IMPLICATIONS AND BENEFITS OF AIR TRAFFIC CONTROLLERS' MANUAL ASSESSMENT OF THE SECURITY SITUATION INDICATOR

M. Schaper, O. Gluchshenko, L. Nöhren, L. Tyburzy
Deutsches Zentrum für Luft- und Raumfahrt (DLR), Lilienthalplatz 7, 38108 Braunschweig, Deutschland

Abstract

Validation trials with air traffic controllers followed by a workshop have confirmed, that the Security Situations Indicator provides valuable information at the controller working position. However, the possibility to adjust it by a competent person was proposed. This paper investigates potential implications of manual changes and proposes rules to maximize effectiveness. It outlines the design of the necessary user interaction and information and closes with some visualized examples.

1. INTRODUCTION

Due to an increasing number of cyber-attacks and other security related incidents, the concern about security threats is rising in the air traffic control domain (1; 2). The German Aerospace Center suggested and validated the Security Situation Indicator by which air traffic controllers can achieve an awareness of the current security situation (3). The SSI uses the traffic lights colour scheme: If the SSI is green, the controller can assume, that the security situation is fine, there is nothing special they have to care for. If it is yellow, there might be something security related going on and they shall be aware. If it is red, there is most probably a security incident and a high awareness and close monitoring is recommended.

The Traffic Management Intrusion and Compliance System (TraMICS) is the system calculating the SSI (4). It supports the ground air traffic controller at his working position and consists of two components: a surface management component, which plans, monitors and, if needed, adapts conflict free taxi trajectories. The second component is the security component, which calculates the SSI and presents it to the controller. Figure 1 gives an example of the SSI design and content and Figure 2 shows a screenshot of the used controller human machine interface (HMI) which includes an SSI message in the left upper corner. The SSI visualisation consists of two elements: a coloured dot representing the severity, which is green, yellow or red, and a text, containing the provoking condition for the colour.

Figure 1. Visualisation of the SSI. A yellow state is displayed, caused by conformance monitoring alerts for the flight DLH6PF.

Figure 2. HMI of the controller working position.

1.1. Considered alerts for SSI calculation

The SSI is calculated based on a rule-set including the following indications:

- the number of non-conformant movements,
- the number of unauthorized speaker transmissions,
- conflicts or
- detected ADS-B spoofing alerts.

To enable the detection of non-conformant movements, the controller has to input given (i.e. spoken) clearances into their working position. In case the controller does not input all clearances and cleared routes correctly and timely into TraMICS, this may lead to a higher number of detected non-conformances (in contrast to the spoken and radio-transmitted clearances to the pilots), which in turn may lead to an indication of a more severe security situation in contrast to inputting all clearances and cleared routes timely (i.e. at the same time as the clearance is spoken). Also, the rule-set used to calculate the SSI is not exhaustive, therefore the controller may notice a security issue, which is currently not covered by the rule-set calculating the SSI. This means, the displayed SSI status might not always reflect the current security situation correctly and should be adaptable by a competent person, which in this case is assumed to be the controller itself.

doi: 10.25967/610049

1.2. Motivation

Human-in-the-loop validation trials with air traffic controllers (3) followed by a workshop (5) have confirmed, that the SSI provides valuable information at the controller working position. Nevertheless, recommendations were collected to improve the usability of the SSI:

- To cover the above-mentioned challenges, the controllers proposed to have a possibility to manually adjust the SSI. E.g. if the SSI is red because the controller did not input the clearances into the system in time. The controller is aware of the fact and sure, that he is the reason and not any security issue. Then he wants to be able to change the SSI back to green.
- The rule-set to calculate the SSI covers already some kinds of alerts. For those, which are not yet covered, e.g. because there is no detector connected or even available, the controller shall be able to add an occurrence and change the SSI according to his experience. E.g. if pilots report a drone, this information shall be add-able to the SSI. Especially in regard with information sharing, when the SSI might be shared with other controller working positions or stakeholders like airport or police, this is assumed to have an added value.

2. CONCEPT FOR MANUAL SSI ADAPTIONS BY THE AIR TRAFFIC CONTROLLER

Before explaining the concept of manual adaptations of the SSI, the evaluation process used to get the SSI is described.

