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

Deutsches Zentrum für Luft-und Raumfahrt e.V. (DLR), Lilienthalplatz 7, 38108 Braunschweig, Germany. E-mail: firstname.name@dlr.de

Milan Rusko, Marián Trnka

Ústav Informatiky, Slovenská Akadémia Vied, Dúbravská cesta 9, 845 07 Bratislava, Slovakia. E-mail: firstname.name@savba.sk

The need to protect air traffic control against attacks and detect security incidents is widely accepted. Nevertheless, depending on the systems and procedures, it is sometimes difficult to distinguish whether "something is not as it should be". On the one hand, it could be due to a failure, on the other, it could be because of an intentional interruption/abuse. This paper lists five specific kinds of indications that may be found analyzing the traffic situation and the radio communication at a controller working position and details how they are detected. Those indications are non-conformant movements, conflicts, unusual clearances/behavior, unauthorized speakers and detected stress. Furthermore, a correlation function is described which determines the security situation indicator. This indicator categorizes the security situation into three different states expressing how likely it is that the detected indications may represent a security situation needing attention: "green", meaning there are no security-related actions needed; "yellow", meaning something seems strange, be aware; and "red", meaning that there is most properly a security incident. The Traffic Management Intrusion and Compliance System (TraMICS) is supposed to assist as well the air traffic controllers and the operators in a security operation center by being part of an airport security architecture.

Keywords: ATC security, TraMICS, correlated security indicator, security situation indicator, airport security, controller working position.

1. Introduction

Security is a raising topic in aviation. Therefore, new security improving methods and procedures are introduced continuously. Nevertheless, some well-established and safe, but not necessarily secure systems are still used like the controller-pilot radio voice communication. This communication channel is not protected, can be intruded (AP 2021) and unauthorized commands to the aircraft can cause irritation or even accidents. The Horizon 2020 project SATIE (Security of Air Transport Infrastructures of Europe) offers new solutions to deal with security even with older systems like the aforementioned voice communications at airports including prevention, detection and mitigation.

It is commonly known that accidents and incidents can happen by human mistake, without any bad intention. This is also true for route deviations and even conflicts on the airport surface. But there might be a situation, where unauthorized speakers breach into the communication and provoke safety critical situations. All others must not necessarily be security related. Nevertheless, if unusual and/or safety relevant situations happen more often than usual, this should be noticed and evaluated by a human operator, if it might be a security issue. The Traffic Management Intrusion and Compliance System (TraMICS) which is described in the following serves as one detector in the SATIE project and links also security findings in the air traffic control domain including the voice communication to the airport domain.

2. TraMICS overview

TraMICS serves as a detector for potential security incidents at a specific area of responsibility of an Air Traffic Controller (ATCO). TraMICS analyses the traffic situation combined with analyzing voices participating in the controller-pilot radio-communication. This leads to five different kinds of indications/alerts which TraMICS aggregates to a security situation indictor. One instance of TraMICS is dedicated to a specific air traffic controller's area of responsibility. As the SATIE project is focusing on the airport, the apron/ground working position was chosen for implementation.

It is sometimes difficult to decide if "something is not as it should be". If e.g., two aircraft conflict, this is for sure a safety issue and is not as it should be. Nevertheless, on the one hand it could be due to a failure, i.e. a pure safety issue, on the other, it could be because of an intentional interruption/abuse, i.e. a security issue which provoked a safety issue. The indications TraMICS could detect and use thereafter for determination of the security situation indicator are: non-conformant movements, conflicts,

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_550-cd

unusual clearances/behavior, unauthorized speakers and detected stress.

Some of the indications used to determine the security situation indicator are also safety related issues and shown to the ATCO. Nevertheless, TraMICS is not intended to be a safety-enhancing tool primarily and to replace existing safety solutions (e.g. using A-SMGCS). TraMICS is conceptualized as add-on.

For TraMICS, two kinds of human operators are concerned: (1) The ATCOs working at a TraMICS-equipped working position; and (2) any other possible downstream operators, dealing with security; in case of SATIE the operator in a security operations center (SOC).

