beyond this occupational community: the directors of the technical and operating units demanded explanations. Enquiries were launched, workers held responsible and possible sanctions mentioned. It is in this context that our research work begins.

These incidents attract our attention from a number of angles. They are all linked to works to modify signalling equipment which are part of these vast projects to which we referred. The first incident shows a lack of vigilance of the modification operations and a certain weariness of designers-checkers. The second incident is more to do with design, typical of a complex system: the modification carried out had unexpected impacts on other systems.

Very quickly, an initial causal analysis brought to light the fact that the incidents occurred in a high-pressure production context particularly due to the deadlines of the different projects. The formal validation processes for the design and implementation plans, based on dual controls (i.e. organisational redundancy), would appear not to have ensured the reliability of the operations carried out on those nights. Finally, the workers involved in these incidents were mostly experienced and considered highly competent within their own occupational community.

Research methodology

So as to address organisational resilience, it is important to understand where the “unexpected occurrences” came from and how they were addressed by the different members of a socially-organised unit (Vaughan, 1999). The mistakes, misconducts or disasters were produced within and by the organisation (Vaughan, 1999), and therefore our attention is drawn to the characteristics of the organisation itself both in terms of structure and process or indeed tasks: organisation redundancy, formalisation, centralisation or decentralisation, occupational groups (Vaughan, 1997).

In the case in point, it is important to understand in detail the organisation of a project. As Strauss points out (1988), “the organisation of the project influences the probability that disruption interactional alignment² will occur and affects the severity, the duration, the strategies used to overcome it and the impact on other aspects of project work”. In other words, the organisation of a project impacts the degree of organisational resilience, i.e. the

² Process by which workers fit together their respective work-related actions (Corpin and Strauss, 1988).

capacity of actors to bounce back, faced with unexpected occurrences, and get back to a state of equilibrium.

So as to carry out our research effectively, we started by listening to feedback and other incident reports and analyses so as to familiarise ourselves with the analysis and event processing methodology used by the organisation in question. We also wanted to understand what the analysis involved, with whom the results were shared, what the attitude of the organisation – and its management in particular – was in relation to these incidents. Finally, we were given access to the causes identified by the actors of the organisation themselves.

We then carried out 50 or so interviews which were recorded and transcribed with the different parties involved in the project: members of the project team, two contractors, the signalling engineering department (engineers or technicians, including the head of this group, supervisors, verifiers and designers) and those working on the tracks (engineers or technicians). These interviews were then subject to in-depth analysis: we were looking to identify the themes cited from within the different technical specialities, identify any divergences in the way in which these themes were addressed and finally, associate the two. Extracts of interviews illustrating the aspects cited by the different technical specialities are presented in the results.

We began by talking to the signalling engineering team. In these interviews, we questioned the actors about the activities involved in their daily work, the different tasks that they had to accomplish and the way in which they went about doing so. We completed these interviews with field observation. This provided us with precious information on the way the work was actually done, on the contingencies which could disrupt working activities, but also on key actors who bear much of the burden of managing unexpected occurrences.

Rail signalling engineering has always been the case that they play a crucial role in rail safety: the team is not just an appendix to the system. Thus, studying the working activities of “signalling engineering” workers gives us crucial insight into how risks are perceived and controlled at their level, within the framework of their tasks, but also how these risks are assessed and negotiated with the other working groups, i.e. the project teams which set system characteristics, budgets and schedules.

We then worked our way up the modification request chain, up to the members of the project teams. With them, our questions primarily concerned the existing organisation, the formally defined roles of the different individuals and the documents which accompany their work activities.

Our purpose was to identify whether negotiations and adjustments of deadlines were routine or not, if the combination of events which had led to the dysfunctionings observed might be reproduced or not. It was also about examining whether the formal structures of the organisation (breaking off into teams, sub-contractor relations, different technical skills, etc...) made the adjustment processes easier or more difficult (A. Strauss, 1988) and participated in the propagation and transformation of constraints, allowed the solving of complex problems. We demonstrated the scope of organisational flexibility, but also

elements of rigidity and thus explained the accumulation of constraints in certain areas of the organisation.

Results

Degrading of “communities of practices” responsible for “older technologies” limits the overlapping of competences required to achieve reliability

Woods (2005) and Weick and Sutcliffe (2001) emphasise that the overlapping of competences is a contributor to an organisation's capacity for resilience. We shall examine how each technical speciality and, in particular, signalling engineering, functions as a “community of practices” (Wenger, 1998); overlapping of competencies, transfer of know-how, mutual aid and mutual control.

