Applying the Resilience Engineering and Management Perspective to Problems of Human Alarm Interaction in ATM

Simone Rozzi
School of Science and Technology
Middlesex University
London, Uk
simone.rozzi@gmail.com

***Abstract*—This paper puts the problem of poor human alarm interaction under the organizational perspective of Resilience Engineering and Management (REM) to explore the insights that such a perspective can bring. The article presents (i) a case study approach through which the REM perspective has been implemented, and (ii) a resulting qualitative framework of the organizational-systemic precursors to poor human alarm interaction in Air Traffic Management (ATM). The REM perspective has been useful in outlining a set of organizational-systemic dynamics located at the blunt end of the ATM system that, despite being neglected by current theoretical perspectives, could be the target of managerial safety interventions aiming at improving the fit between human and alarms at the sharp end.**

Keywords-*Resilience Engineering and Management; Organizational Safety; Organizational Risk Management; Automation; Human-Alarm Interaction.*

I. INTRODUCTION

A. Human Alarm Interaction

Problems of human-alarm and human-automation interaction in safety critical domains have been notably dealt with in a compartmentalized or mechanistic fashion: the focus has been on characterizing the interaction between the human operator and the automated device as a standalone work unit independent of the organizational and work context [1]. Such a unit is conceived as a closed loop system characterized by the exchange of input and output between the human and the machine [2]. An important assumption is that the inner processes or tasks of the human mind could be broken down and studied independently of the work context.

While such human *information processing* perspective has been essential to foster the advancement of human alarm and human automation interface design and evaluation, it has a limited capability to address those undesirable side effects arising from the interaction of automation with the operational practice. Focusing on automated alarm systems, examples of side-effects include false or nuisance alerts, ambiguous alarms, alarm flooding, missed or delayed alarms, undesirable and unintended misuses, conflicts between the authority of the human operator and the authority of the automated alarm [see e.g., 3; 4-7]. Overall, such instances of poor fit between the human and the alarm system are not only problematic from a front-end operator perspective, i.e. pilots or air traffic controllers, but also from a safety perspective: they can in fact contribute to the development of accidents and disasters. For instance, accidents precursors lying at the human alarm interaction level include coordination breakdown between air traffic controller and two distinct crews in course of collision in presence of a highly sophisticated on-board collision avoidance system [8]; inadvertent inhibiting of the same collision avoidance system [9]; improper inhibiting of the ground based terrain warning system [10]; presence of multiple safety alerts disorienting pilots during emergencies [11].

The limitations of the human information-processing paradigm are not a new problem. This paradigm dates back to the 80ies, and since then a significant amount of work has been done from alternative theoretical perspectives. Distributed Cognition [e.g., 12; 13], Computer Supported Collaborative Work [e.g., 14], Activity Theory [e.g., 15; 16], and Situated Action [17] have widened and deepened the unit of analysis beyond the single operator-system interaction. They have considered a larger set of performance shaping factors, like coordination of cooperative activities, structure of goals and motives, historical and cultural conditions. Overall, such theoretical developments have been instrumental in providing a richer set of concepts and vocabularies for characterizing breakdowns at the human automation interaction level.

Considering the availability of such theoretical developments, one might wonder why do the undesirable side effects or anomalies at the human alarm interaction level remain a relevant hazard in organizations operating in safety critical domains. A plausible answer is usually found in the limited consideration of safety and human factors requirements along automation or alarm development process, due for

This work is part of a PhD program sponsored in part by EUROCONTROL Experimental Center, Brétigny-sur-Orge, France. The views expressed herein do not necessarily reflect the official view or policy of the agency.

instance to limited or late involvement of human factors and safety specialists [18; 19]. This view of failure originates from a comparison of actual development practice with respect to an idealized, abstracted, and prescriptive model of automation development. One example of such a model is provided by [20], who specifies the relevant safety assurance activities that should be carried out throughout the lifecycle of an Air Traffic Management (ATM) system, from conception, to development, operation and decommissioning. However, it can be noted that explaining failure as a deviation from an idealized lifecycle model, omits considering the influence of the underlying organizational context. Development and improvement practices do not occur in isolation in fact.

B. Resilience Engineering and Management

The present work has brought the problem of poor human alarm interaction under the safety paradigm of Resilience Engineering and Management (REM) [21-23], to explore the insights that such an approach can generate. REM is a safety management paradigm aiming at enhancing safety interventions at organizational and institutional levels, rather than operational only [23]. Safety is in fact considered to be a control problem requiring a repertoire of careful and dedicated organizational practices [19]. Under REM, complex safety critical systems like ATM can be conceived as made by a sharp end and a blunt end [19]:

- At the *sharp end* are located those operators, like pilots and air traffic controllers, in direct contact with the hazardous process to be controlled safely;
- The *blunt end* is made by the organization or set of organizations, such as regulators, administrators, technology suppliers, that drives, organizes, constraints, and ultimately determines the multiple working conditions and demands to which humans at the sharp end have to adapt.