3.1. *Pre-requisites*

As pre-requisites to build the TraMICS tool some assumptions have to be taken. It is expected, that the ATCO is able to input clearances and taxi routes electronically e.g. via electronic flight strips or the traffic situation display like required for higher levels of A-SMGCS (EUROCONTROL 2018). Additionally, the authorized speakers on the radio frequency have to be enrolled to get their uniquely associated 'X-vector', which is comparable to a fingerprint (cf. section 3.3). The ATCOs' enrolments could be saved on their working position ID cards assuring privacy and data protection. The pilots' ones have to be managed by their employers as well and could be attached to the flight plans which are shared on a need-to-know basis (i.e. only with sectors and airports the flight passes). This enrolment and sharing process is currently not operational.

2.2. *TraMICS architecture*

TraMICS has a modular architecture. As shown in Fig. 1, it is composed of seven modules: The Autorouter to assign initial routes to each flight, the Traffic View Message Interface as interface to the ATCO CWP (Controller Working Position), the Correlation Module (CORE) to determine the security situation indicator and four detection modules: Conformance Monitoring and Conflict Detection (CMCD), Clearance Monitoring, Speaker Verification and Stress Detection. The Stress Detection module is depicted dashed, as it was not integrated in the TraMICS tool due to ethical concerns.

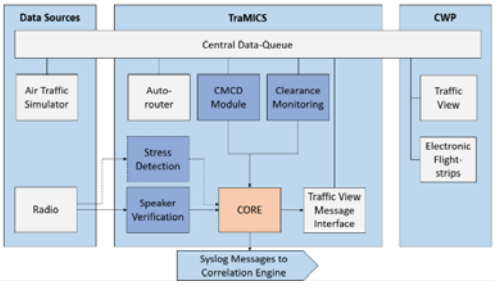

Fig. 1. The TraMICS modules.

3. The detection modules

The TraMICS concept foresees four detection functionalities which will be described in the following sections.

3.1. *Conformance monitoring and conflict detection*

The TraMICS assigns a route to each flight, which can be changed by the ATCO at any time at the CWP. The reception of updated aircraft position data provided by the verification environment triggers:

- monitoring of conformance of the aircraft movement to the planned route,
- monitoring of conformance to given clearances (this includes monitoring of movement to not yet given clearances, e.g. taxi clearance is not given, but aircraft starts taxiing), and
- detect potential conflicts with other aircraft (AC).

The distances used to detect route deviations or conflicts are configurable. Table 1 lists the outputs, the CMCD module could generate.

Table 1. Possible output from the conformance monitoring and conflict detection module.

Short name	Description
ROUTE DEV	Aircraft is deviating from planned route.
ROUTE DEV [opposite heading]	Aircraft is on planned route but with opposite heading.
NO ROUTE	Aircraft is taxiing although no planned route is available.
NO CLR	Aircraft is either pushing back or taxiing without the appropriate clearance.
Conflict with <callsign of another AC>	Aircraft is conflicting with the other aircraft.

3.2. *Clearance monitoring*

Clearance order monitoring is a marker to detect unusual behavior. Depending on the airport and the specific parking position, a well-defined order of clearances is used to process a flight. Clearance input triggers the monitoring of the order/fitting of clearances and updates of aircraft position data trigger the monitoring of conformance to given "hold immediately" (HOLD)-clearances.

To verify the order and fitting of the given clearance they are compared to a specified, but configurable, clearance sequences. Arrivals and departures with rollout or pushback positions are distinguished. The additional HOLD clearance is possible at any time.

Table 2 lists the outputs the clearance monitoring module could generate.

Table 2. Possible output from the clearance monitoring module.

Short name	Description
No appropriate CLR	Pushback clearance is given for aircraft at a rollout stand.
NO PUSH CLR	Aircraft at a gate stand has no pushback clearance but taxi clearance instead.
NO TAXI CLR	Aircraft has no taxi clearance but line-up clearance instead.
NO LND CLR	Aircraft has not received landing clearance but taxi clearance instead.
TX instead of HLD	The aircraft has received a "hold immediately" command, but its speed is increasing. (This may happen either without having stopped or the aircraft has stopped and starts moving again without clearance to do so.)
Not Stopping	Aircraft is not stopping after a "hold immediately" is given and moves constantly. (This will also happen, if the aircraft has decreased its speed but moves constantly with low speed instead of stopping.)