In theory, error-free, reliable signalling modification operations require a formal control process called “dual verification”. This means that any document (drawing, plan, specification, test logs) will be checked twice: once by a person from the group having created the document and a second time by a person from the group working downstream on the them in the modification chain. Thus, the design plan will be verified by a person from the implementation group, the implementation plan prepared by a sub-contractor will be checked by a person from the implementation group. Checks are documented in “opinion forms” in which any errors and modifications to be made to the document are entered. At the end of this process, the document is validated.

As defined formally, the two checks are supposedly independent, i.e. the actors are not supposed to have any exchange outside the opinion forms.

Once all the necessary documents have been validated, the work phase begins, during which the equipment is modified, followed by the test phase where checks are made to ensure the modifications allow the installations to function properly and safely.

Within the signalling engineers group there is a division of work between functions, mostly according to type of project (specifications, design, implementation). In terms of implementation, the activities are divided up between workers from the company and sub-contractors: some of the work is indeed sub-contracted, although a representative of the company will be present in a supervisory capacity.

Furthermore, signalling engineering requires very specific, very sophisticated skills. Apart from the technical signalling logic knowledge (electro-mechanical technology), it is very important to have a clear understanding of existing equipment and their specificities. The task also requires high capacities for concentration and vigilance (Vaughan, 1997), throughout the modification management process: verification of plans, cabling of equipment installed and technical tests. Teamwork therefore plays a crucial role in the development of “mindfulness” (Weick and Sutcliffe, 2001) throughout the modification management process.

“We need to have a different perspective because it is true that when we are involved in a project over many months, our objectivity is affected. Therefore, the fact of having an outsider taking a different perspective gives rise to auto-criticism. Finally, more or less all of us tend to end up putting objectivity back on the rails. It gets us to check with each other. For big projects, it’s crucial.”

Thus, the most experienced members have learnt to be sceptical of dual verification and test logs: it is not because there is dual verification that the design work is flawless. On account of this, nothing totally guarantees that the test log - created from implementation plans - contains no errors or covers absolutely every angle.

In the same way, formal documents (procedures, rail regulations) supply very little information on the precise nature of the tasks to be carried out on account of their very general nature. This is also explained by the fact that signalling equipment is not generic and therefore it is impossible to prescribe precise operating procedures. For each area of the network there is different equipment, depending on the network’s age, the equipment used, etc...Competence is based on a keen knowledge of different installations and the capacity to adapt to the associated specificities and risks.

So, in spite of the formal processes and division of work, we observe a certain level of flexibility, but also a relatively shared and coherent vision of the work to be done and methods to be used. On top of the formal double-check procedures, there are of course less formal forms of doubling up: each person involved, when they have the necessary skills, will, when they carry out their part of the task, re-check whether the previous task has been done correctly.

“This is unquestionably a relatively complicated area and when we are working alone, it is not easy. We need to be able to sound out those around us. There are areas like that where being alone is not a good thing. You need to be able to ask questions around you on areas which seem a little complex to us, where we may have difficulties... It’s good to be able to go and knock on someone’s door and get a different perspective”.

Whilst certain actors are formally entrusted with coordinating specific aspects of a project, they are far from being the only ones to play this coordination role. Everyone, more or less discretely, seeks to inter-connect the work, “hold together” its different aspects (Strauss, 1988). More than the formal dual verification procedure, risk control is primarily dependant upon adjustments, understandings and informal arrangements between signalling engineers, but also with sub-contractors doing signalling works. The designers will talk about plans face-to-face, or go onto the night shift with partially-modified documents, with the intention of checking certain points directly when they get to the site.

These adjustments also allow the construction of collective competencies. It is a fact that informal regulation encourages workers to exchange and talk about their problems and difficulties (within the occupational community) and divide out the tasks, depending on competencies, with each technician not necessarily having the same experience of the technology, or the same knowledge of the sections of track impacted by the modification... Faced with dead-ends, the technicians will talk to each other.

“When we have a problem, we go and see whether someone else has come across it or whether someone has an answer. Even if it’s someone who is not working on it, we can ask all the same. We manage our own activity, but we can ask questions if we have such-and-such a concern. (...) our offices are all close to each other and so, very often, when we come across a problem in our work, something which seems odd, somebody will say to us “yes...I’ve seen that, that happened to me”.

So, problems can “migrate” within the team, from the requester to the most experienced and the most competent member. We observe what Weick and Sutcliffe (2001) call “deference to expertise”, typical of Highly Reliable Organisations: it is the most competent person faced with the given problem at local level who is authorised to take a decision. This not only allows a solution to be found to the problem very possible, but also strengthens occupational group cohesion, and improves knowledge and practical know-how within the signalling team.

