The Organizational Response to Automation Support Degradation. Identifying Air Traffic Control Sources of Resilience in Cases of Radar Loss

Luca Save, Deep Blue s.r.l., Italy, *luca.save@dblue.it*, **Daniele Ruscio**, Deep Blue s.r.l., Italy,
Valentina Cedrini, ENAV s.p.a., Italy, **Laura Cafiero**, ENAV s.p.a., Italy , **Maurizio Mancini**, ENAV s.p.a., Italy.

ABSTRACT

Controllers working in Area Control Centres are supported by highly automated multi-radar tracking system displaying air traffic at different working positions. The automation provides and selects for the controllers the most relevant information associated to each aircraft and assists them while they issue instructions to pilots. But, what happens when the automation fails? These rare situations represent an example of abrupt transition from a highly automated to a severely degraded mode of operation. Exploring sources of resilience during this critical loss from highly automated tasks allows to better understand the effects of automation in a complex transportation system. Safety management and business continuity considerations were made during the DARWIN project whose goal is the development of resilience management guidelines for critical infrastructures. A specific part of the DARWIN resilience management guideline was applied to a loss of radar information scenario, based on the experience of a real event occurred in a European Area Control Centre, in order to assess the resilience responses to automation degradation. The DARWIN guideline concepts supported the identification of individual and organisational resilience mechanisms that allowed the Area Control Centre to operate in a severely degraded mode, with no negative effects on the safety and a very limited impact on the business continuity. Similar adaptive capacity mechanisms can be adopted, for analogy, in other critical transportation infrastructures that aim to achieve highly automated functionalities in the management of assisted human-machine interactions.

Keywords: Automation, Resilience Management, Organizational Response, take-over control.

1 INTRODUCTION

Area Control Centres (ACCs) are responsible for controlling air traffic, from the moment an aircraft takes off from a given airport, until it lands to another airport. Differently from Tower controllers, who rely on out-of-the-window scan over the airport surface, the controllers working in Area Control Centres are always supported by highly automated systems. These mainly consist of a multi-radar tracking system displaying air traffic at different working positions, where the controllers can monitor the evolution of traffic in their respective sectors of responsibility. The automation provides and selects for the controllers the most relevant information associated to each aircraft and it assists them with a set of tools to issue instructions to pilots via radio-telephony and other communication means. But, what happens when the automation fails? Are the air traffic controllers still able to provide instructions to the pilots in case of a sudden loss of radar information? Which resilience capabilities are needed to successfully face sudden automation support degradations? Total losses of radar information are rare events and they represent a form of abrupt transition from a highly automated to a severely degraded mode of operation, in a safety-critical transportation system. They require

that all the Air Traffic Controllers (ATCOs) of the affected ACC handle the traffic (overflying or going to land in their area of responsibility) without being able to visualize it on their radar screens. Exploring sources of resilience in the management of this type of emergencies was one of the topics considered during the DARWIN project, whose goal is the development of resilience management guidelines for organizations managing critical infrastructures, such as the transportation ones. Traditional risk management approaches focus on prediction, prevention and protection against expected events. These approaches cover known system disturbances as initiating events. Consequently, procedures, training, and regulations for operations are put in place to protect from known disturbances and mitigate their consequences. In recent years, different methods have been proposed to overcome the limitations of these approaches, by addressing the interdependencies between critical infrastructures and the increasing complexity of the situations that can escalate off-the-scale. The guideline approach used in the DARWIN project follows this path, by proposing strategies to address the enhancement of the abilities of an organisation to sustain adaptability and continue operations as required to a changing context (Hollnagel, Woods, Leveson, 2006).

The present paper proposes the analysis of a radar loss event based on the use of the DARWIN guideline, to show how it is possible to go beyond traditional risk management practices in response to automation degradation that mainly considers just the individual take-over response (e.g. Zeeb et al., 2015). The analysis will highlight both the reaction capabilities of a single organization in case of automation degradation and the resilience management strategy of more organizations cooperating in the management of the same crisis.

2 METHOD

In order to evaluate the applicability of a specific part of the DARWIN guideline, a workshop was organized with air traffic controllers, safety experts and security experts, in order to explore the available *sources of resilience* in a radar loss scenario, based on the experience of a real event occurred in a European ACC.

2.1 DARWIN Concept Cards for Assessing Automation support degradation

The DARWIN Resilience Management Guideline is a WIKI based tool[1] structured around a set of so-called Concept Cards (CC) that are made available to resilience practitioners. Each concept card is linked to a specific resilience management principle and suggests a number of actions that an organization managing a critical infrastructure should perform in order to increase its level of resilience. For analysing the total radar loss situation, a specific CC named “Identifying sources of resilience” was used in a *pilot exercise* involving representatives of different ACCs. The CC included a number of *triggering questions* aimed at identifying the most effective organizational response to a contingency, emergency or crisis situation, which in this case was

[1] For further information, please refer to https://h2020darwin.eu/wiki/

generated by the degradation of an automation support system. The triggering questions were clustered in different thematic areas that were intended to encourage the practitioners to identify specific sources of resilience available in everyday operations. The thematic areas addressed for this case were: "Adaptive Capacity", "Operational Margins", "Resources", while other thematic areas presented in the CC ("Monitoring", "Goals Trade-offs", "Dependencies and Interactions") were not considered relevant for this scenario.