3.3. *Speaker verification and authorization*

In the speaker verification, a binary decision is done and the claimed identity of a speaker is confirmed or refused.

There are two types of speaker verification: text-independent speaker verification verifies the identity without constraint on the speech content, and text-dependent speaker verification requires the speaker uttering exactly the given password. The approach used in this work is text independent.

In this work, speaker authorization (SA) designates the ability of a system to identify whether a speaker belongs to those having the permission to access the voice communication channel. The speakers trying to take part in the communication without the permission are designated as intruders (impostors). There are several speakers who are authorized to communicate in a certain flight sector in any particular time and the number of potential intruders is practically unlimited.

To address this, a model of the incoming voice is created and compared to the group of models belonging to the authorized persons. The list of authorized persons is called the "whitelist" and the group of persons actually listed is called the "whitelist cohort".

A speaker recognition can generally be done on a closed set of speakers, in which all the possible speakers are known, or on an open set, where the test sample may belong to a speaker that is unknown to the system. In contrast, a speaker authorization is an open-set task that can be considered as a group-verification problem, as the specific identity of the speaker in the group is not important and only the affiliation to the group is verified.

Consequently, a binary decision is done in the speaker-group verification, by which the affiliation of a speaker to the "authorized" group is confirmed or refused. However, to achieve this goal multiple binary comparisons (speaker verifications) have to be done between the incoming sample and all the enrolled voices from the actual whitelist cohort. If the maximum score of all these comparisons is lower than a pre-defined threshold, the tested speaker is considered an unauthorized person.

The illustrative schematic diagram of the architecture of the SA module is presented in Fig. 2.

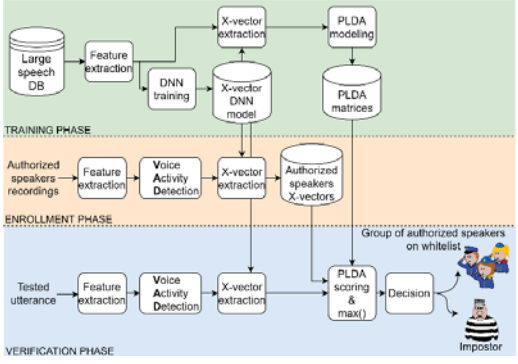

Fig. 2. Schematic diagram of the Speaker Verification module – training phase, enrolment phase and verification phase.

Technically, the Speaker Verification module is based on the X-vector approach (Snyder, et al. 2018). A Deep Neural Network (DNN), which was trained to discriminate between speakers, maps variable-length utterances to fixed-dimensional embeddings that are called X-vectors. Simply put, the X-vectors serve as speaker models.

In the verification phase, an X-vector is extracted from the tested utterance and the Probabilistic Linear Discriminant Analysis (PLDA) (Kenny, et al. 2013) is used to calculate a similarity score against the X-vectors of the whitelist cohort. A decision on belonging to the whitelist cohort is made by comparing the maximum similarity score with a threshold. Table 3 lists the outputs the speaker authorization module could generate.

Table 3. Possible output from the speaker authorization module.

Short name	Description
NOT_AUTHORIZED	Speaker does not belong to the current whitelist.
AUTHORIZED	Speaker belongs to the current whitelist. Speaker ID is returned.
INDETERMINATE	The value of similarity score doesn't allow to make a reliable decision.
TOO_SHORT_FOR_EVALUATION	The utterance is too short for a reliable decision.

3.4. *Stress detection*

The Stress Detection (SD) module continuously monitors the radio voice communication. It searches for known voice qualities and patterns that are typical for speech under stress. This function estimates the stress level of each utterance and provides a stress score. It is expected that unusual/emergency situations like security and safety events lead to stressful situations on the pilot's and controller's side. The stress may be reflected in the person's voice. The measured stress score can contribute to a correlation process and therefore helps to identify such situations.

