Designing Graceful Degradation into Complex Systems: The Interaction Between Causes of Degradation and the Association with Degradation Prevention and Recovery

Tamsyn Edwards[1]
San Jose State University/NASA Ames Research Center, Moffett Field, CA, 94035

and

Paul Lee[2]
NASA Ames Research Center, Moffett Field, CA, 94035

System resilience is critical to safety in air traffic control. An important element of maintaining resilience is the ability of systems to degrade gracefully. Of the available graceful degradation research, a majority of studies have focused primarily on technological causes of degradation only, limiting an ecologically valid understanding of the causes of degradation in air traffic control, and the preventative and mitigative strategies that enable graceful degradation. The current study aimed to address this research gap by investigating causes of degradation in air traffic control across the broad categories of technology, the environment, and the human operator, and the potential interactions between these causes. 12 retired controllers participated in semi-structured interviews focused on previous experience of causes of degradation and mitigation strategies. Findings provide an understanding of causation of degradation in air traffic control, and the prevention and mitigation strategies that moderate the relationship between cause and system effect. Findings confirmed that causes appear to interact to create compound, multiple effects on overall system performance. Findings also revealed prevention and mitigation strategies utilized to moderate the effect of the cause on the system. In order to gain an ecologically valid understanding of the causes of degradation, and effective prevention or mitigation strategies, causes from multiple categories, and the interactions between them, must be identified. Findings have implications for designers of future air traffic control systems to ensure the ability of the system to gracefully degrade, as well as risk assessment and system validation processes.

I. Introduction

WITHIN the air traffic domain, initiatives such as the US-focused NextGen and the Single European Sky Action Research (SESAR) program in Europe are enabling significant change in air traffic management operations. Technological advancements, increased focus on automation, airspace redesign and a redefinition of the control operations are a few of the areas that may be impacted. With such fundamental change to the air traffic management system expected in the near future, system safety and resilience [e.g. 1] is a critical concern. An important element of maintaining system safety and resilience in air traffic is the ability of systems to 'degrade gracefully'. A system that is designed to degrade gracefully can "tolerate failures by reducing functionality or performance, rather than shutting down completely" [2, p111], a necessity in a domain in which there are no physical barriers or defenses to protect aircraft in flight. It is therefore essential that the future air traffic system is designed to have the capability to degrade gracefully.

---

[1] Senior Research Associate, Human Systems Integration Division, NASA Ames Research Center, Mail Stop 262-4, Moffett Field, CA 94043, AIAA Member.
[2] Senior Research Engineer, Human Systems Integration Division, NASA Ames Research Center, Mail Stop 262-4, Moffett Field, CA 94043.

Of the available graceful degradation research, especially within the complex human-machine systems such as air traffic management (ATM), a majority of studies have focused primarily on the impact of technological causes of degradation and the ability of technology to prevent degradation. Although these research areas have provided excellent insight into the role of technology in gracefully degradation, non-technological causes of degradation (such as those arising from a non-optimal environment or from human operators), as well as contributions to degradation prevention or recovery, have been relatively neglected [3]. In an environment such as ATM, environmental factors, technological systems, and human operators are highly interconnected and can all influence the ability of a system to degrade gracefully. The current understanding of gracefully degrading systems is therefore largely out of step with real-world contexts, preventing an ecologically valid understanding of the causes of degradation, the tools and methods that prevent system degradation, and recovery of the system online.

After a systematic review of literature relating to graceful degradation in complex systems, [3] applied a human-systems integration approach to develop a framework of graceful degradation. This framework suggested that there were four main elements of graceful degradation – a degradation cause, identification of the degradation, prevention of impact on the system, and, if degradation occurred, recovery of nominal operations. Findings revealed that causes of degradation could be broadly categorized into technological fault or failure, the environment, or human operators. The review identified that research within each of these categories is highly independent and did not cross domains. As a result, the potential interaction between the causes of degradation, and the resulting possible compound effect on the entire system, was under-researched. In addition, [3] identified a gap in research relating to the contribution of human operators in a gracefully degrading system. Human operators such as controllers, were expected to prevent degradation, or recover a degrading system once technological solutions were no longer viable, such as in aircraft emergencies, and failures or faults in software and hardware. However, the specific techniques or approaches used by human operators to contribute to degradation prevention or system recovery, were under-specified. As a result, understanding was limited regarding the performance limits of the human operator, and the conditions under which human operators would, or would not, be able to contribute to the prevention of degradation, or recovery of a degraded system.

The current research aimed to contribute further understanding to the research gaps identified by [3], and review and extend the proposed framework of graceful degradation. Causes of degradation were defined broadly, as events that had the potential to negatively affect the wider ATC system in terms of safety and/or efficiency without mitigation.

The current research had four specific aims. First, the research aimed to investigate causes of degradation in air traffic control (ATC) across all categories of technology, environment, and human, and the association with controller performance and the ATC system. A second aim was to investigate the relationship, and potential interactions, between potential causes of degradation across technology, environment and human operator categories, and the subsequent association with controller performance. The research also aimed to inform fundamental understanding of prevention and mitigation of degradation in the current ATC system, with a specific focus on the contribution of air traffic controllers (ATCOs). A final aim was to inform understanding of the factors that could negatively affect the ability of an ATCO to prevent degradation or recover a degraded system. To address the aims, a qualitative interview exercise was conducted with retired en-route and TRACON ATCOs. Two specific forms of knowledge elicitation techniques were used; a semi-structured interview that focused on participants' past experience of ATC, and a scenario-focused knowledge-elicitation exercise. The use of multiple techniques allows weaknesses of individual techniques to be addressed, as well as adequately addressing separate study aims. Finally, the use of multiple techniques has the advantage of collecting data in different ways to inform the same aim, potentially providing a more detailed understanding.

II. Method

A. Design

A total of 12 retired TRACON and en-route controllers participated in two qualitative exercises, totaling 2.5 hours. Participants volunteered for the study, creating a self-selected sample. All participants were required to have experience in an en-route or TRACON environment. The number and length of exercises, as well as the number of participants, was based on pragmatic considerations. The first exercise was a semi-structured interview relating to the controllers' previous experience, lasting one hour in length. In the first exercise, participants were first asked about their experience of the common causes that could result in system degradation. Participants were then asked to list, in their experience, both existing practices for how these causes can be mitigated, and also their strategies for mitigating system degradation impacts.

The second exercise utilized a semi-structured interview methodology, although this time responses were targeted to specific scenarios. The objective of this exercise was to investigate the occurrence and of interactions between

causes of degradation. Controllers were asked how a specific technological failure would be likely to impact performance, and then how a specific environmental event would impact performance. Controllers were then asked about the possibility and likely outcome of these two examples occurring together.

A protocol was used to standardize the interview procedure for both exercises. Interview schedules were developed to guide the semi-structured interview; participants were asked pre-designed lead questions which were then followed by probes. The two independent qualitative exercises provided different benefits to the study. As the first exercise related specifically to controllers' experience, this provided breadth of information and enhanced generalizability of the data. However, as the information was based on experience, there was also a possibility that the controllers' experience would be so diverse that comprehensive data on specific topics may not be gained. The second qualitative exercise was used to address this potential limitation, in which questions were focused on specific air traffic scenarios. By grounding the questions to the same scenario for all controllers, it created the opportunity for the comparison of data between each scenario.

B. Participants

In total, 12 retired TRACON and en-route controllers were interviewed. All participants were male. This was a result of the convenience-based sampling method, and not through design. All participants worked as en-route controllers in California. Participants have been based in one of three areas: San Francisco Bay TRACON (2 controllers, 17%), Oakland en route center (9 controllers, 75%) and Los Angeles center (1 controller, 8%). Participants' ages ranged from 51-72. Participants responded to grouped age ranges and so an average age could not be calculated. A total of five participants (41.6%) were in the 51-60 ages range, six participants (50%) were in the 61-70 age range. One participant (8.3%) responded to the 61-72 age range. All participants were qualified ATCOs who had completed training. Years of experience as an ATCO (excluding training) in TRACON and En-route control ranged from 10-35 (M=27.42, SD=7.82). All 12 participants had worked as an on the job training instructor (OJTI). Years of experience as an OJTI ranged from 15-33years (M=25.45, SD=7.88). In total three participants were also supervisors. Experience as a supervisor ranged from 3 to 17 years (M=11 years, SD=7.21).

C. Materials and Equipment

Exercise 1: Semi-structured interview

An interview schedule was designed to structure the interview. The interview comprised of 12 lead, open-ended questions which related to five areas of interest:

1. Impact and recovery of environmental off-nominal events (e.g. thunderstorm, aircraft emergency)
2. Impact and recovery of tool or automation failures (e.g. Radio or radar failures, conflict probe errors)
3. The occurrence and impact of Interactions between environmental and technological off-nominal event
4. Strategies to recover degradation
5. Association of human factors (workload, fatigue, teamwork, situation awareness) with ATCO performance

Lead questions were arranged from general topics (e.g. "Could you please tell me about a time in the recent past when you experienced a non-optimal environment, such as a thunderstorm or aircraft emergency") to more specific questions (e.g. "What are your control strategies for off-nominal situations?"). Examples of common causes of degradation (technical and environmental) were used in the lead question to facilitate participants' understanding. The same indicators were used in examples for all participants [4].

Exercise 2: Semi-structured interview – Scenario based

The second exercise utilized four scenarios in order to explore specific causes of degradation, and the occurrence of interactions between causes. Scenarios were developed in collaboration with two ex-controllers to ensure appropriate exercises and realism. The sector, traffic flows and level of traffic remained constant between scenarios. Only the control environment scenario was changed. Participants were provided with a sector map and traffic flows (Figure 1) and told that the traffic load was moderate-high, with 20 aircraft in sector. Participants were read a specific scenario and asked to imagine the control situation based on the information given and their previous experience. Participants were asked the same series of questions for all scenarios.