Evidence from accidents in complex safety critical systems has turned the blunt end not only into an interesting area of inquiry, but also into a valuable area of potential safety improvements [19]. The main source of risk does not only come from individual errors or technical failures at the sharp end only, but also from biases and blind spots in organizational decision making at the blunt end. These arise out of a constant renegotiation of the definition of risk and of normal practices under strong pressure for productivity. Such dynamic, also called *organizational drift into failure* has been the object of different theoretical models, each one characterizing its constituent traits.

First, it has been noted that organizational drift into failure results from the flow of normal organization activity, and not from some exceptional event or decision (Dekker, 2005). This is due to the limited rationality held by organizational members during their day-to-day activities. It is nearly impossible for them to be fully aware of the undesirable consequences that their decisions might produce on the work system [24]. Each member can see only a portion of the entire work system, depending on his or her role in the organization, available information, and culturally accepted norms. Division of labour in large organizations, although defined for mobilizing organizational resources in function of the institutional relevant goals, has the side effects of 'insulating' different parts of organization, complexify patterns of information flows, and ultimately limiting the purview of local rationalities [25; 26].

Organization members usually act under a strong tension for productivity. In these terms organizational drift is a process induced by the organization trying to pursue efficiency and safety goals at the same time [see e.g., 21; 27; 28]. For instance, management has to find compromises between the allocation of scarce resources—people, funds, expertise and equipment—to meet the goals of the organization [29]. Similarly, operators at the sharp end are pushed to take decisions that might compromise safety goals while favoring efficiency objectives, or vice versa. In particular, Hollnagel notes that the decisions to prioritize productive pressure in a commercial environment is implicit and unrecognized, as usually decisions appear as sound when assessed according to the local time pressures, short-term incentives, and available knowledge [30; 31].

Furthermore, one problem in organizational decision-making is that a clear view of the relevant efficiency-safety trade-off is usually not available at the time of the decision. For instance, it would be incorrect to think of safety goals as clearly articulated in safety policies and procedures [32; 33]. The acceptable level of risk might not be made explicit, and the long-term effects of efficiency decisions on safety might not be known [32]. Also, operators' interpretation of institutional goals might differ substantially from those acknowledged by management. Sense making and interpretation from a local perspective are an important component of organizational drift.

Another important trait of organizational drift into failure is its incremental nature. Organizational drift does not happen overnight; rather accidents are usually preceded by a history of signals (about system anomalies) being downplayed for several years [34-36]}. This trait has been best explained by the theoretical developments of Turner and Vaughan, which are reported next.

Based on the analysis of 84 British accidents occurred over a ten years period, Turner's Man Made Disaster Theory [25] maintains that accidents are usually preceded by an incubation period during which the organization downplays emerging risks and near misses until disaster unfolds. Such an incubation period might last several years and is characterized by a systematic misinterpretation and overlooking of apparently unrelated hazards, so that these can accumulate unnoticed in the work system. In this period the organization gets increasingly attached to a view of the world that is inconsistent with the way the world really is, and is unable to anticipate the incoming failure. Such a failure of foresight suggests that accidents do not result solely from a physical process gone wrong, rather they are the result of a cultural laceration

between the worldview maintained by the organization and the way the world really is [25; 37].

Vaughan departed from Turner Man Made Disaster theory to theorize around the way a complex organization like NASA might end up accepting more risk than it is aware of [35; 38]. In the case of the NASA accidents of Challenger and Columbia, Vaughan [35; 38] noted that the respective anomalies leading to the accidents had a history dating back many years before the disasters. The O-ring erosion (Challenger) and the debris tile (Columba) were not manifested in a clear and immediately understandable manner if not only after the disaster. Engineers were in fact exposed to (i) mixed signals, i.e. signals indicating a potential danger that were followed by either less or no damage, reinforcing the belief that the system was safe to fly; (ii) weak signals, i.e. those signals about risk that after analysis were deemed so unlikely that there was very low probability for them to recur; (iii) routine signals, i.e. signals relating to events that while being dangerous, recur routinely with no accident happening. Ultimately these dynamics, as induced by an institutional context biased towards productivity goals and characterized by structural secrecy, contributed to generate the cultural belief that the system was operational and was safe to fly. An important consideration stemming from these findings is that history and context are important for understanding the etiology of failure and disaster [39].

It is now important to note that the REM perspective and the traits of organizational drift into failure have been characterized mainly in relation to the understanding, modeling, and prevention of accidents and disasters. However, it remains to be explored the benefits that the same lens can bring over other relevant areas of risk management, such as innovation and change. The introduction of new working methods, of new equipment, of new operational concepts, and of new automated tools and alarms are just a few examples of those changes organizations experience periodically for modernizing their infrastructures and for improving their operational productivity and safety. Such activities might be self-initiated or might be mandated by national and international modernization programs, such as SESAR in the Air Traffic Management domain. If not managed effectively, they have the potential to introduce novel anomalies and unintended side effects in the operational system, ultimately introducing new pathways to failure [19; 40].