2.1. The SSI calculation based on the rule-set

As described in (4) the SSI is calculated periodically, e.g. each minute, covering a sliding time interval containing alerts that happened in the past $interval\_length$ minutes, e.g. last 5 minutes. The SSI is determined using a rule-set. Alerts that occurred in the specified sliding time interval are counted according to their type and compared to specific thresholds. Each alert type has yellow and red thresholds.

If at the moment of the SSI calculation the counted number of alerts of at least one alert type in the interval is higher or equal than the alert type's corresponding red threshold, the SSI will be set to red. In the case a counted number of alerts in the interval is not lower than the corresponding yellow thresholds, but all counted numbers are lower than their red thresholds, the SSI is set to yellow. If all the counted alert numbers in the interval are lower than the corresponding yellow thresholds, the SSI will be green.

For creation of the SSI alert types illustrated in Figure 3 and described below are used:

- conformance monitoring alerts. This alert type includes alerts for route deviation, direction or heading deviation and moving without appropriate clearance. The detection of these alerts is triggered by receiving updates of aircraft position data taking place each x seconds, where x depends on the environment.
- conflict detection alerts. Each conflicting aircraft will raise an alert of this type. The detection of these alerts is triggered by receiving updates of aircraft position data taking place each x seconds, where x depends on the environment.
- speaker verification alerts. This type is not flight dependent and raised each time an unauthorized speaker is detected in a radio transmission.
- ADS-B spoofing alert. For this type a message is received that for a specific aircraft received ADS-B (Automatic Dependent Surveillance – Broadcast) data is spoofed.

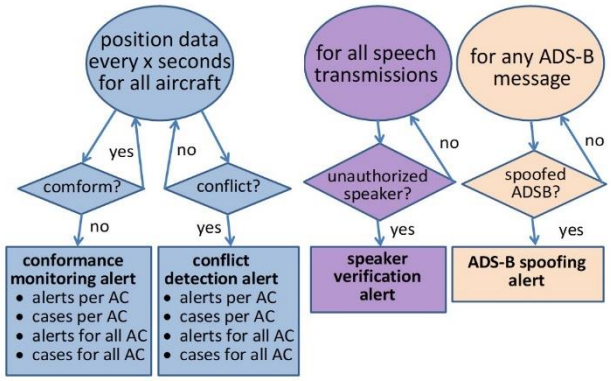


Figure 3. Alert types and their trigger used to create the SSI.

Each alert occurrence is counted in total per alert type and some of them also additionally per alert type and flight. Additionally, conformance monitoring alerts as well as conflict detection alerts are grouped and counted as "cases" if they can be assigned to the same triggering event. This reflects the human perception of one deviation lasting an amount of time.

2.2. General rules for manually changing the SSI

Performed experiments described in (3; 5) have shown the air traffic controllers request to manually change the SSI. The participants stated that this is appreciated, but has to be transparent and traceable. The reasons could be categorized in the cases:

- The alert type is already known i.e. configured in the rule-set. Due to expert judgement the calculated SSI colour does not match the situation.
- The alert type is not configured in the rule-set. The controller had identified a security event that is not yet covered by the rule-set used to calculate the SSI (2), i.e. there is no fitting alert type considered yet and the SSI calculation cannot take it into account.

We suggest the following general rules for the change of SSI by a human operator:

1) only alert type specific up- and downscaling is possible: Every change of the SSI (i.e. down- or upscale, where the lowest is green and the highest is red) refers to one specific alert type. After up- or downscaling of one specific alert type, the SSI calculation is updated immediately and additionally to the configured period. The rules for the red, yellow or green SSI are still applied. (E.g. two reasons both lead to red, but one of them is descaled to yellow. Than the SSI will remain red, until the other reason is either descaled to yellow

as well or out-dated at an update (assuming, that no new reason for red appeared). When both reasons are descaled, the SSI will change from red to yellow.)

