CONNECTIVITY AND RESILIENCE OF REMOTE OPERATIONS: INSIGHTS FROM AIR TRAFFIC MANAGEMENT

***Matthieu Branlat*[1]**
***Per Håkon Meland*[1]**
***Tor Erik Evjemo*[1]**
***Anthony Smoker*[2]**

[1)] *Sintef Digital, Norway*
[2)] *Lund University School of Aviation, Sweden*

Abstract
Greater connectivity is transforming critical infrastructures profoundly. One specific aspect enabled by connectivity are remote operations, which allow for the provision of services difficult to provide in a direct capacity, physically (e.g., due to cost or resource availability). Domains of applications are very diverse, e.g.: industry, public services, healthcare, culture. In the domain of Air Traffic Management (ATM), increased connectivity is seen as one of the main drivers of the improvement of operations and building of capacity to handle the expected traffic increase. The concept of Remote Tower operations provides the capacity to manage tower operations remotely from a virtual tower and remote centre. It increasingly appears as a valuable alternative to traditional control towers. However, one can wonder about the risks introduced by the necessary reliance on network infrastructures and remote sensors. What happens to remote operations when these are not fully, if at all, functional? How dangerously dependent on the digital infrastructure are the capabilities introduced by remote operations? Such questions take particular significance in the face of the cyber threat: cyber-attacks on digital assets and services can impair the capacity to perform ATM safely from remote. Resilience then represents the capacity to handle two interrelated, but different, disruptions: of ATM operations; and of digital services. In the first case, the primary emergency, the system needs to adapt to mitigate the impact on operations (e.g., switch to other modes of operations or divert traffic) and return to sound operations. In the second case, challenges are associated with the system's capacity to identify, understand and address the cyber event. Re-establishing impaired digital services in a timely manner is critical because the adapted ATM operations are not sustainable. Inspired by crisis management, the paper explores challenges and strategies for resilient performance in the face of disruptions to the digital infrastructure.

Keywords: Connectivity, Cybersecurity, Remote operations, Air Traffic Management

ISBN: 978-91-88898-41-8

DOI: https://doi.org/10.15626/rea8.15

1. INTRODUCTION

Greater connectivity is transforming critical infrastructures profoundly. Cybersecurity experts point out that, as digitalisation and connectivity rapidly progress, the scale, complexity and exposure of networks becomes increasingly impossible to fully manage [1]. In other words, it becomes less and less possible to anticipate and build security barriers for all situations. The main consequence pointed out by these experts is that cyber events will occur in spite of organisations' best efforts – it is no longer a question of *if*, but a question of *when*. In addition to securing their systems and networks through traditional means, organisations providing or using digital services therefore need to consider how much they have the capacity to handle the two types of disruption mentioned above: (1) of the digital infrastructure itself; (2) of operations relying on the digital infrastructure.

One specific aspect enabled by connectivity is remote operations, which allow the provision of services difficult to provide in a direct capacity, physically (e.g., cost, resource availability). Domains of applications are very diverse, e.g.: industry, public services, healthcare, culture. Besides the operational relevance and benefits of such new capabilities, one can wonder about the demands and potential risks introduced by the necessary reliance on remotely networked sensors and actuators. What levels of coverage, reliability and integrity are required for the digital infrastructures for such capabilities to be envisaged in the first place? What happens to remote operations when these are not fully, if at all, functional? Can operations actually occur in degraded modes? How dangerously dependent on the digital infrastructure are the valuable capabilities introduced by remote operations? Such questions take particular significance in the face of the cyber threat, whether due to intentional cyber-attacks or network and systems' malfunctions.

In the domain of Air Traffic Management (ATM), increased connectivity is seen as one of the main drivers of the improvement of operations and building of capacity to handle the expected traffic increase. Remote Towers, a fairly novel concept of operations allowing controllers to provide air traffic services from remote locations, have recently started to be implemented in various areas of the world. Such concept illustrates the development of remote operations afforded by greater connectivity and digital capabilities. In this paper, we will draw from our investigation of this concept in order to discuss issues of resilience of remote operations relative to network disruptions (whether intentional or not). We will describe Remote Tower operations as well as elements of vulnerability to cyber events, and discuss how resilience frameworks can provide guidance to understand and address such events. Our ambition is that insights from this specific concept and domain inform the larger question of resilience in remote operations and other domains relying extensively on digital capabilities.

2. BACKGROUND

Remote operations have already been realised in a wide variety of areas, such as distributed or centralised control systems used in manufacturing, remote offshore drilling, driverless mining equipment, loading cranes, telesurgery [2] and remotely piloted aircraft systems (RPAS – commonly referred to as *drones*) [3]. A number of aspects seem characteristic of remote operations, especially:

- Geographic separation of operators from the environment or system they are operating on, requiring the transmission of sensing information from and control instructions to the remote location.
- Novel forms of contingency for perturbed operations.