The stress-inducing events or situations that happen to a person, are called "stressors" or "stressor exposures". The cognitive, emotional and biological reactions that such situations evoke are called "stress responses". Acute psychological stress responses are often measured by detecting specific emotional states. This is because negative emotional responses (fear, anxiety, sadness, anger) to an acute stressor are considered a core component of an acute stress response (Epel, et al. 2018).

In psychological theory, concepts of emotions and stress are largely interconnected (Lazarus 1993). Based on dimensional models of affect (Russell 1980), notion of stress may be associated with high arousal (physiological activation) and low emotional valence (unpleasantness). The stress detection concept adopted in this solution therefore consists of two branches of measurement. Main stress measurement is realized by the system trained on the speech-under-stress database StressDat (Sabo, et al. 2021). This database was developed specially for the purpose of continuous-value stress evaluation and due to the material consisted in the database, the output value of the stress-detection branch is mostly correlated with arousal.

The technology of DNN modelling using X-vectors (Snyder, et al. 2018) was applied to build the SD module. The illustrative schematic diagram of architecture of the SD module is presented in Fig. 3. The output of the SD is a "stress-level score", representing the level of stress in the speaker.

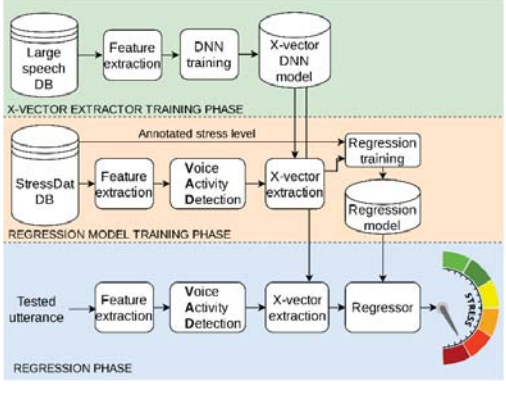

Fig. 3. Schematic diagram of the Stress Detection module – training phase, enrolment phase and regression phase.

For ethical and health reasons, it is impossible to expose subjects to higher levels of stress in validation trials, especially stress-inducing situations where the health of the speaker may be endangered. Therefore, the SD module was not integrated into TraMICS in the current phase of research, and its functionality was verified in laboratory conditions on the available speech-under-stress and emotional speech databases.

4. Determination of the security situation indicator

TraMICS is designed to support the security situation awareness of the operators. It takes all single indications of the prementioned detection modules and determines the current security situation indicator. This indicator categorizes the security situation into three different states expressing how likely it is that the detected indications may represent a security relevant situation: "green", meaning there are no security-related actions needed; "yellow", meaning higher monitoring effort is needed; and "red", meaning that there is most likely a security incident and a high attention is recommended.

In contrast to the GAMMA (Global AtM security MAnagement) FP7 project, where a weighted function had been used to calculate a correlation value (Stelkens-Kobsch, et al. 2016), the approach in SATIE is based on counting the numbers of different kinds of alerts within a specific time window W (e.g. the last 10 minutes), thresholds, and a rule set. The security situation indicator will be re-assessed periodically each P minutes. This approach is expected to be more transparent and adjustable to the user.

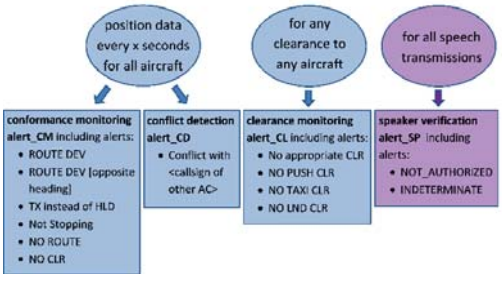

Fig. 4. Schematic of the inputs used to determine the security situation indicator.