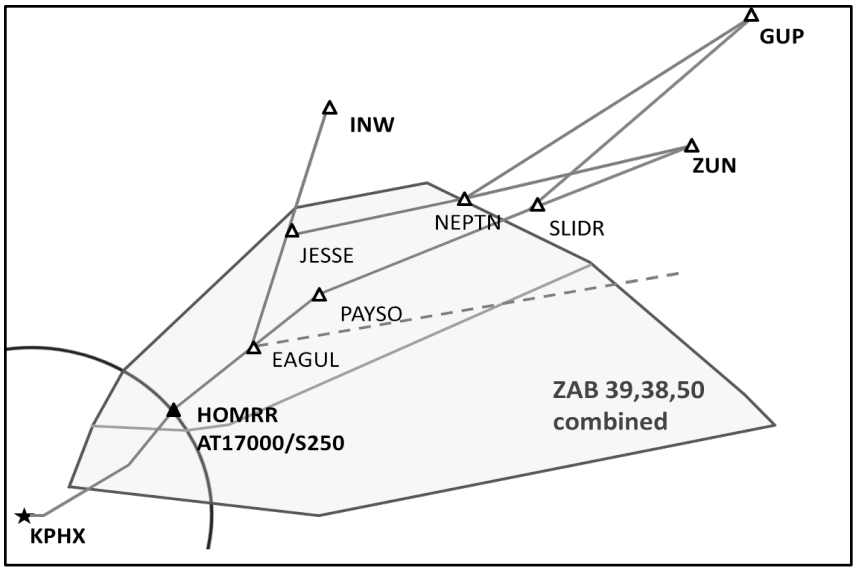

Figure 1. Sector and traffic flow map

The first scenario was a baseline scenario, with optimal sector conditions, and no technological failure. The second scenario related to datalink technological failure. The third scenario described a non-optimal sector environment of a large thunderstorm reaching to 40,000ft and moving across the sector, blocking several traffic flows. The final scenario described a situation in which there was a thunderstorm as previously described, plus the loss of datalink technology (creating an interaction of these degradation causes).

For all scenarios, participants were asked 10 lead, open-ended questions which related to four key topics:

1. Impact of degraded state on capacity
2. Impact of degraded state on performance
3. Ability to prevention or recover degraded system state
4. Methods for prevention or recovery of degraded system state

Both interview schedules were reviewed and approved by a human factors expert and two ex-controllers.

The interviews were recorded on two Olympus DSS Standard digital recorders.

D. Procedure

The participant was welcomed to the interview room and provided with a standardized brief. The participant was then asked to sign an informed consent form if he/she was happy to continue, and complete a demographic questionnaire. The first interview exercise lasted for 60 minutes, and began with an open question, followed by several probes. Once the interview was complete, the participant received a 30 minute break. The participant was then welcomed back in the interview room. The participant was presented with a total of three air traffic scenarios and asked open questions relating to each scenario for a further 60 minutes. At the end of the interview, the participant was thanked for his/her time and given a standardized debrief which contained the researcher's contact details.

E. Strategy of Analysis

Interviews were transcribed orthographically. The level of detail resulting from orthographic transcription was sufficient for the aims of the research and method of analysis. Only the words that were spoken were captured in the transcription. No paralinguistic features were captured (such as sighing, intonation) [5, 6] Thematic analysis was selected as the analysis strategy [5]. In line with the thematic analysis procedure [5, 6] the transcripts were read through, and elements of participant responses that were related to the aims of the study were identified. The transcripts were then re-read with the aim of categorizing the identified elements into emerging themes. No identifying information was stored in the transcription. Where quotations are used, participants remain anonymous.

III. Results

A total of 12, three-hour interviews were orthographically transcribed and analyzed using thematic analysis. Recurrent and relevant themes are presented below with illustrative quotes from participants. The presentation of results is organized by the order of research aims and address the primary elements of [3]'s framework of graceful degradation. Results are presented under five main headings:

A. Main Themes of Degradation Cause

Participants were asked to recall factors that in their experience, had the potential negatively effect the safety or efficiency of the ATC service provision. All controllers (12/12) communicated causes of degradation. Causes of degradation were understood broadly as conditions or events that had the potential to negatively affect the wider ATC system in terms of safety or efficiency. All causes that were listed could be grouped into one of three broad categories: technological issues, environmental conditions and off-nominal events, and causes related to human operators (specifically, ATCOs), confirming the categorization presented in [3]'s framework of graceful degradation.

1. Degradation Cause and System Effect

A description of a degradation cause alone (such as an aircraft emergency, weather) was often not sufficient to identify the potential risk and effect on the ATC system. A distinction was frequently made between degradation cause and the resulting system effect. The relationship between the degradation cause and system effect is often moderated, so that the presence of the same cause can be associated with various types and severities of effect, or even no effect. The following sections explore the relationship between the causes of degradation and the overall effect on the ATC system as described from study findings.

2. Causes of Degradation can Affect the ATC System Directly or Indirectly

It emerged from the data that the occurrence of a degradation cause could negatively impact the ATC system both directly (one-one connection) and indirectly (one-many connection). An example of a direct effect on the ATC system is a catastrophic radar failure. Due to the critical function of this tool, failure has a direct impact on the ATC system, resulting in reduced or stopped traffic, and a lack of visual separation assurance. Depending on the function of the tool, the impact of tool failure will vary: *"There are certain aspects of flight plan processing and things like that that have gone out so you have to sort of wing it. It is a great impact. It will delay everything and slow everything down" (Participant 9).* In contrast, other causes of degradation indirectly affected the ATC system. Indirect effects included changes to performance-influencing factors (such as workload or fatigue), which can subsequently be associated with controller performance decline and potentially increase the likelihood of a performance-related incident. For example, thunderstorms can result in increased task demand and associated workload *"because now you are more constrained but then you need to keep these guys out of that so you will start vectoring" (Participant 10)*. The increased complexity can be associated with increases in workload, stress and fatigue which in turn can influence other factors such as vigilance and situation awareness, ultimately influencing controller performance. Many causes of degradation are associated with both direct and indirect effects on the system, with a technological or environmental off-nominal event often associated with performance-influencing factors as well as a direct system impact.

A characteristic difference between system causes which directly or indirect affect the system is the rapidity of the event, with minimal time to mitigate the effect on the system. For example, a radar failure (direct system effect) will happen quickly and without an operational backup would have an impact on the system. In these instances where an event has already occurred, human operators have limited time to respond to and mitigate the effect of the event. Indirect causes tend to be less immediate, with more opportunities for mitigation. For example, if a controller is aware of an increasing workload, controllers will change control strategy, preventing performance or system decline. However, if not detected or mitigated, system effects can be just as severe as direct causes of degradation. Another key point of differentiation between direct and indirect system effects is visibility. Direct system effects are often more visible than indirect effects and can be overlooked in both system design and risk assessment of new systems. This distinction is therefore important for future systems designers, to ensure that indirect risks to the ATC system are identified and mitigated.

3. The Relationship between Degradation Cause and System Effect can be Moderated

Controller Strategies Moderate the Cause-Effect Relationship

Air traffic controllers ensure the safety and efficiency of all air traffic. When a potential cause of degradation occurs, controllers utilize a variety of strategies to prevent or mitigate negative impacts on the ATC system, moderating the relationship between degradation cause and system effect. Because of this critical role, the association of degradation causes with performance-influencing factors and performance decline is an important concern. If performance declines, the ability to prevent or mitigate the effect of a degradation cause may also decline, potentially resulting in a negative impact to the safety and efficiency of the air traffic service. Section D reviews in detail the specific mechanisms that are utilized by ATCOs to maintain a safe and efficient ATC service.

Causes Characteristics can Influence Severity of System Effect

As participants shared their experiences of causes of degradation, a pattern emerged that the impact and severity of a degradation cause could be modified by specific characteristics:

1. Whether the cause was expected or unexpected
2. Whether the cause gradually built up or was sudden
3. Duration

These characteristics all modified the relationship between cause and system effect through the association with controller state and performance.

Expected or unexpected cause. Controllers differentiated between causes that were expected or unexpected. Expected causes were defined as knowing that something *"is coming in and what is going to come at us ahead" (Participant 6)* as opposed to an event occurring without expectation. When an event is expected, controllers are able to pre-plan a control strategy, and implement it when required, minimizing the potential negative effect of the cause on the system. For example, when weather is expected *"the supervisors or the floor controllers will start planning 24 hours in advance" (Participant 6).* In contrast, an unexpected cause forces an ATCO to react to the dynamically changing situation, "*In some cases all of a sudden a bubble [thunderstorm] comes up. You just deal with what you have right in front of you right then and there" – Participant 6),* Often, controllers will need to modify or re-build 'the picture' (SA), and develop and implement a new control strategy, all within a limited time, *"You did have a plan. Now you don't have a plan. You have to – you're thinking on your feet. Again, you're reacting" (Participant 9).* An unexpected cause therefore results in a lack of preparation time to make and implement a contingency plan, and in addition, requires additional mental resources to rebuild and implement a plan within a limited time. The lack of preparation time could potentially be resolved through system design, by providing information on potential causes to allow for greater preparedness, when possible. However, this would need to be closely balanced with not providing so much information as to overload the controller. In addition, an unexpected cause also results in a more constrained opportunity for mitigation of the effects on the system compared to an expected occurrence. As a result, an unexpected cause may have a greater risk for a negative association with both controller, and wider system, performance.