2) reason specification: The operator has to specify or to select from a prepared menu a causing reason why he wants to scale up or down.
3) update of the corresponding alert counter: To comply with 1), every up- or downscaling of a specific alert type causing a colour change should be done according to the corresponding threshold. This means, that the specific alert counter should be changed (i.e. set to the corresponding lower threshold) and re-evaluated with respect to the available thresholds. Nevertheless, the complete number of alerts of the specific type shall be counted and logged for statistical analysis.
4) validity period of manual changes: If the operator changes the SSI of already rule-set considered indications, this impacts only the current time interval of the last $interval\_length$ minutes. Example: The controller scales the SSI down for conformance monitoring alerts from red to green. After he did this, new conformance monitoring alerts happen. If the count of them is not less than the yellow or red thresholds for the conformance alert type, the SSI will change to yellow or red with the next periodic update.
5) indicating a not yet considered alert type: If the controller changes the SSI because of a new indicator, which is not yet considered in the rule-set, this has to be set back manually. Scaling the SSI up due to a not-yet-considered reason requires, that the controller mandatorily has to add the reason, e.g. using drop-down-menu. Example: The SSI is green or yellow and the ATCO sets it to red, because he spotted a drone. This case is not mapped yet in the rule-set, so the SSI will stay red with the reason e.g. “drone in aerodrome” until the ATCO sets the SSI back to green, selecting that the “drone in aerodrome” is not valid any more. After that the SSI will again be re-calculated and updated according to the rule-set.
6) transparency of changes: Each change other than the initial calculation (i.e. the rule-set-based one) has to be labelled with that information to ensure transparency.

2.3. Detailed concept specification

To realise the implementation of the manual SSI inputs, some details of the above described concept were adapted or specified more precisely considering expected useful interactions.

When the SSI is manually scaled up, it is necessary to add additional alerts labelled with “added”, so that the total number of alerts matches the threshold of the target colour and the rule-set will re-evaluate the SSI in the desired colour. We decided to add those “added” alerts with the timestamp of the upscale-action. This will keep them being counted for the next $interval\_length$ minutes after insertion and they (or parts of them) will not vanish e.g. after the next periodic SSI update.

When the SSI is manually scaled down it is necessary to remove a certain number of alerts from the SSI calculation, so the remaining number of alerts matches the lower threshold of the desired colour and the colour will appear when the SSI will be re-evaluated. This “removal” of alerts is done by labelling the alerts as “devalued”. This way they can still be considered in statistics or be reactivated later. The alerts to be devalued are selected by age, i.e. the oldest alerts are devalued first.

In section 2.1, it is described that some alerts can be counted by the occurrences and by “cases” which encompass multiple occurrences of the same alert for the same flight that lie close to each other time wise. When the SSI is manually scaled up, it is never done based on cases but always based on the occurrences only. This is necessary since the “added” alerts which are used to upscale the SSI, are all inserted at the same time and would therefore only count as a single case. However, when the SSI is scaled down it might be necessary to consider cases. If the SSI has a certain colour because a case threshold but not the corresponding alert occurrence threshold was reached, it is necessary to remove complete cases to reach the proper lower threshold. Therefore, for an SSI downscaling it is always ensured that the case thresholds *and* the alert occurrence thresholds are not exceeded.

As explained in section 2.1, some alerts are counted per flight and some globally only, but even the flight-specific alerts are also summed up for a global value. In the initial implementation of the manual SSI changes, the changes were always done globally for the selected alert type, i.e. they would not count for a specific flight, but rather for the complete traffic situation. During testing this was deemed sufficient for upscaling of the SSI. For the downscaling, it became clear that it often makes more sense to remove alerts for a specific flight. Therefore, it is now possible to either change the SSI to a specific colour for a certain alert type, which will reduce the global alert count for that type, or to remove alerts relating to a specific flight. The latter might not immediately change the colour of the SSI, since the global thresholds could still be exceeded by alerts of other flights.

In section 2.2, it was stated, that the operator needs to specify a reason for any up- or downscaling. During the first tests, this was deemed as not necessary for most alert types. The possibility to devalue specific alert types for specific flights is even better to show the reasoning for any downscaling of the SSI. The reason for an upscaling is implied by the selected alert type. Only for new alert types, that are not yet considered in the rule-set, an explicit reason is necessary and should always be selected.

