DESIGN AND FINDINGS OF A WORKSHOP REGARDING SECURITY PROCEDURES AND DEMAND FOR TECHNICAL SUPPORT AT A GROUND CONTROLLER WORKING POSITION

M. Schaper, O. Gluchshenko, H. Boumann
Deutsches Zentrum für Luft- und Raumfahrt, Lilienthalplatz 7, 38108 Braunschweig, Deutschland

Abstract

Unquestionably, security awareness is an important topic in air traffic control. The ground controller support system TraMICS includes already a security component and displays an indication regarding the current security situation to the controller. This paper reports about a workshop performed with eight controllers. It describes the methodology and the results of the workshop aimed to find out, how the security situations indicator, its concept, calculation and notification could be improved. Moreover, since security situations interrupt planned workflow, the paper investigates understanding and operational interpretation of the term disturbance in the air traffic ground controller domain and specifies its definition.

1. INTRODUCTION

Past projects validated the usefulness of an indication about security at an approach controller working position (1) and the sharing and correlation of such an indication on higher level (i.e. at airport level for an indicator at a ground controller working position) (2). The validation of the so-called Security Situation Indicator (SSI) provided by Traffic Management Intrusion and Compliance System (TraMICS) at a ground controller working position was scheduled together with the workshops this paper is about. The workshop aimed to improve the SSI by getting experts' opinions on some required parameters and procedures. In contrast to the validation experiments, which were performed with a specific parameter set on a specific airport with experts working at different other airports (3), the workshop aimed to be more generic.

1.1. TraMICS' Security Situation Indicator

The objective of the SSI is to enable the ATCO to quickly assess the current security situation at his working position (2). The SSI has a traffic-light colour-coding:

- green: no specific actions regarding security are needed;
- yellow: there were some suspicious actions detected, please monitor;
- red: there is most probably a security incident. Close monitoring is recommended.

It considers the following alerts:

1) non-conformant movement, i.e. it is detected, that a flight is deviating from a given clearance or starts e.g. pushback is performed without clearance:
2) conflicts, i.e. two aircraft are moving too close to each other:
3) ADS-B spoofing, i.e. the data received from ADS-B (Automatic Dependent Surveillance – Broadcast) are detected to be spoofed;
4) unauthorized speaker, i.e. an unauthorized speaker is detected on the used frequency (2; 4).

The SSI covers a specific time interval as sliding window (e.g. the last five minutes) and is updated periodically (e.g. each minute). The displayed colour depends on a set of rules and configurable thresholds depending on each alert type and level (i.e. red or yellow). For example, if the number of alerts of any kind in the sliding time interval exceeds a configured red-threshold, the SSI turns red. If less alerts, than the red-thresholds, but more than the yellow-threshold are counted, the SSI is set to yellow. In case no alerts or fewer than the yellow-thresholds are detected, the SSI remains green.

1.2. Human-in-the-Loop Experiments

The human-in-the-loop (HITL) experiments with a surface management system TraMICS enhanced by a security component to detect single security indications and to determine the SSI, were conducted with the participant just before the workshop. Each set of experiments required one participant at a time. All participants were not familiar with either the layout of the airport used, nor with the controller working position in detail. Certainly, both issues were briefed and trained before the first experiment. To perform the experiments, also the thresholds and time parameter (sliding interval size and refresh rate) which configure how the SSI behaves, had to be set. The experiments were hands-on experience for the participants and supposed to trigger awareness for the security context. A detailed description of the experiments and results can be found in (3).

doi: 10.25967/570102

2. METHODS

2.1. Sample

Eight apron and ground controllers (seven male, one female) from four German airports participated in the workshop. Their work experience as controllers ranged from 2 to 20 years (M = 9.56, SD = 7.47). Participants were aged between 24 and 45 years with a mean age of 35 years (SD = 8.62). Participants provided written consent and received monetary compensation.