Gradual or sudden appearance. Causes of degradation could also occur gradually or suddenly. Gradual events typically build slowly, resulting in the controller perceiving the cause before it become significant enough to disrupt the system, "*typically, weather doesn't just appear…you know it's there, you've seen it coming, and you've watched in the adjacent sector, so you're kind of prepared" (Participant 9)*. Conversely, sudden events happen without warning, such as an aircraft emergency or system failure *"A data link failure or an equipment failure is like; boom, and it just fails" (Participant 7)*. A gradual development of a cause enables ATCOs to develop a control strategy before the situation changes, in contrast to sudden occurrences, "*If I see the weather coming, I'm kind of pre-planning the solution in my head, whereas if all of a sudden, I'm hit with the emergency, then I don't have time to pre-plan" (Participant 9).* The gradual buildup of a degradation cause affords time for the controller to 'stay ahead of the traffic' and maintain SA, whereas sudden changes to the environment forces the controller to become reactive, planning and implementing a control strategy whilst working to 'get ahead of the traffic' and re-build SA. One controller explained *"It doesn't give you enough time to plan… what you need to do and what you need to coordinate and what you need to keep everybody safely separated and away from the thunderstorms. You got to scramble a little bit" (Participant 8).* The underlying issues of lack of preparation time and increased demands on mental resources are similar to the mechanisms seen with expected or unexpected causes, with the addition of an high temporal demand.

Association between characteristics of causes. Findings suggested that the characteristics of expectedness and pace of development could interact to modify the likelihood and severity of the effect on the system. Figure 2 uses a quadrant diagram to represent the interaction between these variables, creating four different cause scenarios, with associated effects on the system. An occurrence that was expected and gradually built, such as a thunderstorm that had been correctly predicted, in general was reported to have a relatively minimal impact on controller state and the ATC system due to the ability for network operations (such as the traffic management unit) as well as controllers, to

prepare for the event. Control strategies could be developed, and preemptive plans, such as flow restrictions, put in place in order to continue safely and efficiently managing air traffic. An occurrence that was expected but sudden, such as a thunderstorm that had been incorrectly predicted, would be likely to have a greater impact. Although control plans may have been prepared, controllers would need to respond immediately to the unexpected change in the ATC environment. The availability of a pre-prepared plan may mitigate the impact of the sudden occurrence however, *"We knew it [thunderstorm] was coming but it came sooner than we were planning. There will already be a contingency plan" (Participant 6)*. An occurrence that is unexpected and gradual, such as an unpredicted traffic build up, would require a controller to build an accurate picture of the situation, and a control strategy, for the changing situation. However, as noted previously, the buildup of an occurrence still provides valuable seconds for a controller to develop and implement a plan whilst still maintaining situation awareness. The reported causes that placed the most immediate demand on ATCOs were causes that were both unexpected and sudden, such as an equipment failure or aircraft emergency. The ATCO must react to the situation, whilst trying to rebuild situation awareness (SA) and maintain safety and efficiency of air traffic. A cause occurrence with these qualities may therefore be more likely to negatively influence ATCO performance and potentially, performance-related incidents.

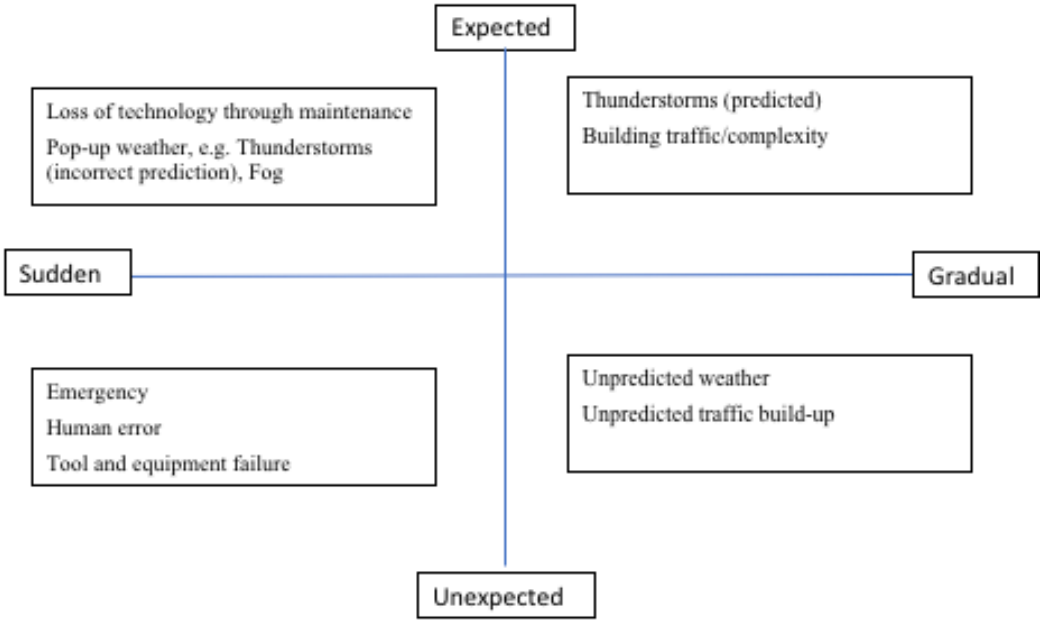

Figure 2 Quadrant representation of causes of degradation

Duration. The duration of a cause occurrence also modifies the resulting impact on the system, both by directly impacting the air traffic service provision, and indirectly, by influencing controller state. When the occurrence is short in duration, there is an opportunity to recover the provision of air traffic services without an observable effect on safety or efficiency. This is less likely in occurrences of longer duration. In addition, occurrences longer in duration can differentially influence a controllers' state. Longer durations of high workload can result in depleted cognitive resources, associated with performance decline, which may be less likely in events of shorter duration, ***"****I am glad it didn't go that long. Because that would have been a lot of work. When things break. Or the weather gets bad" (Participant 10)*.

4. A Note on Interaction Relationships

Interactions between and within degradation causes were reported to be frequent, as were interactions of primary causes with moderating variables, such as the level of traffic and complexity at the time of the occurrence of the cause, and airspace features. Specific interactions between elements of the ATC system are discussed in detail in section C. However, it is relevant to mention here that interactions between causes and mitigations of degradation also result in a modification to the relationship between primary cause and resultant effect on ATCO state and the wider ATC system.

5. Implications

In summary, the relationship between a degradation cause and the effect on the ATC system is complex and moderated by many variables. These results demonstrate the importance of viewing the causes of degradation in the context of the wider system and environment, as identifying only causes does not fully inform the system effect. These findings have important implications for ATC system designers. Designers must create systems that can tolerate causes of degradation and the associated effects on both the controller and the wider ATC system, including the flexibility to allow controllers to respond dynamically in order to mitigate effects on the ATC system.

B. Frequently Reported Causes of Degradation

The following sections describe the causes of potential degradation that were most frequently reported by participants. Although previous studies have documented potential causes of degradation, there is a lack of comprehensive knowledge of the potential degradation causes or risk factors in the ATC system as a whole [3]. ATCOs are particularly well-placed to provide information to address this gap due to their experiences of potential causes of degradation and the active mitigation of these causes. By understanding the potential risk factors that could lead to degradation it is possible to identify and mitigate risks to future ATC systems.

1. Equipment and Tools: Causes of Degradation

Benefits of Technology

All controllers volunteered information on the benefits of equipment and tools for the provision of a safe and efficient air traffic service. Automated tools were frequently reported to reduce workload and support ATCO performance. As one participant stated, *"Anything the automation does that allows you to keep your eyes and ears in focus on the traffic is good" (Participant 3).* Another controller highlighted how essential equipment at tools are to the air traffic control service through describing failures in tools: *"Whenever anything fails...it's going to make things more difficult" (Participant 9).*

Reported Examples of Prevalent Technology-Related Issues That Can Causes System Degradation

Table 1 lists frequently reported causes of degradation in the ATC system. This list does not contain all causes of degradation, but those that controllers raised most frequently. Causes could be subcategorized into different proposed groupings. The proposed categories are not definitive but are intended to represent differences between different technology-related causes of degradation.