II. Research Objective

This work aims at exploring the insights that the 'enlarged' REM perspective can generate over problems of human alarm interaction. The focus is on advancing the understanding about how organizations might drift into poor human alarm interaction, or, on the contrary, about how they can avoid such drift. It must be noted that we have not found other research work pursuing the same research objective from a similar theoretical orientation. Therefore, a specific methodological approach, consistent with our exploratory objective, had to be devised. This is described in the next section.

III. Methodology

We implemented the REM approach through the deployment of two in depth longitudinal-historical case studies centered on an alarm system, the Minimum Safe Altitude Warning System (MSAW), a ground based safety net from the ATM domain. Both studies were developed consistently to the three methodological orientations exposed below.

First, they investigated the interaction over time between (i) anomalies at the human alarm interface and (ii) the underlying organizational context within which the system was introduced and operated. This focus, analogous to that exploited by Vaughan in her investigation of the Challenger disaster [41], allowed tracing retrospectively the 'trajectories' of the alarm anomalies study to understand how they have been interpreted, reported, debated and managed over time. The fact that drift develops over the course of several years provided the rationale for such a longitudinal-historical focus. The same rationale also oriented us towards the selection of a well-established application, the Minimum Safe Altitude Warning System, or MSAW, as application case. This alarm has a long and troubled operational history—due to the high rate of nuance or false alerts it generates, especially when implemented for protection of the final approach path—that was available for investigation and for extracting useful lessons.

Second, both studies maintained an ethnographic orientation. They focused on understanding viewpoints and perspectives of insiders. This was the case for two reasons. First organizations are socials purposive systems. As indicated by foundational work in interpretive organizational research [e.g., 42; 43], the understanding of the motives, perspectives, meanings and intentions which organizational members use to direct their everyday lives maximizes opportunities for generating plausible theoretical accounts about organization behavior. This is even truer for inquiries into a novel or little explored organizational phenomena [44], such as in the present research. Second, considering insiders' viewpoint enable reducing opportunities for hindsight bias. Understanding the evolution of events from the inside out enables the understanding of the uncertainties, alternatives courses of action that were available to practitioners in the field prior the occurrence of failure.

In particular, both studies adopted a *dual focus* approach to data collection, accounting for both the viewpoints (i) of air traffic controllers and (ii) of the other stakeholders at the blunt end, such as supervisors, managers, R&D directors, and safety experts, international and national regulators. The former view provided insights into the role of the alarm in use, possible conflicts with the operational practice, potential for unintended uses, and the like. The latter view provided insights into the rationales, interests, and cultural frames behind the decisions and conditions related to alarm development, adoption, operation, and improvement.

Third, both studies were interpretive and adopted an abductive approach to data analysis based on [45] and [46]. The abductive approach exploits the systematic and

imaginative use of metaphors and analogies in an attempt to produce plausible theoretical readings of complex organizational phenomena, as reflected by insider's account. Such an approach is adequate for exploratory research with theory construction purposes [47; 48]. In these cases, the emphasis is on structuring observations, resulting from in depth investigations, in order to identify and to distinguish novel descriptive and explanatory concepts, and project meanings, rather than measuring and testing consolidated concepts already contemplated by existing theories.

The use of a multiple case approach allowed implementing the above-described case study design first in a less constrained research environment to assess its viability, and subsequently replicate the same design in a more complex and more demanding environment. For this reason the studies differed as regard the scope of the inquiry and the variety of data used.

Study 1 [49; 50] focused on the analysis of the inter-organizational debate between NTSB and FAA over the implementation of the Safety Recommendations issued by NTSB on the MSAW (Minimum Safe Altitude Warning System) system, since the introduction of the alarm in the US in the seventies. This study provided a first constrained environment where to assess the potential of the REM approach. It was scoped on the view of air traffic controllers (sharp end), and a portion only of the safety control structure (the blunt-end) influencing MSAW system adoption, implementation, and operation. Also, it was based mainly on the analysis of documentary evidence, including safety recommendations, safety recommendations letters, follow up letters exchanges between NTSB and FAA, and accident reports related to accidents discussed in the safety recommendation letters. The study has showed the viability of the defined case study approach, and has strengthen in particular our confidence over alarm anomaly trajectory in the organization as an appropriate focus of the inquiry. The outcome of Study 1 included the identification of one organizational-systemic precursor to poor human alarm interaction, Structure of Safety Debates, which related to dynamics that might prevent alarm anomalies at the level of front-end operator from being properly framed at higher organizational levels.