- Often aimed at improving cost efficiency or shielding the operator from hazardous environments.
- Provides the means to group functions into one central location, thus achieving an economy of scale as well as new macro operational concepts
- The combination of different types of sensor data from the remote location, e.g. weather information, radar, lasers, infrared waves, noise, haptic information or system states.
- Typically, inclusion of data transmission with high bandwidth, real-time requirements, such as video/audio.

As a result of these characteristics, remote operations exhibit a high dependence on the digital infrastructure, such as network communication links, computer processing, remote and local technical equipment. The implementation of remote capabilities, however meaningful from operational and economic perspectives, therefore results in a transition from isolated environments to systems more exposed to cyber-attacks and other network disruptions. These disruptions might in turn lead to unwanted incidents with potential consequences to operational effectiveness, safety or physical assets.

2.1. The Remote Tower concept in ATM

The Remote Tower (RTWR) is a relatively novel concept of operations in ATM, which provides the capacity to manage tower operations remotely based on: (1) a tower equipped with various sensors (cameras especially) at the airport to be controlled; and (2) controllers accessing this information at a remote centre, which might be used to control multiple airports [4]. Remote Towers have been developed, tested and validated over the past 10-15 years. It is currently being implemented in various areas of the world (e.g., [5, 6]). Remote towers increasingly appear as a valuable alternative in the context of various business cases, in particular for airports located in remote areas and managing a limited amount of traffic.

Investigations around this concept have covered a variety of topics, such as innovative technologies to support air traffic controllers (ATCOs) manage traffic and assessments of impact of safety of operations. There are several scientific publications on different topics related to Virtual or Remote Tower operation. For instance, in 2006 Schmidt et al. [7] described task analysis and decision making when using augmented vision video panorama systems. Fürstenau et al. [8] compare real view with video panoramas in a field setting. Moehlenbrink and Papenfuss [9] investigate work place variables when controllers operate two airports in parallel. Van Schaik et al. [10] describe their experiences with remote technologies, such embedding the panoramic displays with visibility enhancement, contour lines, weather information and labelled objects (aircraft and ground vehicles). Josefsson et al. [11] identify complexity factors that impacts the mental workload for multiple remote control, however these factors are related to normal operations. Ellis and Liston [12] compares visual cues for anticipated separation in airport map displays and panoramic video. The most useful visual features involved aircraft motion, such as acceleration and deceleration. Wittbrodt et al. [13] have identified a set of communication challenges for remote airport traffic control centres, such that the continuous attention switching between different traffic situations is likely to increase the ATCOs' tasks in complexity and difficulty. Subotic et al. [14] define 20 *Recovery Influencing Factors* (RIFs) for air traffic controller recovery from equipment failures, e.g. complexity of the failure and experience with failures. They pointed out in 2014 that there had been little research on the topic of ATCO recovery from failure. For a detailed description of the evolution of remote tower operations, we refer to Kearney and Li [4]. They also pointed out that during 50 live trial exercises, there were no safety occurrences, but there is an increased likelihood of the controller missing a transmission by an aircraft or vehicle compared to traditional towers.

RTWRs were used in two settings as candidate ATM developments to examine the use of a new resilience engineering assessment method [15]. The two operational settings represented ATC and AFIS based ATM. Conclusions about the resilience performance of RTWRs noted among other things that: (1) the work system could become brittle if the ability to reconfigure positions was not supported, and (2) that any latency in the provision of real time instantaneous meteorological data could lead to increased taskload inducing time pressure of the flight deck as well as other actors. Fundamentally, the nature of the work of ATCOs in RTWR work systems is envisaged to be different from that which it replaces. This being a direct consequence of the new capability that network infrastructure makes possible. Realising this potential also introduces new fallback and degraded modes to learn and develop strategies to manage.

2.2. General approach to resilience

Following Hollnagel's general definition of resilience, we are interested in the "intrinsic ability of a system or organization to adjust its functioning prior to, during, or following changes, disturbances, and opportunities so that it can sustain required operations under both expected and unexpected conditions" [16]. In the context of tower operations in ATM, we are therefore interested in how ATCOs manage, in the face of variability and potential disruptions, to pursue through the provision of air traffic services the safe and efficient the safe guidance of aircraft and other vehicles around the airport in landing, take-off and ground operations, while minimizing the impact (e.g., disruption) on flight schedule.