Table 1 Examples of technological causes of degradation

Total equipment and tool failure	Radar primary, secondary
	Radio Transmitter/receiver
	Internal communication/phonelines
	Issues with aircraft VHF radio
	Weather prediction tool failure
Degraded technology	Flight plan data partial or complete failure
	Callsign failure (just leaving radar target)
Limitations of automated tools	Conflict probe and alert
	Auto hand-off
	Sequencing tools
	Inadequate design for human use
Technology resulting in a loss of flexibility	"In those situations where you need to have that flexibility and adjustment, sometimes it isn't there" (Participant 6).
Indirect concerns resulting from automation	Skill degradation
	Complacency
	Future traffic increases

Failure of equipment or tools included examples of critical equipment such as radar and communications failures. Equipment failures are highly visible and well documented in the literature. Another category of technological cause of degradation was limitations to automation; the tool worked as designed, but the tool may not function optimally in specific environments. For example, the conflict probe and alert tool is an automated safety tool that indicates when two or more aircraft are on a trajectory to lose separation minima. Controllers acknowledged the tool can support safety, "*there are times when you forget something. You know it is there. But you just forgot about it. You have this Conflict Alert" (Participant 6)*. However, several controllers criticized the tool for not being useful in an environment with a lot of climbing and descending traffic, such as TRACON. Due to the parameters for when the alert should occur, the tool *"is just constantly going off it is not much help and you tend to tune it out" (Participant 10)*. This can lead to distraction, as well as the controller ignoring a real alert. This finding highlights the importance of tool reliability, "*If it doesn't work we just say forget it. It's unreliable…Until someone proves to me that it's going to work I'm not going to base my career on accidentally running an airplane into another guy's sector" (Participant 7).*

A general concern was raised by several controllers that more automated tools do not allow for the flexibility needed to respond dynamically to changes in the air traffic environment, exacerbating workload and potentially limiting the strategies available to mitigate effects of a degradation cause, "*Software engineers they're designing the routes and they'll say, well, he's doing 160 knots and that's this many miles per minute and descending at this rate, so if he gets here then this guy should only be here. [But] there's weather, there's emergencies, there's pilot errors" (Participant 7)*. Finally, controllers raised concerns that automated tools could indirectly affect the system through issues of skill degradation and complacency, highlighting the importance of training to maintain skill and contingency plans. Several controllers also raised concerns regarding the influence of technology of future traffic levels. With increased automation and predictability, increased traffic levels are possible due to workload reduction. However, a concern was raised relating to whether controllers would be able to manually control the higher traffic levels if the automation failed, *"Everything is working fine and dandy and then it doesn't work. Can you keep up with the inter-phone, radio calls, and I still have to talk to the people around me" (Participant 7)*. The severity of the impact of technological causes on the ATC system appeared to be influenced by the function of the technology, *"Any tool, if you've got a tool that you're working with and you're relying on it to do something for you, if it fails it make things harder" (Participant 2)*.

2. Environmental Causes of Degradation

Participants reported that unexpected occurrences happen frequently in the control environment, and usually with specific nuances. For example, an aircraft emergency could take multiple different forms. However, in broad terms, the most common environmental events that were reported to have the potential to result in system degradation were:

- Weather
    - Thunderstorms
    - Turbulence
    - Fog (Tower only)
- Aircraft emergency
- Pilot requests

Causes could directly impact the air traffic control service, for example, an aircraft emergency on a runway that delays arrival traffic, or indirectly, through associations with performance-influencing factors. For example, during a thunderstorm, controllers often allow pilots to deviate around the weather at their discretion, and from this, attempt to create a new route for aircraft to follow. This reduced-control situation results in increased monitoring and workload; *"They say we want to deviate left. When they say deviate left, now I'm really having to focus on that... How far is he going to go before he gets back on this normal route" (Participant 5)*. Although these causes were the most frequently discussed, participants emphasized that the occurrence of one of these events does not necessarily result in a negative impact on the safety or efficiency of the ATC system. The causes themselves had different characteristics and could differ in severity. For example, a thunderstorm which is large and covers multiple altitudes has a greater impact on controller workload and efficiency of traffic than smaller, more localized thunderstorms "*If there's severe turbulence and you only have one smooth altitude, everybody's going to want to be at that smooth altitude" (Participant 2).* In addition, several 'background' environmental variables were identified that moderated the complexity of the traffic situation. Many of the reported variables related to increased complexity or airspace constraints. Table 2 lists some of these factors as noted by controllers.

Table 2 Environment factors that moderate traffic complexity

Sector features	Shape and size of airspace
	Crossing routes/conflict points
	Mix of traffic (IFR and VFR)
	Climbing/descending traffic
	Traffic presentation i.e. Integration of arrival streams
Location of sector	Military airspace
	Mountains – takes away airspace/ flexibility
	Mountains – thunderstorms build quickly without notice
Traffic	Traffic amount and complexity

Sector size and location generate additional constraints on the traffic, and the control strategies that can be used. When a sector is narrow, *"you've got to make your turns exactly right, your climbs, your speed, so you've got to be on everything" (Participant 4)*, resulting in a lower tolerance for error. If an error or non-optimal event did happen in constrained airspace, much as a pilot turning wrong way, there is less time to resolve the situation before the aircraft is out of the controllers' airspace. One of the most frequently reported, and most critical, modifying factors was the amount and complexity of traffic at the time of the primary cause occurrence. Higher levels of traffic results in less available airspace in a sector, limiting the available options and flexibility for resending to unexpected events, as well as a smaller margin for error. In addition, greater traffic levels and traffic complexity is associated with increased controller workload, reducing the time available to rebuild SA and implementing new plans in response to the occurrence of an unexpected cause of degradation. With lower traffic and complexity, controllers have more time to develop new control strategies, and implement strategies, to mitigate effects of the primary cause. An example of this is the differentiation of an 'easy' thunderstorm by a controller who has minimal traffic *"The pilot says, 'Can we deviate to the right around it?' I don't have any traffic out there, and no big deal. That's an easy thunderstorm" (Participant 3)*.

Although these variables were not causes of degradation per se, they could interact with the primary environmental cause to modify the effect of the cause on the system. Participants emphasized therefore, that in order to accurately understand the likelihood and severity of the effect of a cause such as an aircraft emergency, the event needed to be considered in context. For example, if a thunderstorm occurred in a sector that was next to an area of unusable airspace, available mitigation strategies, such as deviating into neighboring airspace to route around a thunderstorm, are reduced. These factors can therefore increase the complexity for controllers to mitigate effects on the system. The interaction between environmental causes of degradation, sector characteristics and traffic variables can create a compound effect on the ATC system, above what would be seen by the cause alone. Without understanding the characteristics of the specific event, or the interacting background factors associated with it, an operationally valid understanding of the risks of degradation, when degradation is most likely, and how to prevent degradation cannot be achieved. In addition, without an awareness of these interactions, system designers will not have an operationally valid understanding of system tolerances, and the requirements of the system to be able to gracefully degrade. It is therefore critical to further identify such interactions, and the combined effect on the controller and wider system, for both the prediction of risk in safety critical systems, as well as system design to prevent reaching system tolerances, and the ability to achieve graceful degradation.

Wider, organizational factors can also moderate the relationship between cause and effect. Staffing issues can increase fatigue due to more hours actively controlling traffic, and individual differences, such as amount of experience, can also exacerbate, or protect against, effects on performance.

3. Human Operator-Related Causes of Degradation

The Role of the Controller in the ATC System

Air traffic control is supported by many human operator roles. It was beyond the scope of this study to review each role and the potential contribution to system degradation. Due to the safety critical role of controllers, controllers are the primary focus of the reported findings. ATCOs are at the sharp end of air traffic control. Controllers respond to the dynamic air traffic environment to ensure the safety and efficiency of air traffic. To ensure flight safety, ATCOs must maintain a consistently high standard of performance. Human factors have been repeatedly evidenced to affect human performance [7] and are *"major determiners of human error"* [7, p330].

Human Factors can Affect Performance Directly or Indirectly

Performance-influencing factors, such as workload and fatigue can directly and indirectly affect performance. An example of a direct influence on performance is the maintenance of vigilance. If a controller overlooks an aircraft, this has the potential to have an immediate impact on system safety. "*You are focused on the opposite side of the scope not where this areoplane is. The next thing you know it will surprise you. Wow, I forgot about this guy" (Participant 6).* Factors such as workload, fatigue and stress are more indirectly related to performance through associations with cognitive abilities and other human factors that are critical for controlling, such as inadequate SA. One controller gave the example of an association between workload and vigilance: *"Somebody misses his turn and you are busy someplace else and meanwhile he has gone way past where he is supposed to go" (Participant 8).* Examples of the human factors and associated examples that were raised by controllers are presented in Tables 3 and 4.

Table 3 Examples of influences on controllers from pilots

Proposed category	Examples
Error	Turning wrong way
	Level bust
	Not meeting climb rate
Communications	Missed calls
	Slow to respond
	Asking for repeat

Table 4 Examples of human factor related causes of degradation

Human Factor	**Examples**
Workload	Overload and underload
Inadequate Situation awareness	Incorrect mental picture
	Falling behind
Communications	Transposing callsigns
	Incorrect readback/hearback
	Missing calls
Fatigue	Slower at developing plan
	Slower to respond
	Don't perceive issues are quickly or clearly
Stress	Poor planning
	Inattention
Vigilance	Overlooking things
	Missing hand-offs
Inadequate Teamwork	Passive D-side – needs to be told what to do
	Uncooperative

Reported Performance-Influencing Factors and the Association with Controller Performance

Although not a comprehensive list, controllers also shared how different factors could influence performance, The following summarizes the factors and associated performance influences.

Workload. Extremes of workload such as underload (defined as a low level of objective and perceived task demands, easily met by individual resources) high workload (defined as a high level perceived or actual task demands, with a high level of operator effort) and overload (defined within ATC as a high complexity and/or volume of traffic where individual resources are insufficient to meet objective task demands, potentially impacting safety) were associated with negative implications for controller performance and system safety. Controllers frequently associated low and high workload with influences on performance, and potential human error. For example, low workload and was associated with affects on vigilance *"There's a lot of times when you're probably too relaxed so you get back in there and then all of the sudden you're going, god I better wake up here, a little lackadaisical" (Participant 2).* Perceptions of high workload were associated with traffic complexity and not simply the amount of traffic "*You can have 30 airplanes in your sector and it's a nice day, it's not a problem. Other days I could have five airplanes and you*

could have weather and military and that complexity has gone up with five airplanes more than when you had 30" (Participant 2).