Subsequently, Study 2 [51; 52] brought the REM approach to a less constrained and more complex case: the analysis of the organizational-systemic sources of poor MSAW implementations in the European ATM. This study investigated MSAW implementation and operation within four European Air Navigation Service Providers (ANSPs). It was based on the analysis of transcripts of informal and semi-structured interviews, observational notes, historical company documents, service notes, accidents and incidents reports, requirements and guidance material as developed both at international level national level. This data was collected in 2010 over a period of ten months during attendance of three meetings on Air Traffic Control ground-based safety nets, and during site visits at six Air Traffic Control centers of the four ANSP included in the study. This second case further reinforced our confidence in the defined REM approach, and it allowed defining other categories of organizational-systemic precursors to poor human alarm interaction: Alarm Implementation Expertise Acquisition/Development; Quality of ANSP-Software Vendor Collaboration; Managerial Assumptions Driving Adoption.

Eventually, the categories of precursors emerged from Study 1 and Study 2 were compared, checked for contradictions, and integrated in a single qualitative framework that is presented next.

IV. How do Organziations can drift into poor human alarm interaction?

This section presents a framework of the organizational-systemic precursors to poor human alarm interaction. The framework is qualitative and is composed by four organizational dynamics that appear to affect the ability of a company to control hazardous anomalies lying at the human-alarm interface. Such dynamics are outlined below.

(1) Structure of Safety Debates. This category refers to how safety nets anomalies and problems (e.g. nuisance alerts, alarm flooding, ambiguous alerts) can be reported and debated within a company and across companies, for instance during development projects or requirements meetings. During such safety debates, the underlying theoretical model or perspective of safety, of human performance or of human alarm interaction might remain tacit so that an organization might be unable to learn about the distance existing between the *view of the alarm* as envisaged by its different stakeholders at various hierarchical levels in the organization and the *view of the alarm* as operated by air traffic controllers. Debates within the organization might be plagued by a tendency to keep premises of arguments out of scrutiny and to solve lack of consensus through power. Such tendencies are known to inhibit organizational learning: failing to explicate the premises behind the courses of action intended by different parties hampers confrontation, ultimately leaving opposing parties trapped in conflicting positions [53]. Solving lack of consensus about ambiguous issues through the use of informal or formal power relationships means that the dominant party will ultimately judge what is the most appropriate interpretive frame to adopt [54]. Ultimately, relevant safety net or general automation anomalies related to an operational system might lie unaddressed or underreported for years, even for decades despite these anomalies contributing to incidents and accidents, while the company might ultimately invest in other safety areas since it is not aware of its blind spot.

We observed this pattern in our analysis of the Safety Recommendations issued by the National Transportation Safety Board (NTSB) to the Federal Aviation Administration (FAA) and targeting the MSAW [25]. There, we observed the above mentioned dynamics to have contributed to frame repeatedly the problem of the frequent 'lack of response to MSAW alerts by air traffic controllers' as an issue of 'improving HMI design', and not as one of 'reducing the frequent rate of nuisance alerts'—the fundamental source of

the problem. Such a loose conceptual coupling between an anomaly at the sharp end and its fundamental cause 'resisted' for nearly three decades during reiterated correspondence exchanges at the blunt end between the two agencies. Only in 2006, NTSB recognized the relevance of the nuisance alert issue with regard to the controllers' lack of response.

(2). Path to Alarm Capability Building. This category refers to the process by which a given ANSP develops the capability to set up a novel automated alarm. As for any innovative endeavor, the successful introduction of an alarm system novel the organization requires appropriate organizational capability. This consists on a mixture of knowledge, know how, expertise and competence, specific skills, and technological supports. It can either be built internally to the organization or be integrated from outside sources when others have already developed it. While lack of such capability is usually associated to general innovation failures [55], the specific path to capability building a given organization goes through seems to correlate to its ability to achieve an optimal set up of the system.

All of the ANSPs included in Study 2 encountered a first problematic implementation of their respective MSAW system: in all cases the implemented system generated an high rate of nuisance alerts which was reported to interfere with air traffic controllers practices. However, these service providers differed in their ability to adapt to such alarm side effect depending on their specific path to capability building they followed. ANSP1, a large European ANSP, pioneered the development and parameterization of the alarm in Europe. Although encountering a high rate of nuisance alerts during its first MSAW implementation cycle, such pioneer service provider could recur to internal in-house formal R&D and co-development with its national manufacturer. Notably [56], these two strategies favor learning by doing, which in this case meant carrying forward lessons learned from previous unsuccessful implementations, plus the sharing and linking of complementary knowledge sets, in this case held by service provider and the software manufacturer, in order to solve a complex problem, i.e. MSAW parameterization. Eventually ANSP1 achieved an implementation that was regarded as best in class in the industry at the time of data collection.

When the resources for pioneering development are lacking, other ANSPs interested on the implementation of the same system already implemented by a pioneer might opt for an imitation strategy. In this case the focus is mainly on integrating the capability that has been already made available somewhere outside of the company. For instance, in our study, we observed that a path follower service provider, ANSP2, a mid-size service provider, acquired the capability needed to fine tuning the MSAW by recurring to personnel poaching and by purchasing the system from the same 'expert' software manufacturer which already co-developed the tool with ANSP1. Also ANSP 2 eventually achieved an implementation regarded as a best in class implementer at the time of data collection.