For Remote Towers, a central issue is how interruptions or degraded modes in digital infrastructure and services might impair the capacity to perform ATM safely or effectively from remote. Resilience then represents the capacity to handle two interrelated, but different, disruptions: (1) of the digital services; and (2) of ATM operations. In the first case, we expect that challenges are associated with the system's capacity to identify, understand and address the variability and disruptions on the infrastructure that enables operations. In the second case, which represents the main operational emergency, challenges are likely to be associated with how the system can manage disruptions, particularly because of the context of the underlying infrastructure being only partially (if at all) available. Disruptions might also impact aircraft operations by creating communication delays and confusion on the flight deck.

Our understanding of the first problem is informed by previous research on resilience in cyber security operations (e.g., [17]). This work highlights a number of core challenges to cyber defence, especially: (1) to detecting and making sense of events on the network due to the scale, uncertainty and complexity of network activity; and (2) to addressing these events due to coordination cost and trade-offs between security and production goals.

3. UNDERSTANDING NETWORK DISRUPTIONS, IMPACT AND RESILIENCE IN REMOTE TOWER OPERATIONS

The content of this paper is based on an on-going investigation of cybersecurity threats and potential impact on Multiple Remote Towers. As mentioned previously, MRTWRs do not exist in operation yet, but prototype implementations are currently being validated using simulated traffic or in a shadow-mode of existing ATM operations. This section describes the conduction of and results from the various efforts to develop an understanding of: (1) the cyber threat; (2) expected operations; (3) potential impact of cyber events; and (4) challenges and opportunities for adaptation to variability, i.e. potential for resilience.

3.1. Cyber threats and potential protection measures

The investigation of threats for the RTWR concept took two main forms: a review of relevant documented cyber cases, and a participation in a cybersecurity assessment.

Given that the concept was recently put into operations, no cyber cases have been documented specifically on RTWRs. Overall, cyber security cases affecting ATM remain fairly rare. We can, however, find some examples of cyber events based on malicious intent. For instance, in 2006, the US Federal Aviation Administration's (FAA) ATC systems was infected by a computer virus and had to shut down a portion of it [18]. In 2012, it was demonstrated at the Blackhat conference that ghost (fake) airplanes could be injected into the ATC systems exploiting ADS-B vulnerabilities [19]. There were several occurrences of radar losses from ATC displays in central Europe in June 2014, which were probably due to denial-of-service attacks targeting the Secondary Surveillance Radar (SRR) system [20]. Furthermore, in 2015 the IT systems of the Polish airliner LOT got hacked and random flight plans were sent out to the airplanes [21]. According to the latest *Global Aviation Security Plan* by ICAO [22], terrorists find innovative ways to target systems and States must also address cybersecurity issues in addition to the more traditional risks.

More specifically related to remote towers, the authors participated in a cybersecurity assessment workshop. This assessment was focused on network security threats and protection measures for the MRTWR concept. Among the main conclusions, the remoteness of airports and equipment was found to create opportunities for creating disruptions (e.g., damaging sensors). Four main groups of protection measures were discussed to cover all the threat scenarios: physical protection of the equipment and sensors; correct implementation of logical perimeter security functions; implementation of Security Best Practices (e.g., ISO/IEC 27002); monitoring and inspection of the site, rooms and equipment. It is worth noting that these measures are typically already addressed through the security measures in airport infrastructures and Single RTWR solutions (including network assets and communication channels) that are part of the context of implementation of the MRTWR concept.

Disruptions to the digital assets and infrastructure can, in addition to intentional acts, take different forms with a variety of consequences, such as common technical failures, accidents or human mistakes. Remote towers are for instance implemented in Scandinavian areas where harsh weather conditions can regularly hinder the operation of cameras and other sensors (e.g., ice build-up due to freezing rain). Digital networks also make data available to the aviation industry as a whole, disruptions impacting more stakeholders than ATM operators alone.

3.2. Remote Tower operations

The concept of Single Remote Tower (SRTWR), in which *one* controller manages *one* airport from a remote centre, is already being implemented in various areas of the world. On the other hand, the concept of Multiple Remote Tower (MRTWR), in which *one* controller manages *multiple* (up to 3) remote airports, is under development: technical platforms have been developed by different manufacturers and validated with actual controllers in simulated environments, but MRTWRs do not exist yet at a level of operational maturity. As a result, for the different solutions that have been developed, technical systems are still being tested and improved (e.g., specific aspects of interface design) and a variety of questions relative to operational conditions are still being investigated (e.g., organisational aspects such as roles and resources in Remote Tower Centres).

A Remote Tower Centre is equipped with controller workstations that implement Remote Tower Modules (RTM) to control airports from remote. For each airport, the traffic and activity (air and ground) can be monitored and managed primarily based on:

- Overhead video displays combining video feeds from multiple cameras to provide a wide field of view of the airspace and runways/taxiways;

- an e-strip (electronic flight strip) display, typically, to manage incoming and departing traffic, as well as ground movements on the runway, taxiways and tarmac – this display is informed automatically from flight planning for planned traffic, and updated manually for additional activity (e.g., VFR traffic, ground movements);
- a radar display covering radar information coupled with flight planning information for traffic around the airport;
- a communication display to select/show appropriate channels of communication.