However, signalling engineering has undergone major changes in the make-up of its teams. With the arrival of young, less experienced technicians, a new division of work and competencies has arisen. Whilst before, the designers also piloted works, today this task is the responsibility of the project manager who sub-contracts implementation. The young engineers who have become the main interfaces between design and work do not have the same level of technical competencies and cannot understand and check the work of the designer-verifiers.

“People come and work here with their BTS (BAC +2 in electro-mechanics) and we let them loose on these projects; you have to believe me, it’s complicated ! It’s said that it takes between 5 and 10 years to understand signalling. And even after 20 years, we don’t know everything, and we can all make mistakes”.

“Training in the past was based on apprenticeship, and we had much more time; we could double people up take them to the work sites during the day, during the night. (...) but all that has gone and it’s a real pity, because that’s where we learnt the most”.

For major projects, the type of training favoured in the past (i.e. apprenticeship) has largely been abandoned on account of limited available resources. Young people only receive theoretical training and are sent onto projects as soon as possible. Finally, design and verification operations on plans are increasingly the domain of a handful of people (the most experienced). Thus, informal redundancy based on the overlapping of competencies between all workers no longer really exists. It is more a one-way counselling relationship from the “old hands” to the new arrivals. The more experienced members have few people to whom they can turn.

Also, the latter are given to the biggest and most complex projects. The danger is that they become swamped in the number of tasks to be carried out, lost under a pile of documents connected to the project. Indeed, with the projects, a certain “bureaucratical accountability” is developing (Vaughan, 1999): everything has to be written, tracked and signed, which sometimes leads the older workers to neglect technical tasks (such as the second, informal opinion that they expressed on all plans in the past).

This also leads to a change in the way regulations are obeyed. The more experienced workers, whilst recognising the importance of these rules – and traceability in particular –, do not have total confidence in them. They know how to get around them and make the most of their “practical” and “experienced-based” know-how (Vaughan, 1997), in particular given unexpected occurrences where formal documents do not serve much purpose. On the other hand, the younger workers seem to be very much attached to the regulations. Their philosophy is as follows: *“if I respect the rules, I will have done my utmost to avoid an incident”*. The same applies to test logs: the younger workers are incapable of referring to the electro-mechanical plans from which the test logs originate, and therefore are unarmed if mistakes have slipped into the trial logs.

“The flip-side of this formalisation is that people tend to hide behind documents. I don’t want to seem like an old warrior, but not so long ago, we worked mostly on the plans and people perhaps visualised the diagrams better.” (Signalling engineer).

Informal checking is therefore less systematic or less effective. The very thing that makes the team flexible and highly reliable is being challenged by the progressive diminishing of occupational competencies and all forms of redundancy. The team’s resilience is progressively declining. It would take just one major unexpected occurrence or exceptional workload for the team to start making mistakes and not be able to detect them.

The excess of unexpected modification requests and their non-negotiable nature resulted in fatigue for those who suffered them, which in turn made them less vigilant

The foundations of resilience, according to Weick and Sutcliffe (2001) are a “developing mindfulness” and a “preoccupation with failure”. Within a project, this preoccupation must be shared by all teams, but it must also be part of the project piloting practices which need to be attentive to warning signs which come from the various teams. So, this party is specifically interested in the way the project team (automation engineers) organises and shares out the workload between the teams (signalling engineers).

If we observe the many adjustments within the signalling engineering team, the same does not apply when we cross the “community of practice” border. Thus, between signalling engineering and the project team, negotiations, understandings - informal ones in particular - seem no longer to exist. There is a fault line between signalling and project, which compromises cooperation between them.

The data collected reveals that this absence of negotiation is partly due to competition between occupational territories. The introduction of new automation technology has led to a repositioning of the different professions. Indeed, in the previous technical system used to direct trains, signalling (electro-mechanical technology) was primarily responsible for averting major risks. Because of this, it had a central position within the overall system. With the onset of computerised systems, the automation engineers are now at the heart of the system.

As part of the project, the different technical specialities must adapt to automation technologies and make modifications to their own specialities accordingly. Project management has been entrusted to the automation engineers, who consider the other specialised team as service-providers working at their behest, according to needs generated through the development of automation systems, and without too much concern for the availability of resources.

At project level, between the automation engineers and other occupation groups, there is no regulation governing the number of requests, no negotiation on workload, no collective discussion on the best way of organising requests between them. The other groups are perceived by the automation engineers as the main causes of project delays and exert permanent pressure to ensure that their modification requests are processed.

(Concerning signalling engineering verification practices) "It's very slow, very slow. We go quicker than they do, they get us behind and that's why the dates I'm giving you keep getting postponed" (automation engineer).