If the colour of the SSI is changed for an alert type, that is counted per flight as well as globally, the change needs to be distributed among flights and must not be assigned to a single flight. This is deemed necessary, because it is expected, that the flight specific thresholds are lower than the global threshold of that alert type. So, if the changes to cross the global threshold would be applied to a single flight only, the flight specific threshold would be exceeded most probably for this specific flight as well. Therefore, the alerts that are inserted for an SSI upscaling and the alerts that are devalued for an SSI downscaling should be distributed among flights. For an SSI upscaling the inserted alerts are evenly distributed among *all* active flights. For an SSI downscaling the devalued alerts are selected percentual from all flights with existing alerts. I.e. the more alerts of a certain type a flight has, the more alerts are devalued.

3. SSI HUMAN MACHINE INTERFACE

In this chapter, the HMI is presented with examples showing user interactions. The figures used in the following show user interactions with the system as time series, divided in labelled subfigures. The mouse cursor in form of a hand marks where the user would click to proceed to the next step/subfigure.

The SSI is displayed in a notification box which is permanently visible on the traffic situation display of the air traffic controller. This notification box shows by default only the SSI with the highest severity (see Figure 1). The SSI notification box can be expanded by clicking it (anywhere inside, except the coloured dot. Clicking the coloured dot is described in 3.1 and 3.2) (Figure 4a). It will stay in the expanded view until the controller clicks the top-level alert again to collapse the list. When an update for the SSI is generated by the system, the expanded view will be updated as well. In the expanded view Figure 4b) all alert types considered for the current SSI are displayed. They are organized in separate bays for the different alert types, divided by grey lines. Within the bays the alerts are ordered by the last alert occurrence (i.e. newest alert of this type on top). If an alert case is still ongoing, for example if a flight is currently moving without clearance, that is indicated with “still ongoing”.

Figure 4. Opening and closing the expanded view of the SSI.

The possible interactions are described using the following examples.

3.1. Scaling the SSI up

Figure 5 shows the upscaling of the SSI for the alert type conformance. First, the coloured indicator of the SSI is clicked (Figure 5a) to open the manual selection menu (Figure 5b). The menu opens directly where the SSI notification box was previously shown. Afterwards the desired colour (here: red) is chosen, which opens the type of alerts menu in place of the manual selection menu (Figure 5c). There the type is selected (here: conformance).

After the type selection, the menu vanishes and the SSI notification box re-appears in its place. The newly calculated SSI is shown in the notification box with a remark of the original SSI colour and with the note, that it was manually changed (Figure 5d).

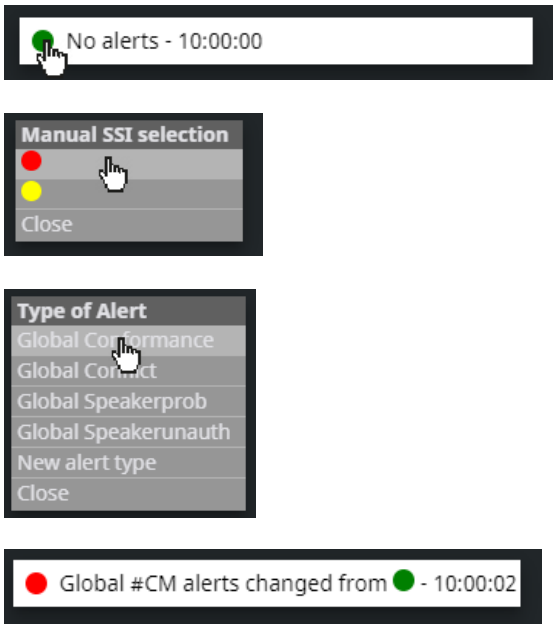
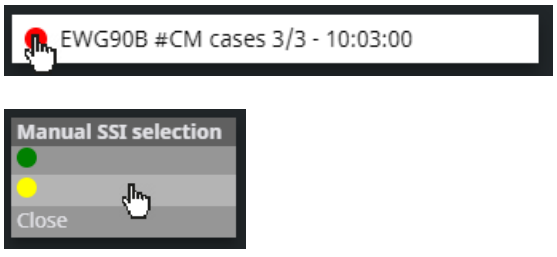


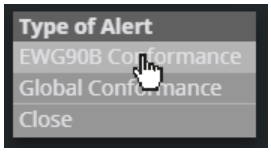
Figure 5. Changing the color of the SSI to red for the alert type conformance.