For the determination of the security situation indicator, the alerts from the detection modules are divided into the following alert types illustrated in Fig. 4:

- alert_CM: conformance monitoring alerts. This alert type includes alerts for route deviation, direction or heading deviation and moving without clearance. The detection of these alerts is triggered by receiving updates of aircraft position data (each x seconds; x depending on the environment).
- alert_CD: 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 (each x seconds; x depending on the environment).

- alert_CL: wrong clearance order or mismatching clearances. The detection of these alerts is triggered by receiving an inserted clearance (depending on the clearance order model it should be less than 10 times per flight).
- alert_SP: speaker verification alerts. This type includes not authorized speaker and alerts resulting from examination of the INDETERMINATE messages: too low score authorized speaker (i.e. the calculated score value is less than the corresponding "red" score threshold) and very low score authorized speaker (i.e. a score below the "yellow" score threshold, but above "red" threshold) alerts. The detection of these alerts is triggered with each radio communication. It is not flight dependent.

As alerts of the types alert_CM and alert_CD are triggered by the receival of updated position data and therefore may occur several times for the same reason. In order to differentiate between the different reasons, the definition of cases of alerts depicted in Fig. 5 is introduced: *For the given ordered set of timestamps* $t_1 < t_2 < \cdots < t_j < \cdots < t_n$, *where* $1 \leq j \leq n$, *when a particular alert was created, a subset of consecutive alerts with the timestamps* $t_i < t_{i+1} < t_{i+2} < \cdots < t_u < \cdots < t_m$, *where* $1 \leq i$ *and* $m \leq n$, *is considered as a* ***case****, if for any consecutive pair* (t_u, t_{u+1}), $i \leq u \leq m-1$ *the difference* $t_{u+1} - t_u$ *is less or equal to a predefined time constant* T, however when $i > 1$ is $t_i - t_{i-1} > T$ and when $m < n$ is $t_{m+1} - t_m > T$.

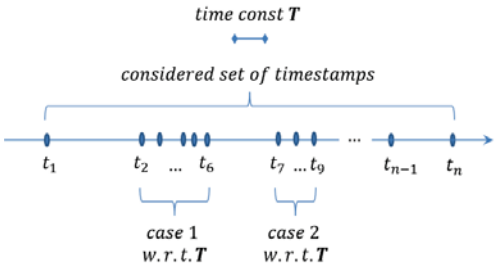

Fig. 5. Schematic of the case definition.

In other words, the time difference between two consecutive timestamps of the considered subset does not exceed the given constant value T and the difference between the first timestamp of the considered subset and its predecessor at the case $1 < i$ and between the last timestamp and its successor at the case $m < n$ in the given ordered set of timestamps exceeds the value T.

This case definition represents the human interpretation of a non-conformance or conflict, whereas the number of alerts belonging to a specific case reflects human interpretation of the duration. For the alerts of types alert_CM and alert_CD both, single alerts and cases, will be counted and considered when determining the security situations indicator. For alerts of type alert_CL each occurrence will be rated according to the human interpretation as case and therefore only the alert_CL cases will be counted.

Table 4 summarizes conditions that are used by TraMICS to generate the security situation indicator. The left column contains the main description of requirements that lead to one of three possible indications – "green", "yellow" and "red". The right column addresses the number of particular alerts and their corresponding thresholds that should be exceeded to cause one of the indications. The thresholds in Table 4 begin with the respective color indication. The character "#" is used to replace the term "number of". For instance, the condition "# unauthorized speaker alerts≥ red_SP_unauthorized" is to interpret as "the number of unauthorized speaker alerts is not less than the corresponding threshold indicating "red" number/too many of unauthorized speaker alerts". Currently red_SP_unauthorized is set equal to 1, as an unauthorized speaker is clearly a security incident and consequential there are no further condition for the number of unauthorized speakers needed.

Table 4. Conditions used to determine the security situation indicator.