Two other ANSPs were found in the process of catching up. These organizations relied initially mainly on the expertise provided by the software manufacturer from which they bough their COTS[1] MSAW system. However, in both cases, such strategy turned out to be less than optimal from an implementation perspective for the reasons detailed in the next sections. Thus one ANSP was found to have removed its MSAW system from operation at the time of data collection. The other was found to be in the process of improving the alarm by relying on the external support by EUROCONTROL, the European Agency for the Safety of Air Navigation. Since 2005, EUROCONTROL has created a dedicated task force, named SPIN, for enhancing and standardize ATM alarm implementations across Europe. With regard to this specific ANSP, EUROCONTROL, through SPIN, acted as a technology transfer agency: it promoted the positive transfer of expertise and competence about the MSAW parameterization process from early best class implementers to a later adopter.

(3). ANSP-Software Vendor Collaboration. Effective collaboration between a software vendor, selling safety critical automation, and the client organization, purchasing and deploying it (the ANSP), appears to be a key component for ensuring the efficient implementation of an automated alarm. While a successful integration requires an optimal blend of software development/parameterization expertise (vendor) and operational expertise (client), we observed that problems might arise due to incomplete contracting, poor alignment, lack of experience with the specific system on the client side, the vendor, or both.

The client ANSP might underestimate the implementation effort, thus omitting to fully specify the requirements of the MSAW to be purchased, and failing to allocate sufficient resources to the parameterization of the alarm. In the absence of specified requirements, the MSAW implementations risks reflecting more the manufacturer's view concerning the set up of the alarm, as the control over the tuning process is transferred almost entirely to the software manufacturer.

In our cases, one manufacturer was reported to reuse opportunistically an alarm key component—the terrain database—which was taken from a previous client site and that however matched poorly the site of the new client. As a result the terrain database contributed to generate too many nuisance alerts. Further, issues related to requirements traceability were reported, and the manufacturer was reported by our informants as not being fully aware of the trade-off involved in the parameterization of the alarm. In these cases, the implementation of the alarm might turn out to be challenging not just for the client but also for the vendor. One additional problem we observed here is that after the contract is signed the vendor's willingness to accommodate client's requests might decrease, so that additional improvements to the implemented system might require extra negotiations to be arranged [51]. When experiencing such a flawed collaboration with its software provider, it may not be easy for an ANSP to recover

[1] Commercial Off-the Shelf

from a poor implementation on its own. Purchasing the system usually has lack of learning as a side effect, so that it is difficult to carry forward the lessons from previous failure/s.

(4) Managerial Assumptions Driving Adoption. This category refers to the assumptions behind the managerial decision to adopt an automated alarm within the organization. Of particular relevance seems to be the balance between the decision to adopt and the availability of appropriate capabilities, expertise, and guidance material to ensure the proper fit of the system to the local operational practice.

In our cases we observed biased assumptions about the organization capability to implement the alarm. Some service providers appeared to commit to adopt the MSAW as if this were a 'commodity', i.e. a standard component in the industry bringing limited impact on operational practices, and which for design and implementation were unproblematic. Such assumption appeared to be partly reinforced by the consideration that the MSAW is usually viewed as not affecting traffic capacity and as exhibiting low technical complexity in comparison to the larger radar processing system of which it is an add on. This assumption was more apparent for one of the catch up ANSPs, which committed opportunistically to the implementation of the alarm after this was proposed to them by the manufacturer as part of the larger software package that was under acquisition. In general, the novelty and difficulty related to the implementation of the alarm went somehow unrecognized. For instance, in none of our four organizations we found evidence of a formalized rationale detailing the reason for having the MSAW installed and the role of the alarm in the ATM system. In general, it was assumed that alarming the imminent infringement of aircraft through a minimum altitude would have been sufficient to avoid Controlled Flight into Terrain—the kind of aviation accident the MSAW system should contributed to prevent.

With these bases, the implementation of the alarm was framed mainly as a technical engineering process, and not as an innovative experimental one presenting many areas of uncertainty. In particular, in at least two cases the implementation schedule was dictated mainly by productivity consideration—such as fixing the O-date (the data a system goes operational) before period of high traffic—in absence of other criteria indicative of the degree of fit between the alarm system and the specific operational practice.

These premises set the stage for an implementation process characterized by a high degree of uncertainty and intense temporal pressure. Personnel reported lacking in-house expertise about the system when they committed to their first implementation. Furthermore they reported that on the one hand early international standards and guidance material related to the MSAW mandated the implementation of this and other alarms, on the other hand these standards and guidance were reported to provide only a minimal definition of the system. Inevitably, the first deployment of the MSAW proceeded tentatively by trial and error, lacking any reference model about the parameterization process. Thus the first operational MSAW turned out to play the role of a nuisance disruptive of air traffic controller practices, to be dismissed, ignored, and in some cases removed from operation.