3.2. Scaling the SSI down

The procedure for the downscaling of the SSI is started analogue to the upscaling, but after the colour was selected, the next menu shows only the alert entries for which a downscaling is possible, i.e. only alert types which have a higher SSI colour than the selected target colour. In case only one alert type with such a colour is present, the type selection is skipped, as can be seen in the example of Figure 10. Figure 6 on the other hand shows a red SSI changed to yellow where the global red conformance monitoring case threshold and the flight specific red conformance monitoring case threshold for the flight EWG90B both are exceeded. Therefore, these two options can be selected in the alert type selection menu (Figure 6c). After the flight specific alert was selected, all alerts of the flight are devalued, which leads to undercutting the global conformance alert case threshold and therewith the SSI changes to yellow (Figure 6d).



c)



d)

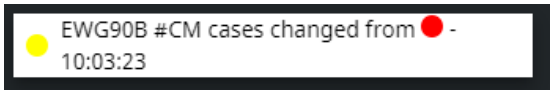
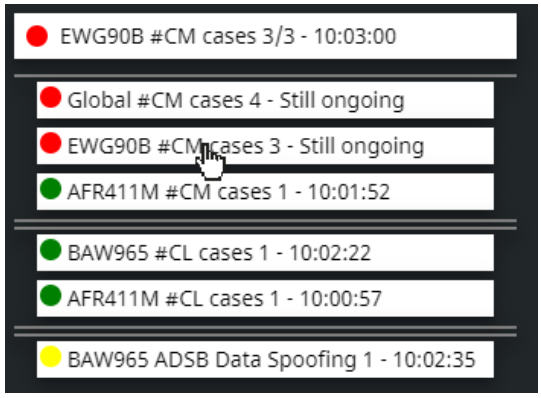


Figure 6. Changing the colour of the SSI from red to yellow for alert type conformance for the flight EWG90B.

3.3. Devalue and re-activate flight specific alerts

If the controller wants to devalue specific alerts for a specific flight, he can do this. He has to expand the SSI information by clicking the text in the SSI notification box (Figure 4a). This will open the expanded SSI view. Here, he can click the alert line(s) to devalue the corresponding alert (Figure 7a). Afterwards, the alert lines are still shown but greyed-out (Figure 7b). The corresponding alerts are devalued and will not be considered in the overall SSI calculation. In the example of Figure 7 the conformance monitoring alert cases for the flight EWG90B are devalued in the expanded SSI view. This leads to a re-evaluation of the SSI which changes the colour from red to yellow.

a)



b)

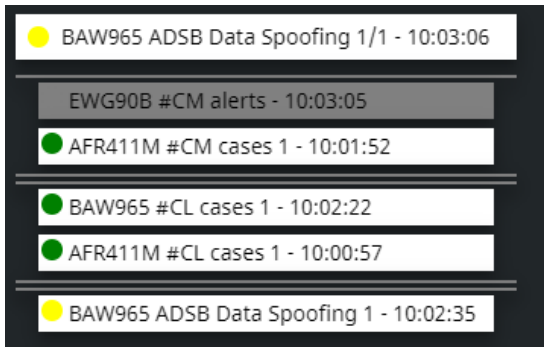
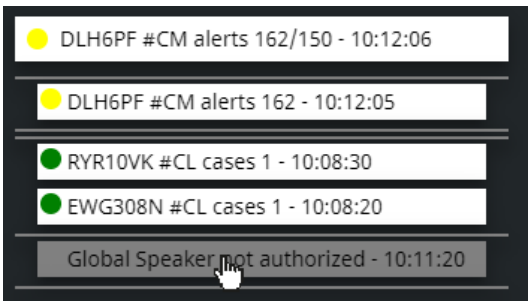


Figure 7. Devaluing a flight specific alert by clicking it in the expanded SSI view.

With a click on the greyed-out entry the controller can re-activate the corresponding alert (Figure 8a), which will trigger a re-evaluation of the SSI, where the re-activated alert is again considered in the rule-set (Figure 8b).

a)



b)

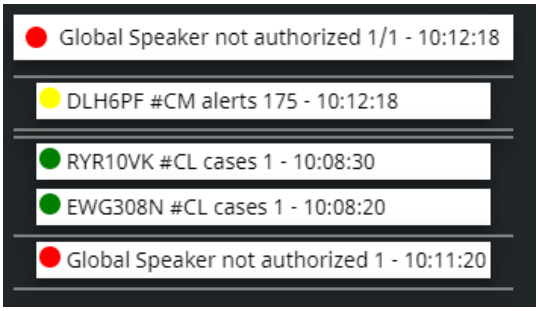
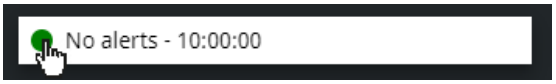


Figure 8. Re-activating a flight specific alert by clicking the greyed-out entry in the expanded SSI view.