Fatigue. Sources of fatigue were linked to controlling tasks as well as external sources such as illness or not getting enough sleep. Fatigue was associated with several negative performance affects. Controllers reported feeling cognitively 'slower' as a result of fatigue, developing poorer plans, and spotting the development of issues later "*When you do start to feel that mental fatigue, and you're falling behind, stop, get your priorities straight, and get back, and get working" (Participant 4).*

Stress. Participants emphasized the distinction between work-related stress and personal stress. Controllers frequently reported that job-related stress was generally task-related, associated with high workload or complex traffic situations. Many participants felt that stress on the job could be exacerbated by external sources of stress *"I really didn't feel like there was stress, but if something else was really going on in my life, I could feel stress at work" (Participant 3).* Stress was experienced as having a negative influence on performance *"when you are stressed, your mind is racing more, your adrenaline is flowing more so you are not able to think as clearly and I think you miss more things, overlook things, which makes things even worse, which raises your stress even more" (Participant 7).*

Inadequate vigilance and SA. Vigilance decline and inadequate SA were perceived to be the result of other human factors influences, such as high workload or fatigue, *"If you are that focused on the opposite side of the scope the next thing you know it will surprise you. Wow, I forgot about this guy" (Participant 6*) as was inadequate SA, or 'losing the picture'. Vigilance and SA are related – without sufficient vigilance, controllers will have an incomplete picture of the traffic situation. Both vigilance and adequate SA has been repeatedly shown to be essential for the work of ATCOs. Inadequate vigilance or loss of SA can result in declines in performance and safety-related events.

*Teamwork***.** Teamwork was confirmed to influence performance both positively and negatively, depending on the characteristics of the teamwork. *"A good D-side kind of looks and sees what's going on, experienced controller working that, and they take care of you" (Participant 2)* and served to mitigate the influence of human factors. However, inadequate teamwork, characterized by being reactive, waiting for instruction or not being vigilant, could exacerbate a high workload situation "*if someone is not helping you or pointing things out or doesn't care what is going on in your sector, then that makes things harder on you" (Participant 7).* Interestingly, controllers felt that teamwork primarily influenced performance when working busy traffic: *"Low traffic teamwork really doesn't come into play. It is when the stress levels move up and the work is harder and there is more going on that is when the teamwork really comes into play. It is not just teamwork between a coordinator and a radar guy. It is other sectors that are planning" (Participant 8).*

Implications

Although this section was not a comprehensive review of all human factors that can influence degradation, findings revealed that controllers have experienced negative associations between specific human factors and performance. Performance-influencing factors may contribute to system degradation through controller performance decline, and may also prevent the application of sufficient mitigation strategies. Therefore, the prevention and mitigation of the influence of human factors associated with performance is critical to system safety.

C. System Degradation: The Contribution of Interactions

It became evident from participant responses that degradation causes do not occur in isolation. Interactions occur between multiple system elements occur to contribute to overall system degradation. Having previously discussed the contribution of single factors (associated with technology, the environment and human operators) to degradation in an ATC system, the following sections explore the contribution of interactions between important system elements to degradation. One of the principal differentiations between interaction relationships was between co-occurrence and association. Co-occurrence of causes of degradation is defined as when two independent causes of degradation occur at the same time, such as an aircraft medical emergency occurring at the same time as a thunderstorm. Conversely, interaction between degradation causes can result through association, in which one degradation cause is related to a secondary cause. Both co-occurrence and association relationships occur within and between categories of degradation cause (technology, environment, human operator), as well as between wider elements of the degradation framework, including causes, prevention strategies and recovery mechanism, creating a wider systemic effect.

1. Co-occurrence of Degradation Causes

Causes of degradation can co-occur, often resulting in a compound effect on ATCO performance and the ATC system. Participants provided examples of the co-occurrence of multiple causes, both within and between degradation cause categories.

Between Categories

Interactions can occur between technological events and environment events. Examples include the failure of critical equipment such as radar or radios whilst there is a thunderstorm. One controller relayed an experience of weather issues as well as radar outage *"We had about 17 or 18 operations. It was IFR weather this one particular night. Maintenance called, they took the radar. I had nothing but the raw primary radar and the beacon targets. I was attempting to keep these guys separated by three more miles while they were doing their approaches. I just barely had the picture - If I had looked away at all, I would have lost that" (Participant 3)*. The combination of these two issues resulted in a task demand for the controller, larger than what would have been experienced if only one of the causes had occurred. In turn, this resulted in the potential loss of SA and reaching performance limits. A second example is between technological or environmental events and the human factors that can influence a controllers' state. Interactions between the controllers' state and causal events, either technological or environmental, can interact. One controller noted "*If you're tired and fatigued, it's always going to add to a bad day. You would just be slower to react to things" (Participant 5)*. These co-occurrences can create a compound effect on the controller that will be more likely to affect performance negatively, as well as influence the ability to effectively mitigate the effects of the event.

Within Categories

Elements can co-occur within categories of degradation cause, such as technological causes or environmental causes, for example, a medical emergency occurring at the same time as a thunderstorm. In this example, the response to the emergency may be made more complex by the limited usable airspace resulting from the thunderstorm. Section 7 reviewed the interaction between primary environmental causes and background factors such as traffic level and airspace design, which is also an example of within-category interactions of co-occurring factors. The relationships between human factors are highly complex, and many are related. However, some factors can co-occur independently. For example, a controller may be fatigued due to lack of sleep, and then work with someone who is has poor teamwork skills. One controller provided the example of personal stress with workload *"While you're working you have to sit there and work but you also have to think of the things that are going on. Like if you've got a crisis at home with the kids or something like that. It weighs on your mind" (Participant 3)*. Co-occurrences may interact to increase the likelihood or severity of impact on the system.

2. Relationships between Causes of Degradation

Between Categories

Functional Failure. An important finding was identified when controllers spoke about technology use in association with environmental off-nominal events. Controllers spoke frequently about automated tools, and the intended function of the automation, such as reducing workload or supporting efficient traffic flows. However, in specific environmental circumstances, although the tool was technically operational, the intended function of the tool was compromised, lending itself to the terminology of 'functional failure'. This is a well-known concept to controllers, with one participant saying quite flippantly *"tools that they need don't work or can't use them because of weather or whatever" (Participant 4)*.

An example of functional failure is the use of datalink communications during a thunderstorm. Controllers reported that during a thunderstorm, datalink communications would not be adequate to control effectively *"Direct communications are extremely important. Using automation in a normal flow of traffic is fine. But increasing capacity or in emergency situations or heavy traffic situations, it becomes a detriment more than an assistance and help" (Participant 6)*. Controllers also provided their own examples of this effect, such as with the safety tool of auto-handoff *"In a terminal environment, it's very unreliable. It doesn't work very well. Rarely do we use [it] (Participant 7)*.

Depending on the tool's function, this interaction can have a negative impact on the ATC system. For example, if a tool's function was to reduce workload, and the function is lost due to an interaction with the environment, controllers now not only need to respond to the additional complexity and associated workload from the event, but also experience additional demand from the loss of the tool's function. Using the datalink example again, one controller predicted *"You would be verbalizing instead of putting in a trial route and sending it by data link. I think if I was at peak numbers and then had to do that, that would push me over the edge. Things wouldn't get done" (Participant 2)*. In addition, because the tool has not technically failed, there would be no obvious indicators that the actual function of the tool is compromised, resulting in the controller experiencing a potentially higher workload without support.

The effects of this type of interaction also have implications for future ATC systems. The function of automation or new traffic systems is often to reduce controller workload in order to enable increased of traffic. If the function of the tool fails with a greater traffic load than can be handled without the tool, the controller could become overloaded and may not be able to mitigate the system effects, resulting in rapid system degradation. This therefore creates the

possibility of a brittle system. The issue is further exacerbated by a lack of specification of risks that are generated by interactions through traditional design specification or risk assessments. This notion can only occur, and therefore be identified, through exploration of interactions between critical elements within the larger ATC system. However, current day system designs and risk assessments do not take into account interactions between system elements. Together, these points raise a serious risk for the design and assessment of future ATC systems. It is critical that technologies be designed to be functional under environments when controllers are dealing with the most workload. If this cannot be achieved, it must be clearly identified under what circumstances the tool will not be functional, so that targeted contingency plans can be developed by the operation.

Many other examples of the relationships between categories of degradation were provided. Technological and environmental off-nominal events, including failure, emergencies, thunderstorms, are associated with increased controller workload *"Sometimes you can be having a ton of airplanes and you throw an unusual event in there that blows it off the chart. And then you've got to scramble as well as keep everything else under control" (Participant 2)*. The two causes occurring simultaneously can interact to create a greater workload that if they occurred individually. Future systems must allow for these types of interactions so that controllers have the ability and flexibility to prevent impact on the system.

Within Categories

Associations can occur between categories. Technology failure can be associated with other failures, although because of various redundancies, this was less common and reported infrequently by participants. The relationships between human factors were most frequently discussed. Relationships are often bi-directional, and factors can interact to produce a greater negative impact on performance. Table 5 presents the human factor associations that were most frequently discussed, with associated quotations from participants.