2.2. Workshop Design

The workshops were conducted in the form of semi-structured interviews (5). Central questions were defined in advance, clustered into topics and prioritised. Even though the questions were structured to enable a smooth flow of conversation, there was some flexibility to the structure of the interview.
The questions for the interview were clustered into four consecutive topics:

A. *Security awareness state-of-the-art and need*: This section aimed to explore in what way knowledge about the cause of security-related incidents is relevant to a controller's work; How security incidents can be detected and whether there is a demand for technical support; And which kinds of security incidents are imaginable at a ground controller working position.
B. *Procedures*: This section dealt with current and possible future procedures that are or would be initiated in case of a security-related incident or the suspicion of such.
C. *Concept*: This section aimed to assess the demand for a support system that displays security incidents, which features such a system should include and which drawbacks could be associated with it.
D. *Calculation of the Security Situation Indicator*: This section aimed to evaluate the perceived usefulness of the SSI and possible improvements. Furthermore, participants were asked to judge the adequacy of the parameters considered by the SSI.

After the first workshops, an additional topic *Disturbances* was inserted. As this one was of general interest to establish a common understanding and not only security-specific, it had to be asked before diving again into the security theme.

2.3. Execution

The workshops were conducted subsequently to HITL experiments (cf. section1.2) as individual interviews. Two researchers were present at the minimum to conduct the workshop and to take notes in parallel. For some questions, answers were not obtained from all participants due to time restraints and the length of the preceding HITL experiments. As this was a known risk, the prioritization of questions was taken as a precaution and ensured that answers to all essential questions were obtained.

3. RESULTS

The following sections describe the answers of the participants in the order the topics were interviewed.

3.1. Disturbances

Any incident, no matter safety or security sourced, influences and disturbs planned controller's workflow. This topic with regard to disturbances aimed to understand operational interpretations of this term in the air traffic ground controller domain and – if possible – to specify a definition. There is a variety of interpretations among respondents how the term disturbance can be defined at the ground traffic control position. However, all controllers emphasised that traffic should be controlled in a 1. *safe*, 2. *orderly* and 3. *expeditious* manner. While acting in accordance with these principles, controllers still apply personal preferences. For instance, "First Come - First Served" or "giving someone who has had to wait a chance to catch up". Therefore, looking on the whole ground traffic control system at an airport, a disturbance could be considered as an event that causes a disruption of safe, orderly and expeditious traffic. Moreover, disturbances can be classified by their disruptive influence on the listed top priority objectives: "light" if the traffic cannot be controlled expeditiously, but still orderly and safely; "medium" if the traffic cannot be controlled orderly, but still safely; "heavy" if safety is at risk. The following list contains details of the six different perspectives:

[1] To one respondent, *disturbances are events that distract the controller from their work* and interrupt their workflow. These include noise in the background, e.g. co-workers speaking too loudly, and perturbances of the controller's mentally planned operational sequence, for instance caused by unruly or anxious passengers, interpersonal troubles, wild animals in the controlled area or bird strikes. Medical emergencies are considered as normal situations in this context. Disturbances according to this perspective can be solved including external persons or entities only.
[2] Another answer was that disturbances are external influences outside of the controller-pilot relationship. *Every event that interferes with the planned processes or has an influence (including positive influences) is a disturbance*. Examples included: technical failures, weather as well as medical emergencies.
[3] *Special cases and emergencies that constitute a hindrance are considered as a disturbance* by another workshop participant. Among them are, for instance, radio interferences, noise, false transmissions, not to get a gap in the frequency when it is critical, thunderstorms that result in holdings, sick passengers on board with need of ambulance service or bird strike with damages.
[4] Another point of view collected at the workshop was that *a disturbance is an event that can be resolved without external help*. This stands in contrast to the perspective summarized in [1]. Examples of a disturbances are pilots, ground staff or ground vehicles deviating from their usual behaviour and everything that can be solved within two to three radio transmissions. All that goes beyond is claimed to be abnormal and a big disturbance in the opinion of this participant. This includes emergencies or accidents that require the controller to initiate special procedures, e.g. writing a report.
[5] One controller divided disturbances into three categories, depending on the danger posed to life or physical well-being and the impact on operational processes: normal events, abnormal events and

emergencies. This means that the categorisation of events depends on the outcome of a situation. *An event is abnormal if it causes a system disorder, but without danger "to life and limb"*, for example medical events, unruly passengers, bird strikes and lightning strikes. *An emergency is an event that causes or potentially could cause people to suffer damage.* For instance, a serious bird strike can lead to an emergency. Weather events are usually normal but they can lead to abnormal or emergency situations, i.e. accordingly to the outcome they can become abnormal or emergency category.
[The authors would rephrase the definitions: *An event is abnormal if it causes a system disorder, but without danger for hull damage or loss of a flight (passengers and crew). An emergency is an event that causes or potentially could cause a hull loss or damage with a high risk for passenger and crew*].