And yet, as we saw previously, the prevention of risks by the signalling engineering team is based on various formal and informal redundancies. This practice is very sensitive to workload. The signalling engineers have to accept a work overload which will quickly erode the redundancies which, until now, guaranteed a high level of reliability (Wood, 2005).

"The guys that manage the schedules sometimes try to put pressure on by saying "when are you going to check it ?, when are you going to check it ?", and then, "go on then....when are you going to get down to it ?", but what they mean is "so....the IT people are waiting for them, contractually we need to do it", and the guys....I think they just feel great pressure... A bit of pressure is put on and that causes problems, because they want to shorten the schedules, and we don't have the input documents and we've got all these procedures which mean that.... It's just heavy going". (signalling engineer)

In principle, signalling engineering intervenes after control engineering on the basis of its specifications. However, on account of time constraints, operations can not be done sequentially: the signalling engineers have to anticipate and launch their studies with information and specifications which are often very approximate. They might make hypotheses on the way signalling will interface with new automation systems. However, these hypotheses are often called into question during the project, when knowledge on the automation part improves and the system evolves. This leads to constant returns to the design plans. But once launched, the signalling operations are very difficult to modify because each time, the whole dual verification process has to be re-done.

"What I'm saying is that generally what happens is that the project team know what they want, but they don't understand the constraints, so all these preliminary meetings which last over several years before we get any financing, are intended to wrap the project up in the finest detail... During this time, we have to work, but we still have no definitive solutions, let's say. It sure gets very complicated." (Signalling engineer)

The signalling team then has to take unreasonable risks, for example by doing only partial dual verifications. Informal redundancy does not allow to compensate the one for the other,

since each actor is focused on his part and doesn't have the time to worry about what his colleague is doing.

"No, but it all adds up, and it means we can't work calmly and it just doesn't help: the atmosphere is deteriorating. That's clear. And then you've got pressure and nerves and there's no way around it... someone who's working so many hours at night, who doesn't have much time to recuperate, at some point in time, if he's working all alone, there's a chance he is going to cock-up. Even for the schematic diagrams, we get to the crunch and we have to get documents together as quickly as we can and we do them as quickly as we can and they get handed in with loads of mistakes... that's just not right!" (signalling engineer)

Little by little, the adjustments are abandoned, whereas previously it was they that helped control risk, leading to a form of "organizational deviance" or "routine non-conformity" (Vaughan, 1999). This organisational deviance is produced or even encouraged by the organisation. The risks are perceived by the signalling engineers individually but they are not subject to a collective initiative.

Contrary to automation systems, a new and innovatory technology and therefore destined to evolve over time, signalling is considered traditional technology which is therefore controlled whatever the context. Signalling engineers cannot make the project teams understand the difficulties that they have in completing their tasks, and the risks that they have to take. This creates demotivation. Their occupational ethic is profoundly linked with controlling railway safety. But in the organisational context described, they say that they can no longer guarantee safety.

"What is getting really hard is this sort of political speak. In meetings, we say that security is the department's number one priority, but if you don't put the staff there to supervise the contractors, it just doesn't add up." (Signalling engineer)

Furthermore, for the signalling engineers, the accumulation of modification requests raises questions. It is a fact that the difficulties encountered by the automation engineers to programme their new system and interface it with existing equipment leads to non-justified emergencies or repetitive modifications which are perceived as incoherent by the signalling engineers.

"And sometimes we do stuff in a mad rush, but it turns out to be for nothing. Well, I say for nothing... We are asked to do it quickly and therefore we do it quickly and, at the end of the day, it's used or it's not used, but later...they've squeezed us and if we hadn't done it so quickly, it would have been better." (Signalling engineer)

"To tell you the truth, I've already had cases where you have had to speed things up... We were getting the test logs a bit late, normally I think it's 15 days minimum before the work begins, and sometimes we get them less than a week before. It's very commonplace, especially with small projects". (Signalling engineer)

The pressure exerted by the project managers on the signalling engineers, the many and incoherent requests bring about a sort of weariness and a feeling that the security issue is

not really shared within the organisation, and with that comes a degree of demotivation. This demotivation makes people less vigilant, both individually and collectively. Everybody goes into their corner and experience-sharing and problem-sharing, previously the real strength of the signalling team, become difficult.

The technological modernisation introduces new risk assessment and prevention techniques which worsen competition between occupational groups

Beyond tensions associated with project organisation, the survey looked at risk assessment and control techniques which have also changed dramatically with automation.