Conditions	Single alerts and their thresholds
● **"red":** when at least one of the numbers of alerts/cases in the time window *W* **is not less than the respective red threshold**	# unauthorized speaker alerts≥ red_SP_unauthorized
	# too low score speaker alerts ≥ red_SP_unauthorized
	# very low score speaker alerts≥ red_SP_very_low
	# CD alerts per AC≥ red_CD_alerts_AC
	# CD cases per AC≥ red_CD_cases_AC
	# CM alerts per AC≥ red_CM_alerts_AC
	# CM cases per AC≥ red_CM_cases_AC
	# CL cases per AC≥ red_CD_alerts_AC
	# CM alerts for all AC≥ red_CM_alerts_ALL
	# CM cases for all AC≥ red_CM_cases_ALL
	# CD alerts for all AC≥ red_CD_alerts_ALL
	# CD cases for all AC≥ red_CD_cases_ALL
	# CL cases for all AC≥ red_CL_cases_ALL

Table 4. (Continued)

Conditions	Single alerts and their thresholds
● **"yellow":** when all the numbers of alerts/cases in the time window *W* **are lower than the respective red threshold but at least one of them is not less than the respective yellow threshold**	red_SP_very_low > #very low score speaker alerts≥ yellow_SP_very_low
	red_CD_alerts_AC> # CD alerts per AC≥ yellow_CD_alerts_AC
	red_CD_cases_AC> # CD cases per AC≥ yellow_CD_cases_AC
	red_CM_alerts_AC> # CM alerts per AC≥ yellow_CM_alerts_AC
	red_CM_cases_AC> # CM cases per AC≥ yellow_CM_cases_AC
	red_CL_cases_AC> # CL cases per AC≥ yellow_CL_cases_AC
	red_CM_alerts_ALL> # CM alerts for all AC≥ yellow_CM_alerts_ALL
	red_CM_cases_ALL> # CM cases for all AC≥ yellow_CM_cases_ALL
	red_CD_alerts_ALL> # CD alerts for all AC≥ yellow_CD_alerts_ALL
	red_CD_cases_ALL> # CD cases for all AC≥ yellow_CD_cases_ALL
	red_CL_cases_ALL> # CL cases for all AC≥ yellow_CL_cases_ALL
● **"green":** when all the numbers of alerts/cases in the time window *W* **are lower than the respective yellow threshold**	yellow_SP_very_low > # very low score speaker alerts
	yellow_CD_alerts_AC > # CD alerts per AC
	yellow_CD_cases_AC > # CD cases per AC
	yellow_CM_alerts_AC > # CM alerts per AC
	yellow_CM_cases_AC > # CM cases per AC
	yellow_CL_cases_AC > # CL cases per AC
	yellow_CM_alerts_ALL > # CM alerts for all AC
	yellow_CM_cases_ALL > # CM cases for all AC
	yellow_CD_alerts_ALL > # CD alerts for all AC
	yellow_CD_cases_ALL> # CD cases for all AC
	yellow_CL_cases_ALL> # CL cases for all AC

Based on the conditions summarized in the left column of Table 4, TraMICS evaluates the current security situation and provides the corresponding security situations indicator to the human operator.

5. User interface

TraMICS' alerts and the security situation indicator are shown to the ATCO as depicted in Fig. 6 using the Traffic View HMI (Human Machine Interface). The safety related alerts detected by TraMICS are flight specific and will be shown in the labels of the specific flights. All entries in the Global Alert List are security related. This differentiation is necessary and may confuse on the first glimpse as e.g. the security situation indicator stays green even if there is a severe conflict of two aircraft (and no other alerts are found). On the other hand, the security situation indicator might be red even if there are no safety alerts shown in any label. This will happen when e.g. an unauthorized speaker is detected or the triggering number of safety alerts has exceeded a threshold in the considered time window *W*, but are already solved. Summing up, the current security situation indicator should not be used to draw conclusions about the current safety situation and vice versa.

The security situations indicator starts always with a green, yellow or red dot, all other alerts do not have any color-coding. Each alert is followed by the timestamp of its occurrence or re-occurrence. No alert will disappear automatically but have to be actively dismissed by the ATCO. The Global Alerts lists holds the latest information on the top.