[6] Another controller described disturbances as *events that can cause dangerous situations.* Those events were subdivided into three categories: red (risky and cannot be influenced by the controller, for instance not authorized persons at the frequency or at the airport facilities), yellow (risky but can be impacted, for instance clearance deviations or foreign objects at the airport area) and green (less risky, for instance wild animals on airport terrain). The respondent gave one more and stricter description of the term disturbance: *an event that led to imminent danger.* This description corresponds to the definition of a red event given by the participant.

3.2. Security Awareness State-of-the-Art and Need

Participants were asked if it makes a difference for their work if incidents have safety (i.e. unintentional mistakes) or security (intentional bad actions) related causes. This was affirmed by three participants and negated by five participants. Participants stated that both safety and security incidents result in an increase of controller workload. Nevertheless, if the source of an event is security related, the controller may not be able to resolve the situation without external help, e.g. the police. The controllers might get nervous and have to inform their co-workers in the air traffic control tower. If the source of an incident is safety-related, the controller is able to affect the situation on their own. In case the controller knew that a flight deviates by intent, the controller would try to stop this aircraft (and all others if necessary) and initiate aviation security procedures. Generally, controllers expressed that they find it difficult to determine if an event has a security-related cause. They have to rely on their experience and common sense as means for this and for some events, the cause gets apparent in retrospect only.
Seven participants were asked about their demand for technical support in the context of security. Two participants stated that they had no need for technical support in this context as they do not see security as a priority for their work or, in contrast to safety, as their responsibility. Five controllers would prefer to have technical support and named possible benefits: 1) Technical support may increase situation awareness, and 2) the information from the system could be used for documentation purposes; A prerequisite is that a support system in the context of security would have to be trustable. Additionally, the idea was raised that a briefing or checklist could be associated with events detected by a system.

3.3. Procedures

As warm up question, controllers were asked whether they have ever experienced a security incident or suspicion of such during their work and how they dealt with it. Among seven responses, there were two confirmative answers only. Additionally, four controllers reported that colleagues had experienced security incidents.
The following security incidents were listed:

- unauthorized access to apron. In this case the controller kept aircraft away until the problem was solved that required a lot of coordination amongst other with the adjacent air traffic control centre;
- unauthorized speaker. The Federal Police was informed;
- bomb threat at a plane. The controller contacted the pilot via an alternative frequency and established contact between pilot and police via mobile phone;
- forgotten luggage. The procedure was done according to a checklist;
- laser and drones. The information was shared with pilots and further procedures were initiated if necessary.

Depending of the severity of incidents different entities will be informed. While some incidents are subject to formal reporting, less severe incidents can be settled internally. For example, if someone enters the protected runway areas unintentionally but stops and does not enter the runway, this person will be instructed internally. However, every incident is processed consequently.
Regarding the frequency of security incidents, participants estimated that minor incidents occurred one to two times a month while major incidents with serious consequences occurred approximately once a year, sometimes with serious consequences. Very frequent security issues were reported to be unruly passengers, whereas medical emergencies occurred rarely, i.e. about once a week.
The interviewed controllers stressed that safety and security are closely related and a security incident may evolve into a safety issue. Safety always has priority for controllers. Therefore, a security issue is perceived as less stressful when safety has not yet been impacted.
According to the controllers, the way a suspected security incident is dealt with depends on several factors, e.g. the case, the possible source, the own perception and experience. In general, controllers will try to keep calm, maintain safety and inform all competent positions. Prevention and training on security events would be welcome.
Next, controllers were asked how a system that detects security incidents would impact the possible course of actions taken by the controller. It was of special interest whether new courses of action would be enabled or whether existing ones could be carried out faster. Eight answers were received. Two controllers did not see any new options to act. Six interviewees proposed new actions that could be enabled: It would be beneficial if the system is connected to the airport, fire brigade and the Federal Police in order to inform them. Also, the system could refer controllers to relevant checklists to follow. Another new option would be an improvement of situation awareness: to be able to classify whether someone is unintentionally not

following instructions or whether there is external influence. Automatic forwarding of information would be very helpful to report confirmed security incidents including callsign, runway and time of incident. This information should be used to automatically draft a report as this would relieve the ATCO by taking away the task of writing reports.