The managerial assumptions driving adoption seems to be important also at international level. Early efforts to mandate the wide spread adoption of an alarm system across different states might not be matched by a formal assessment about the maturity of existing standards and guidance material, and about the path to capability building that can be sustained by different implementers. In our case, early standard and guidance material about the MSAW appeared to accommodate only for a limited portion of the complexity that had to be considered by local implementers. Also, as described earlier, different service providers followed different paths to alarm capability building, so that different states achieved different implementations of the same system. In general, it seems that neglecting how the knowledge and expertise needed to set up an automated alarm can be generated and diffused across the organizations implementing the alarm leaves room to asymmetrical implementations at system wide level.

V. Discussion and Conclusions

This paper has explored the insights that the Resilience and Management (REM) perspective can bring when applied to problems of poor human alarm interaction, and has outlined a case study approach through which the REM perspective can be implemented. As expected, the REM perspective appeared to be useful in unveiling the organizational-systemic dynamics at the blunt end of the system that may influence the quality of human alarm interaction at the sharp end. The appreciation of such dynamics extends the dimension of the problem of human alarm interaction to factors that are exogenous to the unit of analysis defined by the classic human information paradigm, and the other alternative competing approaches. Moreover, understanding such organizational-systemic dynamics is useful to get a grasp on those barriers and biases at the blunt end of the ATM system that might affect the ability of service providers to adapt successfully to the side effects of their automated systems. In particular, the framework presented here has stressed four organizational dynamics, which arguably have to be considered to prevent an organizational drift into the implementation and operation of alarms presenting a poor fit with their intended users.

Compared to REM literature, which notably has an interest on advancing current understanding of disasters and accidents, it can be noted that this paper has the merit of having shown (i) the kind of organizational bias and holes that might affect technological change and innovation in a safety critical domain like ATM, and (ii) a case study strategy trough which they can be investigated.

It must be noted that the reported framework has resulted from the integration of the findings of two case studies focused on the same alarm system. Intentionally, this approach first supported replication: upon uncovering significant findings from a first, tentative, and constrained study, the same

approach could be replicated in a more demanding context. Second, this approach favored depth of the inquiry—a necessary objective in exploratory research on social phenomena [44]—over generalizability of findings. This seemed a necessary and acceptable trade-off as a means to investigate organizational drift into failure. In fact such a phenomenon requires a thorough understanding of history and context in order to make sense of a complex and multileveled organizational reality, and explain how past events and conditions located at different organizational levels and occurring at different points in time are linked to present failures.

One implication from our methodological approach is that at this stage it is not possible to state if and to which extent the same organizational-systemic dynamics might threaten the introduction and operation of other automated systems in the ATM and other domains. For this reasons, the next stage of the work will consist in bringing our framework back to the field to corroborate it with alarm and automation experts, possibly through a survey, and assess its relevance also in contexts other than alarm systems. Also, it must be noted that the kind of criticalities identified in this study do not belong to the kind of issues human factors and safety specialists usually have agency over. Conditions such as structure of safety debates, path to alarm capability building, ANSP software vendor collaboration, and managerial assumptions driving adoption do not translate into practical, specialist level, engineering or HMI guidance. Rather, they appear to pertain more to managerial and administrative spheres of interventions.

So, we are interested on exposing the categories of our framework to managers of automation programs to explore ways in which they could translate into pragmatic, managerial level, safety improvements. At the moment, we expect the framework to inform safety nets and automation program managers about organizational and programmatic sources of risks that might threaten alarm development programs. In particular, the corroborated framework of organizational-systemic precursors is expected to have the potential to enhance the ATM concept lifecycle model (CLM)—as envisaged under the European Operational Concept Validation Methodology (E-OCVM)—by coupling it with the sources of organizational and programmatic risks affecting the Industrialization (V4), Deployment (V5), and Operation (V6) Phases. This is a useful enhancement, as E-OCVM today covers mainly the upstream phases of the CLM, i.e. Scope (V1), Feasibility (V2), Pre-Industrial Development and Integration (V3) [57].

ACKNOWLEDGMENT

The author wish to thank Dr Barry Kirwan and Mr Andrew Kilner, EUROCONTROL Experimental Center, for having promoted the positive initiation of this work and for their useful support during site visits and data collection. Also, the author wish to express his gratitude to Ben Bakker, EUROCONTROL Headquarter, for having facilitated access to the EUROCONTROL Safety Net Performance Improvement Network (SPIN), and for his feedback on previous phases of this work. A special thanks goes to Prof Darren Dalcher and Dr Bob Fields for their critical comments, and to Dr Paola Amaldi, and Mr. Ronish Joyekurn for their editorial comments. Finally, the author also acknowledges the anonymous reviewers for their constructive feedback.