2.2 Sample

The Air Navigation Service Provider (ANSP) is the organization more impacted by a loss of radar information. Therefore, air traffic control experts from different departments of a European ANSP were involved in the pilot exercise. More precisely, the experts had working experience in three different ACCs. One of them (ACC "A") was the control centre that experienced the radar loss, while the other two (ACC "B" and "C") where neighbouring ACCs, i.e. control centres located in different geographical areas and managing the traffic in different airspace portions, but with at least one border shared with the ACC affected by the radar loss. The roles of the actors participating in the exercise were the following: a representative of the Security Operation Centre of the ANSP, two representatives of the ANSP Safety Department, an expert of contingency plans and four ATCOs, with working experience in all of the involved ACCs (i.e. one from ACC "A", two from ACC "B" and one from ACC "C").

2.3 Procedure

The evaluation session consisted of a workshop (see Figure 1) with all the experts brainstorming guided by a handout version of the card, in the identification of the available sources of resilience in a radar loss scenario. One part of the discussion focused on a *BEFORE CRISIS* scenario (how could we manage a radar loss situation due to a cyberattack if it occurs in one of our ACCs?). While a second part focused on an *AFTER CRISIS* scenario (how did we manage a radar loss situation actually occurred in one of our ACCs, due to a technical failure?). The two different perspectives were suggested by the format of the CC, which includes specific triggering questions to be used before, during or after a crisis, contingency or emergency.

Figure 1 – Evaluation session to identify the sources of resilience available in the automation degradation

The analysis of the *before crisis* situation allowed to address preparedness and all the cyber-security issues related to the possible causes of a radar loss, which in this case were never experienced by the ANSP. The analysis of the *after crisis* situation was equally relevant, due to the possibility to learn from a concrete experience of a radar loss event happened in 2017. The event was initially caused by a minor technical failure occurred at an airport and then propagated into unexpected cascading effects to the ACC "A", causing the freezing of radar screens of the Controller Working Positions (CWPs) for more than two hours, during morning operations.

Following the brainstorming on the sources of resilience, a semi-structured questionnaire was also administered, in order to: a) collect feedback on the perceived impact of the CC in improving the organization's ability to respond in case of radar loss; b) collect proposals of improvement actions the ANSP should apply in order to manage the radar loss described in the scenario. The main results of the workshop are summarized in the following section, with focus on the *after crisis* scenario.

3 RESULTS

During the real event occurred in 2017, the frozen radar screens prevented all the ATCOs from visualizing the evolution of traffic for a considerable amount of time. Despite such critical situation, different sources of resilience allowed a full recovery to the normal ACC functionality in less than four hours, with limited impact on the business continuity of some Regional Airports and no negative effect on the safety of air transportation in the concerned area. For each of the thematic sections selected from the Concept Card (i.e. Adaptive capacity, Resources, Operational Margins), it was possible to provide examples of the sources of resilience that were already available in the organisation and the ones that were specifically activated to face automation loss event.

3.1 Adaptive Capacity

For what concerns the "adaptive capacity", two different adaptation strategies were identified: (1) the *reorganization of existing roles* and the *coordination with other Air Traffic Control units* to manage the radar loss. Actually, in the first moment the automation loss, there were three *Supervisors* available in the operational room, who were carrying out their usual tasks. After a while, the supervisors realized that it was more efficient if they split their responsibilities in three different types of tasks. The first one started to take care of flight data management (i.e. to associate the single flights to the corresponding flight plans). The second one was enrolled in phone coordination activities with the nearby ACCs to ensure the most efficient cooperation. Finally, the third one was assisting the ATCOs at individual controller working positions. Such dynamic reallocation of tasks proved to be very effective in sustaining the effort of the whole ACC to maintain an acceptable level of continuity of the Air Traffic Control service. (2) The second adaptive capacity strategy was sustained by the coordination of the ACC with the Flow Management positions at Local, National and European level. Such coordination was necessary to modify the flight plans of all the aircraft expected to enter in the concerned Area of Responsibility (i.e. the airspace portion) of the affected ACC. All these aircraft needed to be diverted/rerouted to bypass the geographical areas affected by the radar loss and this was achieved very quickly thanks to such coordination.