3.4. Concept

As a starting question, controllers were asked if they would like to have a system that displays security incidents. This was answered by seven controllers. Four of them affirmed, one disagreed and two were uncertain as it was not needed before. The advocates nevertheless set conditions: The system would have to be properly functioning, reliable and trustable; it should not increase workload; only events that affect the controller's work shall be displayed. One controller proposed the option that detections of the system could be displayed to a competent position to confirm or reject before announcement to the controller.
According to the controllers, an optimal system that displays security incidents should contain the following information: a categorisation regarding the kind of incident in a standardized form, including its location; time of incident and duration; involved flights; cause of the alert. More information should be visible on request of the controller (e.g. clicking on the alert). Also, linking the appropriate checklist or automatic reporting would be welcome.
Six answers were collected to the question if the controllers want to take part in the decision-making if an incident is security-related or the system shall judge only. Four of them preferred to participate and had the following comments: Confirmation with the possibility to override the system decision is welcome when the controller has the mental capacity for this task. All changes must be documented. Overriding would make sense in some cases, e.g. if the non-conformances detected are caused by an inexperienced pilot. The controller should also be able to insert security incidents the system has not detected. This could be used to make the system learn.
The question, which disadvantages such a system may have, these are the listed potential disadvantages: 1) The controller may need to differentiate which information is shared with other positions, e.g. to avoid panic, assuming, the SSI could be communicated automatically. This might trivialise the event. 2) Getting familiar with the system costs time and mental capacity. 3) The system could potentially cause information overload.

3.5. Determination of the Security Situation Indicator

The calculation of the SSI was explained during the briefing of the experimental trials performed directly before the workshop (ref section 1.2). The participants confirmed they have no questions about how the SSI is calculated. Six to eight participant answers were received regarding this topic.
The traffic light colour-coding was deemed appropriate and understandable. However, participants noted that the cause of a yellow alert level was not always comprehensible and sometimes confusing. Also, for some respondents it was difficult to understand the threshold values between the yellow and red scale of the SSI. Another comment was that the controller should have more freedom to decide themselves whether a situation is security relevant or not by means of a confirmation/rejection function. One controller stated that he would work his shift more carefully and aware in the presence of a red SSI, e.g. by checking or asking twice if their command is understood. It is desirable to have a warning tone or even flashing when the SSI alert level changes to red. The red notification about the detection of an unauthorized speaker was rated as important. However, the SSI should not display too much information at once. Rather, controllers should have a possibility to click on it for more information and to be able to forward information to appropriate positions.
The question whether the controller is the right addressee for the SSI and/or whether the SSI should be displayed to the supervisor received a clear answer: if there is a supervisor, the SSI should be displayed to him or her. Half of the participants suggested that both – controller and supervisor – should be informed because the controller is responsible for the safe traffic control (which might be impacted) whereas the supervisor may coordinate with other entities if there is a real threat and how to mitigate.
Estimations of an appropriate length of the evaluation interval of the SSI were highly varied. For the experiments, the sliding evaluation interval was configured to be five minutes long. According to the responses, different intervals (i.e. more than one at a time) would be preferable, depending on the type of alert and airport specific features. One suggestion was to include an interval with the length of the average or maximum time an average departure needs from pushback to take-off in addition to the five minutes sliding interval. Also, longer observation times (i.e. longer sliding window intervals) were judged to be especially important in the case of an unauthorized speaker, whereas some minutes are enough in the case of a drone. All controllers preferred to have at least two intervals simultaneously, some even three. For instance, a short interval containing the last five to ten minutes, a medium one (length between the maximum time a flight is active at the airport, including all working positions, up to six hours) and a long one covering the last 24 hours. Daily and weekly statistics of alerts produced by the SSI could also be useful.
Regarding the update rate of the SSI, different feedback was received. Four of seven respondents supposed that an update rate of one minute is sufficient, two controllers would like to have updates every 20-30 seconds, and one controller proposed updates every second. Another suggestion was that a red alert level should persist until the cause has been dealt with. The SSI would need to be reset manually in this concept.
The controllers were asked to estimate the helpfulness of automatically communicating security incidents that cause yellow and red SSIs according to a specified reporting chain. Six given responses are divided as follows: "yes, it should be realized" were stressed four times; "yes, but for red indicators only" was noted one time. One respondent had worries that this function could be used as quality control which would induce stress. However, the opposite opinion was also received: Forwarding or recording of SSI information could protect the controller. As part of *Just Culture*, recorded events could be used to improve training. Generally, automatism was found to be efficient and to help avoiding loss of information, to reduce workload and to provide a reliable way for the information to arrive at the right recipient. Such technical documentation makes sense, in retrospect it can still be corrected. Automatic communication could be used to warn neighbouring sectors about certain incidents, for instance unauthorized speakers. Despite the possible benefits an automatic