REFERENCES

[1] Chaiklin, S. Modular or integrated? An activity perspective for designing and evaluating computer-based systems. *International Journal of Human-Computer Interaction* 22 (2007), 179-197.

[2] Hollnagel, E. and Woods, D. D. *Joint cognitive systems: Foundations of cognitive systems engineering*. CRC/Taylor and Francis, Boca Raton, FL, 2005.

[3] Pritchett, A. R. Reviewing the role of cockpit alerting systems. *Human Factors and Aerospace Safety* 1(1) (2001), 5–38.

[4] Xiao, Y., Seagull, F. J., Nieves-Khouw, F., Barczak, N., and Perkins, S. Organizational-historical analysis of the failure to respond to alarm problems. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* 34(6) (2004), 772–778.

[5] Breznitz, S. *Cry wolf: The psychology of false alarms*. Lawrence Erlbaum Associates, 1984.

[6] Allendoerfer, K., Friedman-Berg, F., and Pai, S. *Human Factors Analysis of Safety Alerts in Air Traffic Control*. Federal Aviation Administration, Atlantic City, 2007.

[7] Wickens, C. D., Rice, S., Keller, D., Hutchins, S., Hughes, J., and Clayton, K. False Alerts in Air Traffic Control Conflict Alerting System: Is There a "Cry Wolf" Effect? *Human Factors: The Journal of the Human Factors and Ergonomics Society* 51(4) (2009), 446–462.

[8] BFU Investigation Report. (May 2004),

[9] CENIPA. *Aeronautical Accident PR-GTD and N600XL B-737 8EH and EMB 135 BJ Legacy 29 September 2006 Final Report*. 2008.

[10] NTSB. *Controlled Flight into Terrain, Korean Air Flight 801, Boeing 747-300, HL7468, Nimitz Hill, Guam, August 6, 1997*. Washington, DC, 2000.

[11] Perrow, C. *Normal Accidents. Living with High- Risk Technologies*. Princeton University Press, Princeton, New Jersey, 1999.

[12] Hollan, J., Hutchins, E., and Kirsh, D. Distributed cognition: toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction (TOCHI)* 7(2) (2000), 174–196.

[13] Hutchins, E. How a cockpit remembers its speeds. *Cognitive science* 19(3) (1995), 265-288.

[14] Schmidt, K. and Simone, C. Mind the gap. *Towards a unified view of CSCW. COOP* (2000), 205–221.

[15] Kaptelinin, V., Kuutti, K., and Bannon, L. Activity theory: Basic concepts and applications. *Human-Computer Interaction* (1995), 189–201.

[16] Bertelsen, O. W. and Bødker, S. Activity theory. *HCI models, theories, and frameworks: Toward a multidisciplinary science* (2003), 291–324.

[17] Suchman, L. A. *Plans and situated actions: the problem of human-machine communication*. Cambridge University Press, 1987.

[18] Cardosi, K. Human factor lessons learned in the design and implementation of air traffic control systems. *The Controller, 11-15, first quarter* (1998), 11–15.

[19] Dekker, S. *Patient Safety: A Human Factors Approach*. CRC Press, 2011.

[20] Kirwan, B. Safety informing design. *Safety Science* 45(1–2) (2007), 155–197.

[21] Hollnagel, E., Woods, D. D., and Leveson, N. *Resilience Engineering: Concepts and Precepts*. Ashgate Pub Co, 2006.

[22] Leveson, N. G. *Engineering a Safer World. System Thinking Applied to Safety*. The MIT Press, 2011.

[23] Woods, D. D. Creating Foresight: Lessons for Enhancing Resilience from Columbia. In W. H. Starbuck and M. Farjoun (Eds), Blackwell, 2005.

[24] Reason, J. *Managing the risks of organizational accidents*. Ashgate, 1997 Jan 1.

[25] Turner, B. A. and Pidgeon, N. F. *Man-made disasters (2nd ed.)*. Butterworth Heinemann, Oxford, 1997.

[26] Rasmussen, J. and Svedung, I. *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, Karlstad, Sweden, 2000.

[27] Rasmussen, J. Risk management in a dynamic society: a modeling problem. *Safety science* 27(2–3) (1997), 183–213.

[28] Marais, K., H., S. J., and Leveson, N. Organizational Risk Dynamics in Complex Goal Environments, in *Proceedings of the ESREL 2007* (Norway, June 2007).

[29] Farjoun, M. Organizational Learning and Action in the Midst of Safety Drift: Revsing the Space Shuttle Program's Recent History. In *Organization at the Limit: Lessons From the Columbia Disaster*, W. H. Starbuck and M. Farjoun (Eds), Blackwell Publishing, 2005 Jan 1.

[30] Hollnagel, E. *The ETTO Principle: Efficiency-Thoroughness Trade-Off-Why Things That Go Right Sometimes Go Wrong*. Ashgate Pub Co, 2009.