Until now, signalling technologies were at the heart of collision prevention. With automation, it is the IT system which is progressively taking collision prevention in hand. The computer system is tagged onto existing signalling equipment which provides information on train positions. In other words, in order to be perfectly reliable, the system must now combine three checks: proper functioning of signalling equipment already in place, the interface between signalling equipment and automation and the automation system itself. We have moved from a situation where the signalling engineers were the main actors in risk prevention to a situation where the responsibility is shared between automation engineers and signalling engineers. Let us examine in more detail the practices upon which risk prevention is based.

On the signalling engineers side, risk control is primarily based on the rigorous application of formalised design rules. There is no real prior risk analysis (in the AMDEC or operational security sense of the term): the risks are primarily identified on the ground, near to the equipment and in a very practical way. Designers, developers and checkers must adapt to the variable nature of situations and equipment in place (their ageing, etc...). The “subject matter”, the “technical object” in its “resistance” to human logic played a vital role here and many problems were solved on the ground and working with cables.

On the automation system side on the other hand, all safety analyses and all tests are carried out upstream, before they are actually installed on-site and, more often than not, using formal methods and simulator tests. On-site, the tests on the automation elements are monitored by supervisors. If the tests are not compliant with their test logs, they must attempt nothing on-site: in fact, they are not asked to think about the causes of these non-conformities. They just look at their results: it is up to the engineers to analyse them and to decide on any corrective action on the software.

So, the field phase during which the equipment is physically installed, is much less critical in automation systems than in signalling. On the software side, the tests carried out upstream during design ensure that the system is reliable: it is at this moment that the reliability of the software has to be checked. Once installed, improper cabling cannot lead to non-safety problems. In signalling engineering, on the other hand, the field phase is really critical: a single bad connection can trigger a non-safety incident.

“In signalling, it’s very delicate, because you have only got yourself to blame. There is no system above. We are in a signal box and it’s completely autonomous. If you get it wrong, there’s no system above us which will necessarily pick up the mistake. Whilst the software, with all the loops and redundancies built in, safety is more diffuse” (automation engineer).

The different interpretations of risk control crystallise the conflicts or at least the splits between these occupational groups. Signalling engineers practice is not understood by the automation engineers who criticise their deadlines and verification procedures.

“The problem with signalling engineering is that you have a specifier, a specification verifier, a designer, a design verifier, an implementer, an implementation verifier... So, to make a modification, it takes more or less a year. So, imagine the case of [this project] where there are several hundred modifications! We know it’s the key to success” (automation engineers).

With automation, a new form of risk has arisen: risks of technical incoherence and in particular with the interfaces between the automatic system and existing signalling equipment. These new risks are the subject of real concern both for automation engineers and signalling engineers.

Numerous modifications resulting from automation engineers’ demands mean that the signalling team has completely lost its overall vision of operations required of it, in particular the sequential splitting of modifications into more than one night. For example, an operation which was to be carried out one night may be cut up at the request of the project into two because further tasks have been added in the meantime.

Furthermore, signalling engineers reject the “traditional technology” label that the automation engineers give them: the environment in which signalling operates has become so complex that their operations cannot be qualified as “traditional” and “controlled”. The signalling engineers now have to deal with technologies that they do not understand.

“We are taking new IT systems on board...and we say, well signalling...we know that, so it’s not a problem. Except that signalling is understood in a given environment, but that environment is changing. And these environments... when we are reasoning no longer in signalling sub-systems but in overall systems, these other sub-systems have a direct impact on signalling and its functioning and there we have no experience...” (Signalling engineer)

“Currently, we are creating new stuff in signalling which has never been tried and tested which means we have no absolute guarantee on functional and safety aspects. But our bosses continue to consider that signalling is something that is known and controlled and that the guys know how it works. No, I’m sorry, we have changed environment and we are in the process of reinventing elements of signalling...and there, there is a real risk. And what’s sure is that they don’t understand that today. They just don’t understand”. (Signalling engineer)

The automation engineers on the other hand, criticise the signalling engineers for not taking an interest in new system risks, but focusing only on risks that are inherent to signalling, and by extension, on their risk-prevention methods.

“When they (the signalling engineers) validate their diagrams and all that, they’re not worried at all about system safety, they’re worried about obeying the rules listed in the signalling instructions and that’s all. And so the safety of the whole is based on the analyses of these instructions upstream. It is upstream that we need to take a hold of it because after, it is too late, and it takes time”. (Automation engineers)

In fact, these different interpretations of risk control reflect tensions between these “occupational groups” (Bechky, 2003). In the medium term, the signalling engineers are in danger of losing the “noble” part of their profession. As a project manager confided to us, *“the signalling engineers remind me of the Gauls in the Roman Empire”*. This metaphor perfectly illustrates what is going on between the two groups: the Gauls are indeed seen as an archaic community which are using old, or even obsolete, tools. The Romans are modernity, but also the invaders coming to conquer the Gauls’ land. In keeping with the metaphor, the signalling engineers are there to resist the automation system “invaders”.