communication of information could offer, controllers stressed that the manual way of communication is still important as the system may fail or have errors.

4. CONCLUSIONS AND OUTLOOK

The workshop collected a lot of information and opinions with regard to increasing security awareness and events affecting air traffic (control). Even though both safety and security incidents result in an increase of controller workload, security related incidents may not be resolved without external help. Hence, technical support could be beneficial to increase situation awareness being able to classify whether someone is unintentionally not following instructions or whether there is intention behind, to inform responsible entities and to check or to document necessary information. It may also include manual or automatic communication of event information to the airport, fire brigade and the Federal Police. Checklists are proposed to be linked. The event information could also be used to automatically pre-draft a report to reduce ATCOs workload.
In summary, the following insights were obtained confirming our expectations: A security incident detection system shall work reliably and display as much information as needed with additional information on request only. Such a system has to be well configured (e.g. the thresholds for the SSI, local and common checklists, automatic communication configured to local conditions), briefed and trained before being used operationally. A function that enables the controller to input security events and modify, confirm or reject incidents detected by the system may ease coordination with other positions and entities in case of a security incident support controllers in the documentation of incidents.
In addition to the preceding HITL experiments which used one SSI with a sliding evaluation interval of five minutes, two additional ones were proposed covering a medium and a long (e.g. 24 h) time interval.
The results of the workshop offer several impulses for further research. As a next step, a concept for the calculation and display of three SSIs covering three different evaluation intervals at once could be explored. Another promising addition could be the design and implementation of an interactive function that enables the controller to confirm, reject or change detected security incidents and add new incidents. We are looking forward to pursuing investigations using the documented practice and approaches in the future methodological and experimental study.

5. ACKNOWLEDGEMENT

The project on which the presented research is based is funded by the German Federal Ministry of Education and Research (BMBF) as part of the call „Zivile Sicherheit – Kritische Strukturen und Prozesse in Produktion und Logistik“ with the funding number 13N15104. The responsibility for the content of this publication lies with the authors.

6. REFERENCES

1. *Validating an ATM Security Prototype - First Results.* **Tim H. Stelkens-Kobsch, Michael Finke, Matthias Kleinert, Meilin Schaper.** 2016. Proceedings of the 35. DASC conference.

2. *The Traffic Management Intrusion and Compliance System as Security Situation Assessment System at an Air Traffic Controller’s Working Position.* **Meilin Schaper, Olga Gluchshenko, Kathleen Muth, Lukas Tyburzy, Milan Rusko, Marián Trnka.** s.l. : 31st European Safety and Reliability Conference (ESREL), 2021.

3. *Validation of the Traffic Management Intrusion and Compliance System as Security-Awareness-Component at the Controller Working Position.* **Meilin Schaper, Hilke Boumann, Lennard Nöhren, Lukas Tyburzy, Kathleen Muth, Nils Carstengerdes.** Desden : submitted to: Deutscher Luft- und Raumfahrtkongress (DLRK) 2022, 2022.

4. *Speaker Authorization for Air Traffic Control Security.* **Marian Trnka, Sakhia Darjaa, Milan Rusko, Meilin Schaper, Tim H. Stelkens-Kobsch.** s.l. : SPECOM 2021, Springer-Verlag, Berlin, Heidelberg, vol. 12997, pp. 716–725, 2021.

5. *The qualitative interview in IS research: Examining the craft.* **Michael Myers, Michael Newman.** 2007. Vol. 17, pp. 2-26.