Table 5 Examples of associations between human factors

Workload and Stress	Well, whenever your workload goes up your stress goes up. It kind of goes hand in hand (Participant 7)
Teamwork and Trust	"Working with somebody that you know just so smooth. So easy going. You trust that guy. He trusts you. He trusts you to make the right decisions and he knows what to do as far as coordination" (Participant 8)
Teamwork and Workload	"Low traffic teamwork really doesn't come into play. It is when the stress levels move up and the work is harder and there is more going on that is when the teamwork really comes into – into play" (Participant 8)
Fatigue and Workload	I wouldn't want to go back into the pressure cooker you know what I am saying with a 15-minute break. I wouldn't want to (Participant 10)
Stress and Vigilance	I think you wind up overlooking things, not noticing little variable that can turn into something worse later on because your mind is just—I guess when you are stressed (Participant 9)
Workload and Vigilance	somebody misses his turn and you are busy someplace else and meanwhile he has gone way past where he is supposed to go so now you are getting him back and trying to get him back quickly, so a couple of those and then it can just all start to snowball (Participant 10)
Fatigue and SA	Sitting there at a busy radar sector… my fourth shift of the week, I've already had the quick turn to the day, and then I came in, and I probably got out of bed at 3:30 that morning to come to work, and I'm on my fifth cup of coffee for the day, and I remember just feeling like I'm barely hanging on by my fingernails for dear life (Participant 9)
Teamwork and Trust	You have got to figure that at this point, the people higher up the food chain are doing whatever they need to do to number one get the problem fixed (Participant 10)

Although these examples are not exhaustive of all associations that can occur, it does suggest the complexity of the relationships between human factors, as well as the possible interactions and associated impact on controller performance. By understanding these interactive mechanisms, mitigative strategies can be implemented prior to performance decline and performance related incidents.

3. Co-occurrence and Association of Causes of Degradation

Although for clarity the above information has been presented by co-occurrence and association between factors, in reality, situations can include aspects of co-occurrence and association to create highly complex interactions. The following participant quotation illustrates the interconnectedness of elements within the ATC system *"It's a buildup of, culmination of different things. I might be at 50% because everything is taken care of, normal. Weather. Oh okay. The weather becomes a distraction. I'm using the keyboard because everything is working. The only thing that's different is the weather. All of a sudden data link goes down. Oh. Stress level just went right up because data link went down. And I'm continually scanning the scope to find out if everybody's separated" (Participant 6)*.

4. Impact of Interactions

The occurrence of multiple causes of degradation, as a result of co-occurrence or association, created a greater risk to controller performance decline than the occurrence of single factors alone. As one controller explained *"We're very good jugglers. Something goes wrong. That's not that big a deal. You can handle it, and no problem. Then something else happened. Here comes another ball. Pretty soon, you're going to drop a ball (Participant 10)*. Responding to, and mitigating the impact of, a single cause was seen as 'part of the job'. It was the occurrence of multiple factors that created great risk of performance decline and a negative impact on the system. In addition, controllers saw this interaction effect as a compound, as opposed to linear, effect, *"I don't think it is linear. It just starts to be exponential as things happen, it never seems to be linear, it just goes like that, it just goes, first a lot faster" (Participant 8)*.

As a result of interactions, and the associated compound effects, factors that would not ordinarily crate an effect on the system alone, can combine to negatively affect controller performance and the ATC system. It is therefore more frequent for multiple, smaller things to combine and negatively affect the system than more catastrophic events such as a complete radar failure "in *the extreme, things like you lose radio or you lose radar that's going to affect things. But it's not usually that, it's those smaller things that build up" (Participant 9)*. This is a critical finding, as interaction between factors, and the associated effects, are not well understood or specified in the current ATC system, nor in the design of future systems. It is essential that future system design, and risk assessment consider these interactions and the possible compound effects in order to design a system that is optionally valid and can tolerate the dynamic nature of the ATC environment. It is these relationships that needs to be understood in order to design enough flexibility into the system, so that performance or system tolerances are not reached.

It should be noted that the interaction between factors is not always negative. Various combinations result in 'protective' relationships which mitigate potential impacts on the system. For example, a controller experiencing a high workload may be more prone to errors or declines in SA. However, a well-rested state may prevent these effects to some extent, and the application of teamwork to offload workload to a colleague will prevent a negative effect on the controller and the system.

There are an almost infinite number of these types of combinations, but the exact interactions are not critical to specify. Instead, it is the concept of interactions between causes of degradation, leading to compound effects on both controller performance and the wider ATC that is important to specify. System risk or tolerances cannot be fully understood without the consideration of interactions between causes and prevention mechanisms, and as a result, cannot be mitigated or prevented. In addition, without considering the interactions between causes and the associated impact on the system, operationally valid guidance on the tolerance of the ATC system will not be available for designers of future ATC systems, limiting the ability to design systems that will not go beyond the system tolerance limits, and that are capable of graceful degradation.

5. The Importance of Understanding System Interactions

Identification and understanding of interactions between system elements, and the associated effect on controller and system performance, is critical for the design of a system that can gracefully degrade. Without this awareness, the system effect can neither be designed out, or prevented in future designs. In current day systems, controllers work to seamlessly ensure the safety and efficiency of air traffic in a dynamic environment. However, future systems are predicted to be more precise, less flexible, and use more automation to control higher levels of traffic, and by not designing the system to be tolerant to negative influences, the system may become brittle. As one controller stated, "*ATC and aviation is a continuing evolutionary process. The variables always change, and we try to beat them. We try to control them, like the old West, like riding a bull. But we're trying to make it so this would happen all this time this way, and we're going to beat the variables, and it's just—it's just the equipment's not up to it, the system is still not designed for it" (Participant 7)*. By understanding interactions between degradation causes, and the total effect on the system, risks can be identified and deigned out, and controllers can be given the correct amount of time and flexibility to mitigate issues. Future system design must take into account the overall tolerance envelope of the ATC

system, determined through specification of the causes of degradation and the resulting system effect of factor interactions. Without acknowledging these elements, future systems may not have the ability to gracefully degrade.

D. Strategies to Prevent and Mitigate System Degradation

The air traffic control system is well-defended from potential causes of degradation. Once a potential cause of degradation has been identified in the system, various mechanisms are available to mitigate the effects of the cause. However, when these mitigations are limited or inhibited, degradation can occur. Based on findings from the interview studies, the following mitigative strategies can be utilized at various stages to prevent or mitigate system degradation:

1. Pre-degradation prevention strategies
2. In-time prevention strategies
3. Strategies to recover the system once the system has degraded.

Pre-degradation strategies are implemented prior to the occurrence of degradation, with a goal to prevent the occurrence of a potential cause or mitigate the effect so that the system will not be negatively affected. Examples include backup systems for technology, that are activated as soon as critical technologies fail, procedures, and training for air traffic controllers. The other categories of mitigative strategies are highly dependent on controllers. In time prevention strategies are applied by controllers in an attempt to mitigate the degradation cause and minimize impact on the system. If degradation to the system is unavoidable, controllers will also engage strategies to limit the degradation and recover the system. Therefore, the majority of strategies that mitigate negative effects on the system are highly controller-oriented. These results represent an extension to [3]'s framework of graceful degradation, and in addition, address a gap in previous research regarding the specific mechanisms by which controllers protect and maintain the safety and efficiency of air traffic. The followings sections examine the three identified categories of mitigative strategies in more detail, based on responses from controllers.

1. Pre-degradation Prevention Strategies

Pre-degradation strategies were mentioned throughout the interview, although the main focus of participants' responses related instead to in-time strategies. Controllers reported several mechanisms that could prevent degradation and mitigate the impact of degradation. These strategies could be broadly categorized into mechanisms to prevent effects of technology decline, mechanisms to reduce environment complexity or the likelihood of environmental causes of degradation, and mechanisms to prevent performance decline in humans. For an extensive review of previous research on pre-degradation strategies, please refer to [3].

Technology

Backup systems for hardware were frequently mentioned as a contingency for failure of critical technological systems, "*You don't want to see a catastrophic failure. That there are safeguards that are built in that you have to rely on and you just pray that they come back up right away. It's not fun." (Participant 6)*. However, it was also noted that in some cases, the backups also fail or take time to activate. In these cases, controllers needed to rely on paper strips and procedural control, with reduced traffic. In addition, procedural contingency plans for technology failure, such as using radar only is ads-B failed, were referred to, but often these were reported to not reflect he exact situation that was experienced, resulting in interpretation of the implementation by human operators (including supervisors and controllers).

It should be highlighted that since the findings are focused on the controllers' experience of mitigation strategies, technology backups were not reported prominently in the findings; however, technology backups are a critical feature of a resilient ATC system nevertheless.

Environment

In terms of mitigating potential environmental causes of degradation, responses were focused mostly on discussing airspace features, such as shape of airspace and crossing routes, *"I think most airspaces are built so that you have a little bit of flexibility as far as being able to use somebody else's airspace. There's some built-in buffer space between airspaces" (Participant 8)*. Mechanisms were focused on not so much a redesign of airspace, but mechanisms to enable the controllers to work around the constraints and restrictions. Shorter-term mitigative strategies for weather were also reported, using weather reports to plan for poor weather in advance *"It makes our job a lot easier. In the sense that when weather comes, the plans are already in place as to what happens" (Participant 6)*. In future designs, designers should ensure to include some buffers into the airspace and traffic, rather than maximizing utilization in nominal operations, which results in a reduction of flexibility to respond to environmental occurrences.

Human Operators

Training was raised as a means to support controller performance in challenging situations. In addition to the rigorous training program to be a controller, there were also various training programs on degraded operations, such as a technology failure or weather *"We try and do refresher training before the rainy season starts and think about it a little bit but until you actually start doing it and get that timing again" (Participant 8)*. Training was viewed to have a positive impact and helped prepare controllers for challenging situations, mitigating potential human factor influences and decreasing response time through familiarity. Although facility-specific, another strategy for mitigating potential influence ion controller performance was to brief the controllers daily *"One facility worked out, when they had the morning briefing, they brought it back to you, and they told you, 'Here's what's going to happen today, guys'" (Participant 7)*. This information allowed controllers to prepare for events, and reduce the potential effect of expected events on the air traffic system. Controllers would control differently even before the event, such as creating standard flows or controlling more conservatively, in order to keep workload low when the event occurred.