In the context of MRTWR, an RTM operated by one controller, can combine up to 3 airports through dedicated displays (i.e., the video, e-strip and radar displays for the different airports are separated – however, the voice channels may be merged for inflight communication). As a whole, a MRTWR operation may have air traffic services provided to three or more airports from the multiple remote tower facility.

Observations, Q&A sessions and informal interviews during validation exercises and demonstrations of MRTWR (simulated environments, real ATCOs) generated a number of insights about future operations:

- Parallel activity in 3 airports is challenging, ATCOs suggesting a significant difference between parallel control of 2 and 3 airports. Parallel traffic can be a source of confusion for ATCOs and potentially for the crew of managed aircraft. Ways to lower confusion include for instance the use of improved phraseology. It has to be noted, though, that simulated conditions tested traffic levels significantly higher than expected future operational conditions.
- The capacity to transfer airports from one controller to another offers flexibility to deal with the variability of traffic. However, it creates new coordination challenges as ATCOs need to manage such handoffs effectively, i.e. determine appropriate times (for themselves and other ATCOs) to operate handoffs, conduct handoffs efficiently to minimise risks of interruption due to other activities, etc.
- Various technological capabilities are under development to address these challenges, such as time-based activity displays to better anticipate potential workload peaks.
- Many organisational questions remain open and will be clarified as the concept gets closer to operation (validation efforts aim at uncovering such issues), for instance how to organise a supervisor role in different centres or how to address certification needs in remote centres to ensure flexibility between ATCOs.

3.3. Exploring the potential impact of cyber events and resilient performance

The following vignette is a fictional scenario constructed based on the knowledge generated from various sources, especially: (1) understanding of envisioned MRTWR from the different activities described above; (2) previous investigations of resilience in SRTWR; and (3) research on cyber security. The scenario captures elements of the expected operations in the context of Multiple Remote Tower, as well as potential disruptions.

On 24/06 at 10:00, ATCO1 is providing ATM to two airports (AERO1, AERO2) simultaneously while ATCO2 is controlling AERO3. AERO1 and AERO3 are small airports with a single runway, usually less than 1 planned movement per hour and limited VFR flights. AERO2 is a small airport with little planned movements, but higher VFR activity during nice weather.

10:25 – ATCO1 observes 2 incoming aircraft on the radar display for AERO1: LAND1 is on approach, expected in about 5 min, while another aircraft, LAND2, recently appeared on the radar – besides the call sign, altitude and flying vector, no flight plan or information is visible. Aircraft DEP1

is scheduled to depart from AERO1 in 10 min. In parallel, at AERO2, a VFR aircraft has communicated a plan to land in about 10 min.
10:27 – ATCO1 has been communicating with the various aircraft, but still does not see information for LAND2 on the radar or e-strip display. ATCO1 attempts to address LAND2 on the tower frequency, but is still unable to establish communication with the aircraft. In anticipation for having to manage multiple planes at AERO1, ATCO1 wants to transfer the control of AERO2 to ATCO2.
10:28 – ATCO1 clears LAND1 for landing at AERO1 and contacts ATCO2 for transferring control of AERO2. ATCO2 is busy and does not answer immediately. ATCO1 contacts the Area Control Centre for the region to gather information about LAND2, but they are not aware of the aircraft.
10:30 – ATCO2 replies and accepts the control of AERO2. The two controllers initiate the handoff, ATCO1 describing expected movements (VFR flight only). In the meantime, ATCO1 monitors LAND1 landing at AERO1 on the video display. ATCO1 interrupts the handoff to provide taxi information to LAND1.
10:31 – ATCO1 resumes handoff of AERO2 and confirms the transfer to ATCO2 RTM.
10:32 – Aircraft DEP1 contacts ATCO1 to get clearance for take-off in the coming minutes. The displays still do provide information about LAND2, and communication attempts remain unsuccessful. Based on position and progression in the past minutes, it now appears less than 5 min from landing. ATCO1 puts DEP1 on standby, hoping to coordinate with LAND2 first.
10:33 – ATCO1 starts being surprised not to observe LAND2 on the video feed given the clear conditions and proximity; the controller wonders whether some cameras at AERO1 are experiencing technical problems. ATCO1 calls the technical engineer, describes the problem and asks to confirm all cameras are operational.
10:35 – DEP1 is still on standby and is getting impatient. The technical engineer, having run a quick diagnosis, calls back to inform ATCO1 the video system is working properly. Suspecting an issue with LAND2 equipment, ATCO1 contacts emergency personnel at AERO1 to have them ready to intervene.
10:37 – According to radar information, LAND2 is now landing. ATCO1 calls AERO1 ground personnel, who explain they cannot observe any aircraft. All of a sudden, LAND2 disappears from the radar display. During the following 10 min, ATCO1 interacts with AERO1 ground personnel to try to understand what is happening, confirm no plane is indeed there and to finally clear DEP1 for departure.
In the following days, forensics analyses of network activity reveal that the ATC system *might* have been compromised, leading to the appearance of a "ghost aircraft" on the radar display.