One of the reasons that there is not really any shared representation of operations and therefore of risks, is that errors and difficulties encountered by signalling engineers are rarely fed back or discussed. Between the different occupational groups there is “structural secrecy”, a concept that Vaughan (1988) uses to understand why organisational deviance in a given group is not perceived by anyone outside the group. Secrecy is induced by the very structure of the organisation: division of work, hierarchy and physical distance segmentalise knowledge about objectives and tasks and make the actions of one part invisible from the other. Like the Gauls, the signalling engineers go off into their occupational corner and exchange less and less information with those from outside the group, and continue to pursue their own objectives (Metiu, 2004).

This is also explained by the rivalries between occupational groups, and more precisely between the group which delegates risk (here, the automation engineers) and that which actually takes that risk (the signalling engineering). He who delegates risk will also be quick to accuse the other group in case of mistakes. An informal standard within the colleague group will then come into being for fear that errors may be used by the others: errors are only discussed in your own occupational group because “the colleague group would consider that it alone fully understands the technical contingencies and that it should therefore be given the sole right to say when a mistake has been made” (Hughes, 1951). Of course, this creates opacity, which is primarily based on “the feeling that outsiders will never understand the full context of risk and contingency that makes colleagues so tight-lipped”.

So, the modernisation of equipment leads to a wholly paradoxical situation: occupation rivalry, exacerbated by different risk assessment practices, does not help us to understand new risks induced by technological hybridation. There is no “collective state of awareness” (Weick and Sutcliffe, 2001), which limits “continuous adjustments that prevent errors from accumulating and enlarging”. Each party has its own interpretation of risks, and the most appropriate means to control them, and ignores the particular situation of other actors involved in the project. Concerns are not shared between teams and each focuses on its own turf.

Reaction to incidents, in a tense atmosphere between occupational groups, increases organisational rigidity

Incidents observed (as described above) have really raised awareness amongst signalling engineers as to the shortcomings of risk control. This awareness has resulted in substantial investment in formalising feedback, detailing technical causes, errors and organisational causes. We wondered whether this awareness had only affected signalling engineers or whether it had affected the project as a whole. In other words, does this project organisation show any real capacity to manage its errors (Weick and Sutcliffe, 2001) beyond its internal occupational boundaries ?

The interviews we carried out with signalling engineers revealed an occupational community that has been severely shaken, and where the dominant feeling is one of fear.

“Personally, that’s what really got to me... retrospective fear. Because there, we focus on this incident, but we fiddle with the whole of the line and when we make modifications, it’s like that all the way down the line! You should see some workstations. It’s amazing what’s going on. So things like that... we’ve got dozens and dozens all the time... is what shocks people, retrospective fear, fear that one day, we’ll miss something which has some nasty consequences” (signalling engineer).

All of them had a sharp sense of the risks they were running, but also of the risks for projects and especially for future users. Incident cause analysis established limits to current practices within the signalling team, both in terms of test procedures and design verification.

“These trials are based on the competencies of the agents. After every operation, the workers wait for the first two trains to come through in each direction (in compliance with prevailing regulations).” (feedback).

“The trial log described the test for modifications on circuit number 1, but not modifications to the other circuits. The impact on the other circuits was not shown either during the trial log draft, nor during verifications, nor during field trials”. (feedback).

However, dysfunction cause analysis also pointed to project piloting, in particular the rate at which modification demands arrived and the deadlines imposed...

“This operation has been subject to successes modifications (studies completely reworked) at the request of the project. Respecting an evolving, tight schedule means slicing up interventions and increasing risks”. (feedback)

Successive delays in functional specifications at system level (automations) generate multiple phasings which require successive and partial reworks on studies that have already been done globally, to carry out trials in a context where pressure is on in terms of schedule”. (feedback)

When we talked to the project teams, on the contrary, we were struck by the little concern that these actors showed for such events: either they had never heard of them, or they had interpreted them as having no relationship with the project, except in a sense that they might delay it. In other words, the feedback which was limited to the signalling engineers' team did not lead to their questioning project management more globally.

Thus, the incidents were perceived very differently by the signalling team and the project team. These incidents are a strong indication for signalling engineers which show that time pressure and shifting constraints lead to dangerous situations. And this signal (Vaughan, 1997) was not heard or taken into account by the project teams which made no modification to their working methods.

Faced with this situation, the signalling engineering management team saw no other alternative to attempt to maintain safety and get the project teams to take their constraints into account than making their organisation more rigid through formalisation.