2. In-time Prevention Strategies

Controllers are active agents in the management and maintenance of the air traffic service system. Once identification of a non-optimal event or performance-influencing factor is detected, controllers apply a supportive strategy to mitigate the potential negative influence of the issue on the system, to support the maintenance of performance, and system safety and efficiency. These 'In-time' strategies are applied dynamically, according to the needs of the current control environment.

Commonalities Between Strategies: Time and Space

In-time strategies differed by type, and the element of the system that was addressed. The compensation strategies that controllers apply are specific to the situation. For example, strategies to keep traffic separated in a thunderstorm were different to techniques used to respond to a communications failure. However, strategies appeared to have common goals of achieving more airspace to work with, and more time, *"Just to give yourself more time, more space. You just do whatever techniques you got to fix it" (Participant 10)*. The more available airspace a controller has to work with, more 'outs' and backup options are available. Therefore, by engaging strategies that create space, controllers have more flexibility and available options to mitigate the situation. In addition, time allows controllers to build and implement new strategies based on the changing environment. The commonalities of the goals for many control strategies provides information about what controllers need in order to mitigate negative influences on the system, specifically, time and flexible use of airspace. This has particular implications for future systems which advocate increased precision and reduced flexibility, highlighting that further research is needed on the balance between increased precision and efficiency, and flexibility for controller to respond in-time to the dynamic environment.

Strategies Are Learned Through Experience

Compensation strategies are not formally taught, *"a lot of it becomes stuff you learned through your experience. Let's say you try to train to developmentals. And they hear you, but they haven't done it yet so they don't really until they have to do it later" (Participant 2)*. Therefore, strategies are primarily based on experience, *"with time you know that hey, just because I'm focusing on him doesn't mean I better stop looking at this too" (Participant 7)*. Because strategies are learned through experience, trainees and newly checked out controllers may be more limited in the strategies that they have available, creating vulnerability to performance influencing factors or negative system influences. Therefore, training on mitigation strategies may serve as a protective factor for controllers with minimal experience. Automation support could also contribute to training, providing increased advisories to trainees to highlight a building situation, or when a specific change in control strategy would be beneficial.

Controllers Use Internal and External Indicators to Decide when to Change Control Strategies

Controllers use indicators as information regarding when compensation strategies are needed. Indicators are learned through experience and can be external and observable or internal. For example, a controller who is feeling fatigued will control differently, such as increasing safety buffers, to minimize the potential effect of fatigue on performance. It is beyond the scope of this paper to review the indicators that controllers use. This finding has significant implications for future technologies which can 'monitor' controllers through psychophysiological measures. As indicators of performance-influencing factors and performance decline are increasingly specified, these indicators can be monitored. Changes in indicators such as heart rate, blink rate (fatigue, workload), percentage of time scanning outside areas of the sector versus inside the sector (contributing to information about situation awareness

and 'tunneling') could be used provide information to ensure controller awareness, so that the controller may then mitigate these potential influences prior to performance or system decline.

Use of Compensation Strategies are Dependent on Awareness

When an influencing factor is present, performance may be protected by several 'barriers' (created from awareness and compensation strategies) before becoming vulnerable to factor influences. If an influencing factor occurs (e.g. fatigue) internal indicators such as feelings of discomfort may alert the radar controller and trigger the application of a compensation strategy. Performance may then be maintained. If an internal marker did not occur or was not detected, another opportunity to detect the issue may occur through observable indicators. However, if the controller is not aware of these indicators, protection of performance is dependent on a colleague's (i.e. the D side) awareness. If neither controller notices an issue, participants suggested that performance is more likely to decline than if a compensation strategy was applied.

Mitigation Strategies Associated with Technological Causes

Controllers primarily mitigated the effects of technological causes of degradation by attempting to replace the function of the failed technology. For example, if a communication system failed, controllers would find a neighboring sector or control center that could take over communications and operations. Due to the unexpected nature of technological failures, controllers were primarily reactive. If critical equipment failed, such as radar or communications, controllers prioritized safety *"If tech fails there are two tasks that are imperative at that time. First, it's just to make sure that everyone is separated, and then I think that the second imperative is to try and get everyone out of the sectors as quickly as possible" (Participant 11)*. If operating under degraded operations, such as with a secondary radar as opposed to primary, or loss of flight processing or data tag failures, controllers would change strategies to become more conservative, increase safety buffers, and go 'back to basics'.

Mitigation Strategies Associated with Environment Causes

There were many strategies that controllers identified to manage causes of degradation associated with the air traffic environment. Controllers reported a 'hierarchy' of control strategies that were used to control traffic in off nominal situations. For example, in a constrained airspace environment, altitude separation is preferred, as the controller can be confident that aircraft are separated with minimal monitoring. If this is not possible, vectors are used to maintain separation, followed by speed and miles in trail. Controllers will also 'borrow' some airspace from colleagues to gain more fallibility, however this strategy would only be used when many other options had been exhausted. Finally, as a last resort, a ground stop program can be implemented to stop further traffic from entering the airspace.

Mitigation Strategies Associated with Human Operator Related Causes

In general, controllers reported strategies to mitigate influences on human performance that were targeted either to mitigate the cause of the human factor influence (such as holding traffic in order to reduce workload) or mitigate the impact of human factor influences, such as the use of compensation strategies if feeling fatigued. This process occurs both for controllers to support their own performance, and controllers who apply adaptive strategies to support their colleagues' performance.

The application of the compensation strategy can result in the maintenance of performance even when associated with negative factor influences. The experienced negative influence may therefore not be reflected in the controllers' performance even though the influence is present.

E. The Concept of a System Envelope

Figure 3 is a conceptualization that aims to present a visual representation of the findings relating to interactions between degradation causes and the association with system performance. It should be emphasized that this is not a validated model, but a conceptualization only. It builds on the concept of a human performance envelope [8], applied to the wider ATC system. Its proposed that safety critical systems will have maximum 'limits' or tolerance – beyond which, system decline is likely to occur. It is also assumed that the system will have an optimum level of performance, and beyond this, a margin of tolerance, beyond which system performance limits are reached.

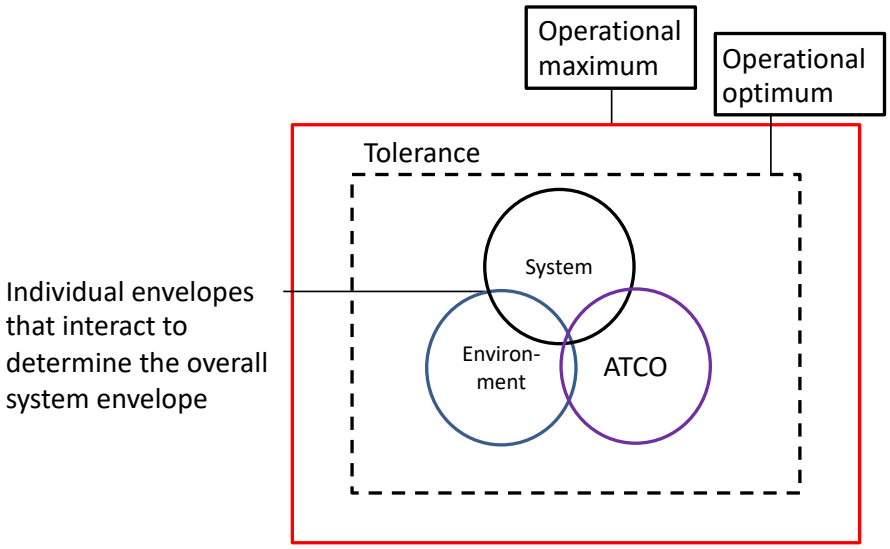

Figure 3. The concept of a system envelope

As identified in previous literature [3], and confirmed by the findings in the current study, causes of degradation can be broadly categorized into those resulting from technology, the environment or human operator. It is proposed that each of these component categories have an 'envelope', with an optimal operating level and performance limits. Each component category can also interact. For example, a technology failure, such as a critical failure of primary radar (without a backup) can be associated with higher workload and higher stress in controllers – moving beyond optimal operations in both categories. In this example, the environmental context could moderate the overall impact on the system. With low traffic, a controller may still be able to control procedurally, providing a control service to the airborne traffic, and maintaining system performance (with reduced traffic). However, if a radar failure were to occur in a high traffic scenario, the controller may not have the time or capacity to provide a service to the aircraft without further support from colleagues or supervisors, increasing the risk that a performance limit may be reached. In another example, a non-optimal event in the environment, such as an emergency or a thunderstorm, is likely to raise the workload of the controller. Depending on the context of the event, if the task demand and complexity was low at the time of the event, controller workload may not rise beyond capacity. however, if the controller was working a highly complex situation with many aircraft, and an emergency occurred, the additional task demand could push the controller to the limits of performance, if the additional taskload cannot be offloaded quickly. Although these are examples, it should be emphasized that it is the resulting combination of these interacting components that could provide insight into the system envelope, and the risk of reaching the limits of the system tolerance, leading to potential system decline. It is therefore essential to consider each element, and the interactions between them, to understand when the system is most at risk. In addition, by investigating and identifying the underlying relationships between these components, and the association with the effect on the wider system, a trade space for ATC system designers can be developed, so that future systems can be designed to stay within system tolerance limits when degradation causes occur.

IV.Discussion

The presented findings identified frequently reported causes of degradation, and prevention and mitigation strategies in the ATC system, based on controllers' experience. Reported findings have implications for designers of future ATC tools and systems, as well risk assessment and validation of future technologies.