The vignette is a way to explore the impact of potential disruptions on digital services, a topic which was beyond the scope of the security assessment. For a concept still under development, building such vignette allows to anticipate how the system might adapt to the variability introduced by disruptions and, importantly, which challenges might exist to these adaptations. In other words, the vignette serves as a means to go beyond common approaches to safety or security focused on threats and barriers, and to investigate the resilience of the system. The following points emerge from the scenario:

(1) Identifying that an event is occurring takes time and extra resources. The ATCO needs to devote attention to the situation, and to coordinate or engage with a multiplicity of other actors to make sense of events, impacting his/her ability to sustain concurrent provision of ATS.

(2) Extra resources are difficult to produce, especially in the context of parallel activity. The controller's capacity is indeed already stretched (attention, tasks) as he/she is operating at different locations.

(3) The MRTWR concept supports new forms of adaptive capacity. While a source of parallel activity, the MRTWR concept also offers some flexibility to offload some of the tasks, through the capacity to transfer the control of airports

(4) Implementing this form of adaptation has, by itself, an additional coordination cost. The coordination necessary to transfer airports might indeed interfere with operators' other tasks and goals

Supporting resilience then involves supporting the system's ability to address challenges or seize opportunities similar to the ones described above. Means of interventions include the design of technology, the development of operational processes and resources, or the implementation of learning activities at the organisational and individual levels.

4. DISCUSSION: POTENTIAL DIRECTIONS TO ENHANCE RESILIENCE

4.1. Cyber resiliency for Multiple Remote Tower operations

Compared to traditional resilience, cyber resiliency is more focused on adverse conditions and the abilities to *anticipate*, *withstand*, *recover* and *evolve* from malicious cyber activities [23]. In Table 1, we have mapped the proposed cyber resilience techniques from NIST SP 800-160 [24] with relevant implementation approaches we have observed during validation exercises for Remote Tower operations. We have also identified a set of domain specific challenges for each of these techniques, that can potentially create a conflict with others.

Table 1. Cyber resiliency approaches for remote towers

Techniques from NIST	*Observed implementation approach*
Adaptive response: *Implement nimble cyber courses of action to manage risks.*	• The ability to dynamically transfer the control of airports to other modules or a contingency site without interrupting the service. • Deployment of additional resources (ATCOs) to increase the capacity of handling simultaneous movements. • Supervisor role to control adaptive allocation of airports to ATCOs. • There is always a fallback or degraded mode of operations that should maintain the same safety level. **Challenge:** The overhead of reconfiguration can itself lead to additional strain and increased complexity.
Analytic monitoring: *Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.*	• A supervisor role to monitor changes in the operational environment. • Correlate data from different remote sensors, such as radar, automatic dependent surveillance broadcast (ADS–B) and visual monitoring. • Dedicated network monitoring position at the remote tower centre. **Challenge:** Multiple sensor data takes extra attention from the ATCO.
Coordinated protection: *Ensure that protection mechanisms operate in a coordinated and effective manner.*	• Contingency sites with independent network capabilities. • Actively use simulation centres for training exercises and validation of new procedures. • Civil aviation authorities in different countries share experiences with unwanted incidents (real and exercise results). **Challenge:** It is difficult to simulate and train on unwanted incidents.
Deception: *Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.*	• Obfuscation/encryption of data between RTWR and control centres. • Secretly placed contingency/emergency sites. **Challenge:** Security by obscurity has a limited effect, it is necessary that communication links are open to provide situational awareness to all pilots nearby the airport.
Diversity: *Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.*	• Provide information diversity using different remote sensors. • Fallback solutions based on different technologies. • Establishment of path diversity using alternate network services with separated physical infrastructures. **Challenge:** Heterogeneity increases complexity and potentially creates a larger attack surface. Maintaining a heterogenous digital infrastructure increases costs.