So, the signalling team made a choice of controlling their internal control and redundancy rules more strictly so as to avoid being confronted again with a situation where they may find themselves being held responsible. New procedures, such as impact analyses, were even created, which sought to analyse all the risks associated with a new modification, and tracking them.

The workers therefore did not deviate from the formal dual verification process. Further to the incidents, they collectively decided to abandon informal night verification and no longer to work under emergency conditions. They will no longer compromise to guarantee the delays at just any cost.

"We don't work last minute in this area, or....I should say, now I refuse to. I have always tried to get stuff out in time. Given what happened recently, I'm taking my time. It was a real wake-up call !" (signalling engineering)

They cite respect for the dual verification procedure (and the associated regulatory verification times) to justify any delays, and through this, try to reduce the number of modifications which progressively added to their workload.

Rigidification of design and verification practices is not without impact on the project: longer deadlines, worsening of the conflict between the project team and the signalling team, no in-depth dialogue on the risks of the new socio-technical system, etc... Negotiation with the project teams, in particular on resources, has not got any better. The question of deadlines is even more thorny and more inclined to worsen the conflicts than help to resolve them.

Recourse to strict application of procedures leads to rigidification. And rigidity can harm resilience (Woods, 2006), in the sense that it reduces a system's capacity to face up to unplanned events and to bounce back when under pressure: "rules – and whether to obey them or not – are part of an organisation's culture. Organisations create rules to ensure safety. But in practice, the rules themselves may create additional risks" (Vaughan, 1997).

Also, this strict respect for procedures leads to isolation of the different actors: there is less sharing of experience and the workers increasingly face problems alone.

Discussion

Our in-depth analysis took a new look at the organisational conditions of resilience in automation projects of a highly reliable technological system. Adding new technologies to existing ones generates numerous unanticipated modifications and the highly integrated nature of these technical systems makes the propagation of modifications worse. Furthermore, *“large accidents were in plants with high complexity and tight coupling and these characteristics were apparently heightened as a result of incremental growth through add-ons and technology patches to older systems”* (Perrow, 1999, Wolf and Berniker, 1999). In such a context, guaranteeing a high level of reliability is especially difficult and requires particularly “resilient” project organisation (Wood, 2005).

This case re-visits the organisational conditions of the resilience of such a project. First of all, it shows how, within a single community of practices - here signalling engineering - there is a fairly high resilience based on extensive social and epistemic cohesion. More detailed analysis nevertheless showed several latent sources (Perrow, 1996) of non-reliability, and greater division of work within the teams, with insufficient competence overlap.

By taking interest in interactions between teams within the project, our study shows that there are discontinuities between “communities of practices” (Mork and ali, 2008) which do not encourage coordination (Carlile, 2004). The existence of very specialised occupational groups in their technical areas is in opposition to one of the conditions of resilience: the redistribution of technical competencies in the organisation (Kendra and Wachtendorf, 2003).

Furthermore, because it redefines occupational territories (Abbott, 1988; Mork and ali, 2008; Bechky, 2002), questions roles, identities and status of certain groups within the organisation (Metiu, 2004), the automation project is challenged by deliberate obstacles to cooperation (development of opacity), “obstacles” to the management of unforeseen events, and an absence of informal regulation between the different teams. Low cooperation limits capacities for forward planning, perception and reaction to variations (Hollnagel, Leveson and Woods, 2005).

Tensions affect risk assessment directly: “divergence is aggravated if different parties also have different knowledge and perceptions of the nature of sources of uncertainty and different capabilities for managing them” (Atkinson et al., 2006). We observe divergence in the interpretation of events which do not encourage collaborative action (Weick and Sutcliffe, 2001). In such a conflictual context, piloting projects is to do with “classic command and control bureaucracy” described by Weick and Sutcliffe (2001), “that is adequate for a stable world, but too inflexible in times of change”.

So, all it took was for the workload to increase on the signalling engineering teams for the usual verifications to fall away. Internal flexibility of these teams ended up turning against them because of a lack of redundant resources, “organisational slack” (Wood, 2005): the

pressure exerted on them encouraged them to take excessive risks whilst they had been rendered more vulnerable in other areas.

For Perrow (1999) for example, “decentralized units are better able to handle the continual stream of small failures, forestalling the widespread, multiple failures”.

Continuing with the metaphor of the reed allows us to discuss the notion of resilience. We can imagine that the project organisation, like the structure of the reed, comprises zones of variable rigidity and variable fragility. In the same way that the strength of the wind hits the reed, the uncertainties of project management bear forces on the social organisation of the project, which are propagated by adjustments and which sometimes accumulate and lead to more pronounced distortion on certain teams from within the project. Some parts of the organisation, because they are more flexible than others, because they have less power than others, concentrate the pressure resulting from these uncertainties. These teams can have a certain capacity to manage contradictory demands, but an excess may result in them making errors. Resilience does not apply to the project as a whole.