Several of the findings that are discussed below can be argued to be 'common sense', or that are colloquially known, such as the importance of the role of the ATCO in achieving graceful degradation of the system, or that other causes of degradation apart from technological causes can negatively impact the ATC system. However, the specifics of such findings have been underrepresented in the research literature, enabling the current study to address these research gaps by specifying the degradation causes, and mechanisms by which controllers prevent and mitigate degradation in the ATC system and the requirements for these strategies to be implemented.

Categories of causes of degradation. The findings from the current study confirmed that many causes of degradation can be categorized into the broad categories of technology related causes, environment related causes and human-related causes. This result highlights the importance of recognizing causes of degradation in each category (rather than focusing only on one, such as technology failure) in order to gain an ecologically valid and comprehensive understanding of degradation in ATC. Subsequently, in order to predict and mitigate causes of degradation, causes from all three categories must be identified, as well as the interactions between them.

Direct and indirect effects of causes of degradation. Causes of degradation were identified to affect the ATC system both directly and indirectly. For example, the system impact of critical technology failures (such as radar and communications) has a direct impact on the ability to provide air traffic services, and is often highly visible. Indirect system effects, for example, a degradation causes that increases the likelihood of performance-influencing factors (such as an increase in workload or fatigue), which then is negatively associated with controller performance, can also result in a negative system impact, but are generally less visible and more challenging to predict and prevent due to numerous associations. Indirect effects on the ATC system are therefore more likely to be overlooked in both system design and the risk assessment of new systems. This distinction is important for future systems designers so that potential indirect effects on the system can be identified and mitigated.

The relationship between cause and system effect. The relationship between degradation cause and effect on the ATC system was confirmed to be moderated by many variables. The occurrence of one cause could result in no effect, or separate effects with differing severities. Moderating variable that were reported included the environmental context of the cause of degradation, including the airspace characteristics, characteristics of the surrounding airspace of the controlled sector, and traffic level. These findings emphasized that the potential causes of degradation must be interpreted within context in order to predict and mitigate the overall impact in the system. Findings from this research began to identify some of the key contextual factors that should to be taken into account when identifying the overall system effect. Further research should be completed to identify additional contextual factors, as well as online monitoring of these factors to predict when a system impact is most likely based on the causes present. This finding has important implications for system designers. By utilizing information regarding environmental and human operator moderators and complexity factors, it is possible to identify when systems are most vulnerable to system decline. Designers could account for this within a design trade space, for example, by ensuring that tools are not vulnerable to such complexity factors, or that tools should be used with specific traffic counts that are appropriate for all sectors and traffic levels. The implications of this finding are also important for the risk assessment process of technology, and validation specialists. Often, technology or system validations are conducted under nominal conditions. If 'off-nominal' (non-optimal) events are considered, the technology is usually assessed in context of one event, which is out of step with real-world operations. Testing and risk assessment should consider potential hazards and outcomes within real-world contexts, of different sector types, airspace characteristics, traffic levels and type, and off-nominal events that can co-occur, or relate to additional off-nominal events. Without taking into account the wider context, technology vulnerabilities and risks can be overlooked.

Controllers prevent and mitigate degradation. The importance of the role of the controller in modifying the relationship between degradation cause and system effect through prevention and mitigation was repeatedly highlighted in the findings. In general, potential degradation causes that are known and expected have already been mitigated, such as hardware backups for technology failures. Controllers therefore maintain system safety by identifying and responding to often unpredictable, dynamic events. The role of the controller in preventing system degradation is critical. This has several implications for system design. Causes of degradation that could relate to performance influencing factors such as workload should be prevented, potentially through the application of human-cantered design processes. In addition, time and airspace flexibility were identified as critical features that enabled controllers to adapt to dynamic changes in the control environment and respond with mitigation strategies. It is critical that future systems are designed to support controllers in responding to these dynamic situations, by designing in the flexibility that is required. For example, in future trajectory based operations(TBO), traffic efficiency will be increased through increased precision and reduced flexibility. However, maximum utilization of the system in terms of traffic loading could remove the required flexibility and time needed by controllers to implement a different control strategy. Therefore, an optimum level of traffic must be identified and implemented in system design which allows for increased traffic and efficiency, but still includes buffers that give the controller enough time and flexibility of the airspace to respond to dynamic events or risks.

Interactions between causes of degradation. A novel finding focused on the specification of the relationships and potential interactions between causes of degradation, and the subsequent association with controller performance and system impact. Interactions could occur as a result of co-occurrence or association. Identification and understanding of interactions between system elements, and the associated effect on controller and system performance is critical for the design of a system that can gracefully degrade. System risk or tolerances cannot be fully understood without the

consideration of interactions between causes and prevention mechanisms, and as a result, cannot be mitigated or prevented. By further understanding the relationships that can occur, predictions can be made regarding when degradation is most likely. Findings from this study provided an initial step to explore the relationships between these causes of degradation. Future research should further investigate interactions and relationships between degradation causes and association with controller performance and system effect.

Functional failure. An example of the potential consequences of interaction relationships was termed as 'functional failure' of ATC tools. This terminology descried a situation in which the tool was operational, but due to interactions with other systems or variables, the function and purpose of the tool was inhibited. Functional failure has the same potential consequences as actual failure of the tool (as the function is removed) but without the visibility of the tool actively failing. Potentially, mitigations or contingency plans may not be implemented. This is important, as controllers could then need to control without the tool, with levels of traffic that are calculated based on the assumption that the tool is functional. Depending on the function of the tool, and the benefits that it provides (such as reducing workload), functional failure may have a negative impact on controller or system performance. Functional failure may be prevented through prior identification of the potential interactions that could inhibit a tool's function. However, the potential of functional failure can only be identified through the assessment of interactions between the tool and other variables in technology, the environment and human operator. Assessment methods do not often take into account such interactions, resulting in a lack of identification and guidance of potential issues resulting from interactions. Future research should provide guidance for system designers and assessors to identify potential interactions that could result in 'functional failure' so that these occurrences can be prevented, or mitigated through contingency plans.

System envelope and implications. The implications of interactions between degradation causes on the overall system were represented using the concept of a system tolerance envelope. The representation has not been validated and is only intended to be used as a visualization of findings; however, it provides a presentation of the association between interaction relationships and the overall effect on the system. The concept suggests that a single component failure, unless critical to the provision of control, is unlikely to create a system impact to the extent that system limits, or tolerances, are reached. However, the combination of several 'failures', or degradation causes, can combine to potentially create a compound effect, potentially pushing system performance to, or beyond, tolerance limits. Future research should continue to investigate interaction relationships, and provide specification of the limits of each component: technology, environment, and human performance envelope [8], as well as system tolerance limits. Further identification of these interaction relationships, and system tolerance limits, could allow the design of a trade space for designers so that system performance remains within envelope limits, regardless of the context of the control situation. Future system design must take into account the overall tolerance envelope of the ATC system to guide designers to create the ability for graceful degradation and resilience of future ATC systems.

V.Conclusion

The current research had four specific aims. First, the research aimed to investigate causes of degradation in ATC (across all categories of technology, environment, and human) and the association with controller performance and the ATC system. A second aim was to investigate the relationship, and potential interactions, between triggers of degradation across the technology, environment and human operator categories, and the association with controller performance. The research also aimed to inform fundamental understanding of prevention and recovery of degradation in the current ATC system, with a specific focus on the contribution of ATCOs. A final aim was to inform understanding of the factors that could negatively affect the ability of an ATCO to prevent degradation or recover a degraded system.

Each aim was addressed and associated with findings with implications for both safety critical risk assessment and future design of air traffic systems. The influence and importance of interactions in the ATC system cannot be underestimated. However, previous research on interactions and the associated influence on performance and the wider system is sparse. Further research must be completed to fully specify the interactions that can create most risk to the ATC system, and how to predict and mitigate interaction effects. In addition, methodological should be developed to assess risk of interactions occurrences and effects.

With the vision of future ATC systems to increase precision and reduce flexibility (such as TBO), findings also have important implications for future system design. By providing designers with the principles of system tolerances – developed from understanding of degradation causes, interactions, and imitation mechanisms, a trade space could be developed to support designers in developing systems that operated within system tolerances, and are capable of graceful degradation.

References

[1]Hollnagel, E. "How resilient is your organisation? An Introduction to the Resilience Analysis Grid (RAG)." In *Sustainable transformation: Building a resilient organization*. 2010.

[2]Shelton, C. P., Koopman, P., & Nace, W., "A framework for scalable analysis and design of system-wide graceful degradation in distributed embedded systems", *Proceedings of the Eighth International Workshop on Object-Oriented Real-Time Dependable* Systems, CA, USA, 2003, pp. 156-163

[3]Edwards, T., & Lee, P. (2017). Towards Designing Graceful Degradation into Trajectory Based Operations: A Human-Machine System Integration Approach. *In 17th AIAA Aviation Technology, Integration, and Operations Conference*, p. 4487

[4]Millward, L. J. (2006). Focus Groups. In G. M. Breakwell, S. Hammond, C. Fife-Schaw, & J. A. Smith *(Eds.). Research methods in psychology* (3rd Ed.). UK: Sage Publications.

[5]Strauss, A., & Corbin, J. M. (1997). *Grounded theory in practice*. UK: Sage Publications

[6]Wilkinson, S. (2004). Focus Group Research. *Qualitative research: Theory, method and practice*, 177-199.

[7] Chang, Y. & Yeh, C. (2010). Human performance interfaces in air traffic control. *Applied Ergonomics*, 41, 123-129.

[8]Edwards, T., Sharples, S., Wilson, J. R., and Kirwan, B. (2012). Factor interaction influences on human performance in air traffic control: The need for a multifactorial model. *Work: A Journal of Prevention, Assessment and Rehabilitation*, 41(1), 159-166.