Dynamic positioning: *Distribute and dynamically relocate functionality or system resources.*	• The ability to redirect aircraft to other airports not affected by unwanted incidents. • Laptop version of control modules that can be operated outside the control centres as additional contingency options. • Mobile remote towers placed on vehicles. • Reconfiguration of panorama views; change of screens, angles, augmented information. **Challenge:** It can be difficult to get approval from aviation authorities for dynamic functionality. Reconfigurations can be resource demanding.
Dynamic representation: *Construct and maintain current representations of the posture of missions or business functions considering cyber events and cyber courses of action.*	• Dynamic monitoring of virtual and physical threats through surveillance systems. • e-strip-based systems that represent the current state of mission critical resources. **Challenge:** Traditional systems do not capture cyber events or states. Voice-based information sharing ("All systems are in order").
Non-persistence: *Generate and retain resources as needed or for a limited time.*	• ATCO-pilot communications are short sessions. • Only the necessary STRIPS are shown to the ATCO. **Challenge:** It is mandatory to maintain records of everything that happens.
Privilege restriction: *Restrict privileges based on attributes of users and system elements as well as on environmental factors.*	• ATCOs must be endorsed for specific remote airports and types of air traffic services, creating operational privilege restrictions. **Challenge:** There is currently no authentication of ATCOs. Also, identities from secondary radar systems (transponder-based) are easy to manipulate and no digital authentication of pilots is implemented via VHF radio.
Realignment: *Align system resources with core aspects of organizational missions or business functions.*	• Strict restrictions on software installs within control centres. • Mandatory certification or approvals of equipment, software and update procedures. • It is possible to dynamic configuration of user interface to provide only essential capabilities (less *bells and whistles*). **Challenge:** Focus on critical functions might conflict with other techniques and goals (diversity, rich technical features).
Redundancy: *Provide multiple protected instances of critical resources.*	• Standby control modules in the control centres. • Physical contingency cites, typically the training sites. • Additional control towers/cameras at remote airport locations. • Use of ACC as contingent facility **Challenge:** same as *Diversity*.
Segmentation: *Define and separate system elements based on criticality and trustworthiness.*	• Separate sub-nets for connecting to different security domains • Various sensor data and communication systems have different levels of criticality and trustworthiness. **Challenge:** For remote tower operations, the datalink is the single point of failure for almost all system elements.
Substantiated integrity: *Ascertain whether critical system elements have been corrupted.*	• Trusted provenance of mission critical external data, such as weather information and flight plans. • Security through voice context, deviations from phraseology can indicate adversary man-in-the-middle attacks over VHF radio. • Coordination with various roles (e.g., personnel at remote airport, ACC). **Challenge:** With increased features and complexity, there could be many sources of failure/corruption, i.e. increased difficulty to verify information.
Unpredictability: *Make changes randomly or unpredictably.*	**Challenge:** Random changes are difficult to implement in an aviation setting.

4.2. A closer look at some cyber resiliency approaches

Consider ATCO1 in the fictional scenario. As LAND2 appears to be closing in on AERO1, ATCO1 is following the flight progress on the approach radar screen. An initial call to the area control (ACC) provides no help in identifying the approaching aircraft and one can argue that the situations' complexity on part of ATCO1 is increasing. This is because of increased uncertainty, and the need for identification implies that other tasks get less attention causing the system to experience less slack, or redundancy. According to the *adaptive response* approach (Table 1), a resilient capacity for MRTWR in this situation would be to deploy an additional ATCO with the sole task of identifying LAND2. However, there is no extra ATCO or supervisor role available at present to locally support ATCO1, i.e. to only carry the identification task. A transfer of control is not an ideal solution either since ATCO2 would then inherit the entire situation of AERO1 in addition to AERO3. A possible way of supporting resilience based on adaptive response might be to allow distributed ATCOs to support each other by simultaneously working the same airport without explicitly splitting or merging, thus allowing for flexible airport control sharing and concurrent work for limited periods of time. Thus, there is no quick fix to reduce complexity by applying adaptive response as reconfiguring resources can itself result in additional strain and hence increase complexity. The supervisor role might be a key resource in such situations to shield the ATCO and take tasks away, and also control the tempo of work – which requires developing various skills and strategies.

The above challenges are relevant also in the context of *analytic monitoring* since to individually monitor and continuously analyse system behaviour can be demanding, especially when situations arise where there is an increasing degree of uncertainty, something we see when ATCO1 needs to clarify LAND2's intentions. However, a distinct supervisor role to monitor and coordinate resources could help to support the ATCO and mitigate uncertainties in order to keep situational complexity within acceptable boundaries. However, the task load in these situations is such that there is likely a need to double the supervisor task so that one looks after the event while the other looks after the operation. Overall, the supervisory role needs to be designed so that it supports a much broader range of anomaly response than currently.