3.2 Resources

The management of the loss of radar information immediately caused an imbalance between the *capacity* of the ACC and the *demand* in terms of air traffic. This required more resources to be called into duty, including both human and technical ones. For what concerns the human resources, the ATCOs involved in the management of the contingency situation were firstly helped by the ACC Operational Chief and Supervisors. Then, additional help was provided by the ATCOs that were on break during the event. According to regulations, at least the 30% of the overall ATCOs workforce needs to be available during breaks. This is a standard 'buffer' representing a source of resilience available by design. For what concerns the technical resources, some support was offered by the so called *flight progress strips*. They are small strips of paper that contain the essential information of the flights in the area of responsibility of the ACC. They represent an older type of controlling tools that were used in the past when the controller working positions were less sophisticated and did not include all the information in digital format, as in todays' multi-radar tracking systems. Nowadays, the strips are only used in combination with the *fallback* system, i.e. a backup system which is automatically activated in case maintenance operations or radar loss, or on ATCOs request. During a typical radar loss scenario, the *fallback system* has the capability to process radar data independently from the main system and to display them in less sophisticated and smaller screens. However, also the screens of the *fallback* system were frozen during this event, therefore only the capability of printing the *flight progress strips* could be used. Finally, another technical resource was used to manage the contingency, despite not being anticipated at all by official procedures. This was a simulation and training platform, located next to the main operational room, whose screen was working properly. During this situation, one of the Supervisors intensively used it to help the ACTOs in controlling the traffic at their own working position, by providing them with constant updates on the position of individual flights.

3.3 Operational Margins

In order to face with the contingency situation, different strategies where put in place *to modify the normal operational margins*, also through negotiation with other air traffic control entities. For the sake of brevity, we here mention only two of them. The first one was actually implemented, while the second one came out not to be necessary, due to specific circumstances on that day.

The first strategy consisted in negotiating with some of the nearby airports a different altitude for the flights that were being transferred. For example, one of the major airports in the areas was used to take under its control the descending traffic received by ACC "A" at an altitude of 90.000 feet (about 27 Km). During the contingency, it was agreed that the ATCOs working in the Control Tower of that airport would have taken the control much earlier – i.e. at 200.000 ft. (about 60 Km) - in order to reduce the workload of the ATCOs of ACC "A". While the second strategy was the modification of the operational layout of the ACC "B" and "C". Both centres had their radar functionalities fully operating and could provide support to ACC "A". As mentioned before, the management of traffic is organized in sectors (i.e. specific volumes of airspace), each one controlled by a couple of ATCOs. When the traffic is very low, just a few sectors are sufficient. On the contrary, when the traffic is very high, the capacity of the ACC is increased by *opening* more sectors. In this case ACCs "B" and "C"

could have opened more sectors at the boundary with ACC "A", in order to have more ATCOs providing support to the centre affected by the radar loss. At the same time, they could have gradually *closed* one or two sectors in the airspace volumes farther from ACC "A", to compensate for the reallocation of their ATCOs in a different area. Such reconfigurations of the Air Traffic Control system are always possible and intrinsically make it more resilient. In that specific day, however, the second strategy was not needed as all the three ACCs had a sector configuration that exceeded the demand of traffic at that time of the day, because they were testing a new procedure.

4 DISCUSSION

The application of the principles of the DARWIN guideline and of the triggering questions included in the CC "Identifying Sources of Resilience" showed how it is possible to think about the resilience capabilities of an organization managing a critical infrastructure like the Air Traffic Control, when experiencing a major degradation of its automated systems. Interestingly enough, the identified sources of resilience concern both the reorganization of tasks and resources inside the same organization (the ACC "A") and the reconfiguration of resources in different organizations (the neighbouring ACCs, the regional airports and the Flow Management positions at local, national and European level). Some of the resilience strategies are already embedded in the design envelope of the system (e.g. 30% of ATCOs to remain available during the break), while other strategies were identified tactically during the development of the contingency (e.g. the use of the radar screen of the simulation and training platform located close to the operational room). Overall, the personnel of the affected ACC and of the other units showed important abilities to put in place strategies compensating for the lack of the automation support, which were not fully anticipated in the official procedures. The questions still remain open: should such capabilities be incorporated in the design of the system (e.g. via improvements to the equipment and the procedures) as a response to specific events? Or rather, should these capabilities be enhanced by training, encouraging out-of-the box thinking and generation of ad-hoc solutions by the personnel? There is, of course, no univocal response, but it is very important to be aware that both strategies are needed when dealing with degraded automation scenarios affecting critical infrastructure.

REFERENCES

DARWIN. Expecting the Unexpected and Know how to Respond. Deliverable D4.3 Pilot's Implementation and Evaluation (https://h2020darwin.eu/project-deliverables/).

Epstein, S., (2008). Unexampled events, resilience and probabilistic risk assessment. In Hollnagel, E., Nemeth, C., Dekker, S., Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the possibility of failure. (pp. 49-59) Aldershot, UK: Ashgate.

Hollnagel, E. (2017). Safety –II in Practice: Developing the Resilience Potentials.

Zeeb, K., Buchner, A., & Schrauf, M. (2015). What determines the take-over time? An integrated model approach of driver take-over after automated driving. Accident Analysis & Prevention, 78, 212-221.