The flexibility of part of the organisation maintains the illusion of resilience. Flexibility, the capacity to improvise, redefine roles, immediately correct errors and learn from them, sharing experiences and collective anticipation (Weick & Sutcliffe, 2001) do not work for the project as a whole. They are concentrated in those areas where constraints accumulate and the divide generated by the difficult combination between the rigidity of certain elements and the flexibility of others constitute a major risk factor. A resilient organisation is not an organisation which prevents adjustments but an organisation which can identify the circulation of adjustments within it, regulate that circulation, avoid substantial imbalance and ensure that the different links of the chain are capable of dealing with them.

References

- Abbott, A., *The System of Professions: An Essay on the Division of Expert Labor*. 452 p. 1988.
- Aggeri F., Segrestin B., « Comment concilier innovation et réduction des délais ? Quelques leçons tirées du développement de la Laguna II », *Gérer et Comprendre*, Mars 2002.
- Atkinson, R., L. Crawford, S. Ward, Fundamental uncertainties in projects in the scope of project management, *International Journal of Project Management*, 24: 687-698, 2006.
- BE Mork, M Aanestad, O Hanseth, M Grisot, Conflicting epistemic cultures and obstacles for learning across communities of practice, *Knowledge and Process Management*, Volume 15 Number 1 pp 12–23, 2008.
- Bechky, A. B., Object Lessons: Workplace Artifacts as Representations of Occupational Jurisdiction, *American Journal of Sociology*, Vol. 109 No 3: 720–52, November 2003.
- Bechky, A. B., Sharing Meaning Across Occupational Communities: The Transformation of Understanding on a Production Floor, *Organization Science*, Vol. 14, No. 3, pp. 312-330, May-June 2003.
- Glasner, B. G. and A.L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago, Illinois, Aldine, 1967.
- Heimann, L., Repeated failures in the management of High Risk Technologies, *European Management Journal*, Vol.23, n°1, February 2005.

Hollnagel, E., Woods, D. D. and Leveson, N., editors, Resilience Engineering: Concepts and Precepts. Brookfield, VT: Ashgate Publishing Company, 2005.

Horne, J.F. III., J.E. Orr, Assessing behaviors that create resilient organizations. *Employment Relations Today*, 24 (4): 29-39, 1998.

Hughes, E.C., Mistakes at work, *Can. J. Econ. Polit. Sci.* 17: 320-27, 1951.

Hughes, E.C., *The Sociological Eye: Selected Papers*, Chicago, Adline, 1971.

Metiu, Anca Maria (2004), "Escalation of Disengagement Across Distributed Groups: Ownership and Opacity", in: INSEAD Working Paper Series, Februar 2004.

Perrow, C., *Normal accidents*. Basic Books, New York, 1984.

Perrow, C., Organizing to reduce the vulnerabilities of complexity, *Journal of contingencies and crisis management*, Vol.7, n°3, September 1999.

Star L. S., Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39, *Social Studies of Science*, Vol. 19, No. 3, 387-420, 1989.

Strauss, A., The Articulation of Project Work: an organizational process, *The Sociological Quarterly*, Vol.29, n°2, 1988.

Strauss, A., Work and the division of labor, *The Sociological Quarterly*, Vol.26, n°1, 1985.

Vaughan, D., *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago: University of Chicago Press, 1996.

Vaughan, D., The dark side of organizations: Mistake, Misconduct , and Disaster, *Annu. Rev. Sociol.* 25: 271-305, 1999.

Vaughan, D., The Trickle-Down Effect: Policy decisions, risky work and the Challenger tragedy, *California Management Review*, Vol.39, n°2, 1997.

Weick, K. E., & Sutcliffe, K. M., *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Francisco: Jossey-Bass, 2001.

Wenger E., Communities of practice and social learning systems, In Nicolini D., Gherardi S., and Dvora Y. (eds) *Knowing in Organizations, A practice-based approach*, M.E Sharpe, pp. 76-100, 2003

Wolf, F. and E. Berniker,) *Validating Normal Accident Theory: Chemical Accidents, Fires and Explosions in Petroleum Refineries High Consequences Engineering Conference*. Sandia National Laboratories, Albuquerque, NM, USA, 1999.

Woods, Creating Foresight: lessons for Enhancing Resilience from Columbia, in Starbuck W.H., Farjoun M., eds, *Organization at the limit: lessons from the Columbia Disaster*, Blackwell, 2005.