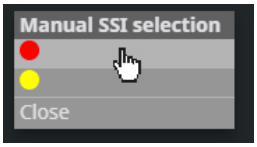
3.4. Adding and removing a currently unknown alert type

An alert with a new type, that is not yet considered in the normal rule-set of the SSI, can be inserted with the same mechanism as described in section 3.1. As shown in Figure 9c, the only difference is, that the user has to select “new alert type”. This action will remove the menu and open another menu, where the reason for this new alert has to be selected (Figure 9d). The entries of this reason menu are configurable and can therefore be easily exchanged or expanded. After the reason is selected, the SSI will be updated and displayed in the notification box with the selected reason (Figure 9e).

a)

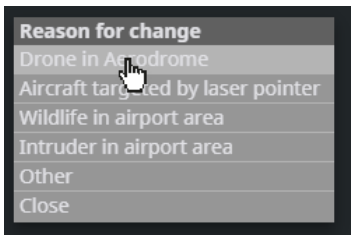


b)



c)

d)



e)

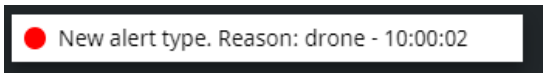
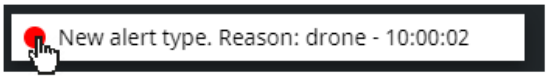


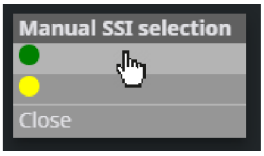
Figure 9. Changing the colour of the SSI to red for a new alert type after a drone sighting.

As described in section 2.2, a manually inserted alert for an unknown alert type needs to be manually removed by the controller. To do that the same procedure as described in section 3.2 can be applied: clicking the coloured indicator (Figure 10a) to open the manual selection menu (Figure 10b). To fully remove the alert, the green colour can be selected. In case the manual alert was the only alert with a severity higher than green, like in Figure 10, the alert type menu is skipped. After selecting green, the notification box without the drone alert is displayed (Figure 10c).

a)



b)



c)

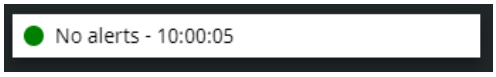


Figure 10. Removing the alert with an unknown alert type.

4. CONCLUSIONS AND OUTLOOK

As described above, a concept and its implementation enabling air traffic controllers to manually change the SSI are presented. The user interactions and their implications to comply with the rule-set calculating the SSI are described. The latter is mandatory to allow automatic changes of the SSI in case the situation gets more severe. Nevertheless, erroneous assessments can be corrected by the controllers. As next step, experiments will be designed and conducted to get experts' feedback of the concept in general and the HMI usability.

REFERENCES

1. **AP News.** Berlin man caught directing flight traffic with radio. [Online] 29 01 2021. [Cited: 14 09 2022.] https://apnews.com/article/arrests-berlin-f56833f73c7ecfa34a5ed5e6461669bc.
2. **Security Magazine.** Air Traffic Control System Vulnerable to Cyberattack. [Online] 10 4 2015. [Cited: 04 09 2023.] https://www.securitymagazine.com/articles/86298-air-traffic-control-system-vulnerable-to-cyberattack.
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.** Dresden : Deutscher Luft- und Raumfahrtkongress (DLRK) 2022, 2022.
4. *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.
5. *Design and Findings of a Workshop Regarding Security Procedures and Demand for Technical Support at a Ground Controller Working Position.* **Meilin Schaper, Olga Gluchshenko, Hilke Boumann.** Dresden : Deutscher Luft- und Raumfahrtkongress (DLRK) 2022, 2022. Deutscher Luft- und Raumfahrtkongress (DLRK).