Considering *coordinated protection*, this means for the MRTWR concept to provide for independent network capabilities within contingency sites, while actively training and simulating how to effectively handle unexpected events. The situation with the "ghost plane" illustrates Weick and Sutcliffe's notion of "unexpected" [25], including the unimaginable, which is closely related to if and how one has trained on similar scenarios in advance. This is very important in an MRT concept when events are escalating, i.e. the ability to handle complex situations through preparation and behind ahead. Thus, strategic use of training centres can potentially reduce MRT complexity.

In the scenario, ATCO1 becomes surprised when LAND2 does not materialise visually via the video feed. However, ATCO1 can only conclude that something is wrong and needs outside help to clarify whether the error is due to e.g. technical problem with a camera. In terms of *diversity* it could mean that one retrieves ATM information from different sensors, and to design for backup systems using various technologies. On the other hand, increased differentiation can lead to a paradoxical increase in complexity, including vulnerability to cyberattacks due to a larger attack surface. At the same time, more diversification also entails increased costs. The same argumentation applies to the principle of *redundanc*y, which involves several technical or organisational layers of protection, for example standby control modules in MRT centres, physical contingency sites or extra cameras at the remote airports. As for complexity, redundancy can result in both reduced complexity but also increased. For example, this may be

related to how quickly redundant capabilities help to deal with unexpected and or unclear operational situations.

4.3. Managing resilience for remote operations

The vignette in section 3.3 above also suggests that resilient performance is fundamentally based on a number of intra- and inter-organisational sensemaking, adaptation and coordination processes, which share similarities with aspects of crisis management. This view of resilient performance has been described in the form of fundamental challenges to adaptation in complex work systems [26]. Resilience management guidelines have been developed recently, consistent with this view and targeting organisations operating critical infrastructure [27, 28]. These guidelines propose several concrete interventions relevant to the situations described in this paper and which complement at the organisational level the techniques proposed by NIST, those being more focused on cyber issues. In particular:

- Methods for *resilience assessment*, such as workshops in which stakeholders discuss scenarios such as the fictional one above, can help organisations understand and identify sources of resilience (e.g., flexibility provided by the capacity to transfer an airport between controllers in case of emergency) as well as sources of brittleness (e.g., unmanaged cost of coordination associated with transfer of airport).
- Approaches to better consider *adaptation* in the organisation, for instance by purposefully setting up training exercises that include surprising factors and require innovative ways of operations, as well as by maintaining "old ways" of operating (e.g., paper-based) to guide operations when the digital services are not fully functional.
- Interventions to improve the conditions for *coordination* within and between impacted organisations, for instance collaborative events aimed at identifying potential gaps in common ground between organisations and clarifying the roles and responsibilities involved in the response to cyber disruptions.
- Approaches to *training* for both operational and non-operational actors (e.g., remote tower ATCOs, supervisors and technical staff) with the formal objective to develop strategies that can be deployed when anomalies such as cyber-attacks take place. Such training provides the basis for coherent approaches to the strategies that can be developed and deployed as well as to prime an informed approach to developing an understanding of the situation that supports an agile and flexible mindset.
- Developing a capability at the operational level of the organization to escalate from an orthodox approach to anomaly response and degraded modes to one that is better equipped to deal with the intricate and complex nature of disruptions to the digital infrastructure and the inherent uncertainties that cyber events introduce.

5. CONCLUSION

A stated objective of the development of the Remote Tower concept is that operational and safety performance is at least as high as in conventional towers [6]. Our investigation is still at an early stage and further work is needed to identify challenges and approaches to resilient performance in remote ATM operations. Such work can be based on fictional scenarios such as the one presented in section 3 (which can be used in different settings, such as simulated exercise, table top exercise or workshop with stakeholders).

However, the insights described here already raise a number of issues relative to the resilience to network disruptions. Interruptions or degradations of the digital infrastructure and services can impair the capacity to perform ATM safely or efficiently from remote. Resilience then represents the capacity to handle two interrelated, but different, disruptions: (1) of the digital

services; and (2) of ATM operations. In the first case, challenges are associated with the system's capacity to identify, understand and address the cyber event. In addition, reestablishing impaired digital services in a timely manner is critical because ATM operations performed in a degraded mode risk not being sustainable with regard to safety and/or costs. In the second case, which constitutes the primary emergency, the system needs to adapt and mitigate the impact on operations (e.g., switch to other modes of operations, reduce or even divert traffic to alternative airports) before returning to sound operations.

More generally, the resilience engineering conceptual framework, methods and tools appear particularly well-suited to approaching the question of reliance, and potential risks of dependency, on digital infrastructures. More specifically, insights are generated from the focus on adaptation to variability as well as from uncovering the challenges (organisational, technical) to adaptation. One of the main features of discussion about resilience is that it requires the broadening of the system of interest to include a larger set of stakeholders and actors and investigate larger system interdependencies. Implications include requirements or directions for the design of the underlying technology (e.g., design of control room and interfaces supporting sensemaking and coordination) as well as identification of new forms of adaptation and potential approaches to the organisation of work.