[31] Hollnagel, E. *Barriers and accident prevention*. Ashgate Pub Ltd, 2004.

[32] Marais, K. B. and Saleh, J. H. Conceptualizing and communicating organizational risk dynamics in the thoroughness-efficiency space. *Reliability Engineering & System Safety* (2008 Jan 1),

[33] Woods, D. D. and Cook, R. Perspectives on human error: Hindsight biases and local rationality. *1999)* (1999 Jan 1),

[34] Woods, D. Creating Foresight: Lessons for Enhancing Resilience from Columbia. In *Organization at the Limit. Lessons from the Columbia Disaster*, W. H. Starbuck and M. Farjoun (Eds), Blackwell Publishing Ltd, 2005.

[35] Vaughan, D. System Effects: On Slippery Slopes, Repeating Negative Patterns, and Learning from Mistake? In *Organizations at the Limit: Lessons from the Columbia Disaster*, W., A., Starbuck and M. Farjoun (Eds), Blackwell Publishing, Ltd, 2005.

[36] Dekker, S. *Drift into failure: From Hunting Broken Components to Understanding Complex Systems*. Ashgate, 2011.

[37] Pidgeon, N. and O'Leary, M. O. Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science* 34 (2000), 15–30.

[38] Vaughan, D. Organizational rituals of risk and error. In *Organizational encounters with risk*, B. Hutter and M. Power (Eds), Cambridge University Press, 2005 Jan 1.

[39] Le Coze, J.-c. Disasters and organizations: From lessons learnt to theorizing. *Safety Science* 46 (2008), 132–149.

[40] Perry, S. J., Wears, R. L., and Cook, R. I. The role of automation in complex system failures. *Journal of Patient Safety* 1(1) (2005), 56–61.

[41] Vaughan, D. Theorizing disaster: Analogy, historical ethnography, and the Challenger Accident. *Ethnography* 5 (3) (2004 Jan 1), 315–347.

[42] Weber, M., Shils, E., Finch, H. A., Antonio, R. J., and Sica, A. *Methodology of Social Sciences*. Transaction Pub, 2011.

[43] Schütz, A. Concept and theory formation in the social sciences. *The Journal of Philosophy* 51(9) (1954), 257–273.

[44] Stebbins, R. A. *Exploratory research in the social sciences*. Sage Publications, Inc, 2001.

[45] Morgan, G. *Imaginization: New Mindsets for Seeing, Organizing, and Managing*. Sage, 1997.

[46] Weick, K. E. Theory construction as disciplined imagination. *Academy of management review* (1989), 516-531.

[47] Charreire, S. and Durieux, F. Exploring and Testing. In *Doing management research, a comprehensive guide*, R.-A. Thietart (Ed), SAGE, 2001.

[48] Blaikie, N. *Approaches to social enquiry: Advancing knowledge*. Polity, 2007.

[49] Rozzi, S., Amaldi, P., and Kirwan, B. From Intent to Action: Evolution of a Safety Net, in *Proceedings of the Close Calls: Organizations, Near Misses and Alarms* (London, March 26–27, 2009).

[50] Amaldi, P. and Rozzi, S. Inter-Organizational Safety Debate: The Case of an Alarm System from the Air Traffic Control Domain. *International Journal of Sociotechnology and Knowledge Development* 4(1) (2012), 30–47.

[51] Rozzi, S., Amaldi, P., and Kirwan, B. IT Innovation and its Organizational Conditions in Safety Critical Domains: The Case of the Minimum Safe Altitude Warning System, in *Proceedings of the 5th IET International Conference on System Safety* (Manchester, UK, October 2010), IET, 1–7.

[52] Rozzi, S. and Amaldi, P. Organizational and Interorganizational Precursors to Problematic Automation in Safety Critical Domains. A Longitudinal Ethnographic Case Study from the Air Traffic Management Domain, in *Proceedings of the ATACCS 12* (London, Uk, May 2012).

[53] Argyris, C. and Schön, D. A. *Organizational Learning II: Theory, Method, and Practice*. Addison-Wesley Publishing Company, Reading Mass, 1996.

[54] Milliken, F. J., Lant, L., and Bridewell-Mitchell, E. Barriers to the Interpretation and Diffusion of Information about Potential Problems in Organizations: Lessons from the Space Shuttle Columbia. In W. A. Starbuck and M. Farjoun (Eds), Blackwell Publishing, 2005.

[55] Malerba, F. and Nelson, R. Learning and catching up in different sectoral systems: evidence from six industries. *Industrial and Corporate Change* 20(6) (2011), 1645-1675.

[56] Tidd, J. and Bessant, J. *Managing innovation: integrating technological, market and organizational change*. Wiley, 2011.

[57] EUROCONTROL E-OCVM, Version 3.0, Volume I. European Operational Concept Validation Methodology. (2010).