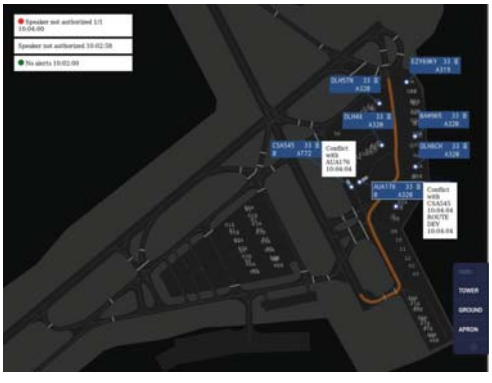

Fig. 6. TraMICS alerts on the Traffic View HMI. The Global Alerts List in the upper left corner.

The presentation of TraMICS results to the SOC operator is up to other tools (SATIE Project 2021). TraMICS sends as well the security situation indicator (which is processed/interpreted data) as well as the single

alert messages (which is raw data) according to the ontology developed by SATIE (SATIE Project 2020).

6. Conclusions and Outlook

The TraMICS' modules were built to detect different kinds of safety and security indications and a new method to correlate them to a security situation indicator is described. TraMICS results are shown on the CWP and send to the SATIE Correlation Engine. The tool is verified and ready for validation. To validate the TraMICS and get ATCOs feedback, human-in-the-loop experiments in an air traffic simulation facility are needed, which would require many people at one location. This has not been achieved yet due to the COVID-19 pandemic impact and the resulting partners' strong protection policies for their employees and potential validation participants. The SOC operator's feedback will be tracked and analyzed during the remote SATIE simulation trials scheduled in April 2021. In contrast to TraMICS, the other SATIE detection systems do not require human-in-the-loop simulations and are integrated on a virtual simulation platform. Pre-recorded TraMICS messages will be sent to Correlation Engine in this virtual platform to contribute to a complex attack scenario the operator is exposed to.

Acknowledgements

This paper is based on the SATIE project's deliverable D4.2 - Traffic Management Intrusion and Compliance System (SATIE Project 2021). The SATIE project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein. For more information on the SATIE project see: http://satie-h2020.eu/.

References

AP. 01 29, 2021. https://apnews.com/article/arrests-berlin-f56833f73c7ecfa34a5ed5e6461669bc (accessed 02 15, 2021).

Epel, Elissa S, et al. "More than a feeling: A unified view of stress measurement for population science." *Frontiers in neuroendocrinology* 49 (2018): 146-169.

EUROCONTROL. "EUROCONTROL Specification for Advanced-Surface Movement Guidance and Control System (A-SMGCS) Services." 2018.

Kenny, Patrick, Themos Stafylakis, Pierre Ouellet, Md. Jahangir Alam, and Pierre Dumouchel. "PLDA for speaker verification with utterances of arbitrary duration." *Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing*. Vancouver, BC, Canada: IEEE, 2013. 7649-7653.

Lazarus, R. S. "From psychological stress to the emotions: a history of changing outlooks. Personality, critical concepts." *Annual review of psychology* 44, no. 1 (1993): 4-179.

Russell, J. A. "A circumplex model of affect." *Journal of Personality and Social Psychology* 39, no. 6 (1980): 1161–1178.

Sabo, R, et al. "StressDat - Database of speech under stress in Slovak." *submitted to Jazykovedný časopis, (SLOVKO 2021: 11th International Conference)*, 2021.

SATIE Project. *D4.1 - Specification of data exchanges, interfaces and log semantic.* Project deliverable, https://cordis.europa.eu/project/id/832969/results, 2020.

SATIE Project. *D4.2 - Traffic Management Intrusion and Compliance System.* Project deliverable, submitted to https://cordis.europa.eu/project/id/832969/results, 2021.

SATIE Project. *D7.2 - Training handbook.* Project deliverable, in preparation for https://cordis.europa.eu/project/id/832969/results, 2021.

Snyder, David, Daniel Garcia-Romero, Gregory Sell, Daniel Povey, and Sanjeev Khudanpur. "X-Vectors: Robust DNN Embeddings for Speaker Recognition." *Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP)*,. Calgary: IEEE, 2018. 5329-5333.

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