ACKNOWLEDGEMENTS

This paper is based on the authors' work in project PJ05. The PJ05 project is co-financed by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Programme. Opinions expressed in this work reflect the authors' views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

REFERENCES

1. Bochman, A., *Internet Insecurity.* Harvard Business Review, 2018.
2. Meng, C., et al. *Remote surgery case: robot-assisted teleneurosurgery*. in *IEEE International Conference on Robotics and Automation, 2004. Proceedings. ICRA'04. 2004*. 2004. IEEE.
3. Creutzburg, R., *European activities in civil applications of drones: an overview of remotely piloted aircraft systems (RPAS)*. SPIE Sensing Technology + Applications. Vol. 9497. 2015: SPIE.
4. Kearney, P. and W.-C. Li, *Multiple remote tower for Single European Sky: The evolution from initial operational concept to regulatory approved implementation.* Transportation Research Part A: Policy and Practice, 2018. **116**: p. 15-30.
5. AirportTechnology. *Remote control: investigating the UK's first digital ATC tower.* 2018 [accessed 05/05/2019]; Available from: https://www.airport-technology.com/features/cranfield-digital-atc-tower/.
6. AVINOR. *Remote Towers: the technology of the future at Norwegian airports.* [accessed 05/05/2019]; Available from: https://avinor.no/en/avinor-air-navigations-services/services/remote-towers/.
7. Schmidt, M., et al. *Remote airport tower operation with augmented vision video panorama HMI*. in *2nd International Conference Research in Air Transportation*. 2006.
8. Fürstenau, N., et al., *Steps towards the virtual tower: remote airport traffic control center (RAiCe).* 2009. **1**(2): p. 14.

9. Moehlenbrink, C. and A. Papenfuss. *ATC-monitoring when one controller operates two airports: Research for remote tower centres*. in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 2011. Sage Publications Sage CA: Los Angeles, CA.
10. Van Schaik, F., et al., *Advanced remote tower project validation results.* 2010. **43**(13): p. 135-140.
11. Josefsson, B., et al., *Identification of Complexity Factors for Remote Towers.*
12. Ellis, S.R. and D.B. Liston, *Static and motion-based visual features used by airport tower controllers: some implications for the design of remote or virtual towers.* 2011.
13. Wittbrodt, N., A. Gross, and M. Thüring, *Challenges for the communication environment and communication concept for remote airport traffic control centres.* IFAC Proceedings Volumes, 2010. **43**(13): p. 129-134. https://doi.org/10.3182/20100831-4-FR-2021.00024
14. Subotic, B., et al., *Controller recovery from equipment failures in air traffic control: A framework for the quantitative assessment of the recovery context.* 2014. **132**: p. 60-71.
15. SESAR, *Application of resilience & robustness guidance to remote tower and ASAS. Resilience Engineering Final Deliverable, WP16.06.01b*. 2016, SJU: Brussels.
16. Hollnagel, E., *Safety-I and Safety-II : The Past and Future of Safety Management.* 2014, England: Ashgate Publising Limited.
17. Branlat, M., A. Morison, and D.D. Woods, *Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cyber security exercise*, in *ASNE Human Systems Integration Symposium*. 2011: Vienna, VA.
18. London Cyber Security (LCS), *Hackable at any height*. 2015.
19. Costin, A. and A. Francillon, *Ghost is in the Air(Traffic)*. 2012: BlackHat USA 2012.
20. EASA, *Detection losses in Central Europe on the 5th and 10th of June 2014*. 2014, European Aviation Safety Authority
21. Zetter, K., *All airlines have the security hole that grounded Polish planes*, in *WIRED*. 2015.
22. ICAO, *Global Aviation Security Plan:*. 2017.
23. Bodeau, D.J. and R. Graubart, *Cyber Resiliency Engineering Framework*. 2011, MITRE.
24. Ross, R., et al., *NIST Special Publication 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. 2018, NIST.
25. Weick, K.E. and K.M. Sutcliffe, *Managing the unexpected: Resilient performance in an age of uncertainty*. Vol. 8. 2011: John Wiley & Sons.
26. Woods, D.D. and M. Branlat, *Basic Patterns in How Adaptive Systems Fail*, in *Resilience Engineering in Practice*, J. Pariès, D.D. Woods, and J. Wreathall, Editors. 2011, Ashgate: Farnham, UK. p. 127-144.
27. Branlat, M., et al., *Supporting resilience management through useful guidelines*, in *7th Resilience Engineering Association Symposium*. 2017: Liège, Belgium.
28. *DARWIN Resilience Management Guidelines*. [accessed 05/05/2019]; Available from: https://h2020darwin.eu/wiki/.