SATIE NEWSLETTER

SEPTEMBER 2021 ISSUE 3

INSIDE THE ISSUE

PROJECT CONTACT

Tim H. Stelkens-Kobsch
communication-satie@dlr.de

ONLINE LINKS

Twitter
SatieH2020

LinkedIn
showcase/satie-h2020

Website
satie-h2020.eu

Foreword

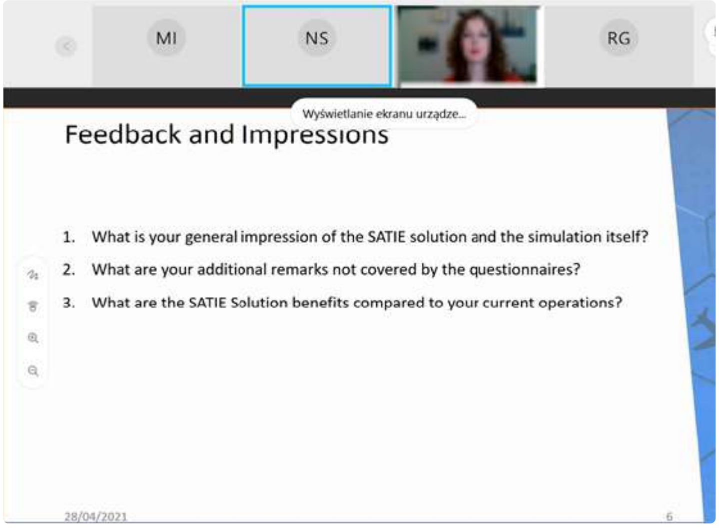
By Tim H. Stelkens-Kobsch, DLR, SATIE Project Coordinator

With the project entering its final stage, the third issue of the SATIE newsletter focuses on reporting the recent advances the consortium has made towards verifying, validating, and demonstrating the SATIE Solution.

Thus, this newsletter opens with the article on Simulation Validations, which took place between April 23rd and 28th, 2021. With the help of multiple airport professionals, the event successfully validated and verified the SATIE Toolkit on the dedicated simulation platform, using five cyber-physical threat scenarios.
The Simulation Validations were an important step towards the final SATIE demonstrations which were planned to take place in airport environments. Following this, I am pleased to inform you, that the first of three SATIE demonstrations was carried out on the 11th of June, 2021 at the Athens International Airport (AIA) premises, whereas the second SATIE demonstration was conducted on the night of the 27th of July, 2021 at Zagreb International Airport. The events were a success. Both, operational experts trained to use the novel SATIE systems and security experts observing the demonstration evaluated the SATIE Solution very positively. In this newsletter we report on the Athens demonstration, while the Zagreb demonstration will be in the focus of the next issue.

All of the above would not have been possible without adhering to the highest ethical standards for the development of technologies within SATIE. As such, we also take opportunity in this newsletter to highlight some of the work done by SATIE legal experts. In the final months, the SATIE team plans a series of events to demonstrate all major outcomes of the SATIE project. As such, I also take the opportunity to welcome users, stakeholders, and security experts to engage actively with the project. As always, I hope this newsletter will further stimulate your interest in SATIE.

Simulation Validations



Feedback and Impressions

1. What is your general impression of the SATIE solution and the simulation itself?
2. What are your additional remarks not covered by the questionnaires?
3. What are the SATIE Solution benefits compared to your current operations?

28/04/2021 6

Figure 1: Partners from DGS leading the session to gather feedback during Simulation Validations

Scan the QR code to view video one of the SATIE scenarios used in Simulation Validations

The SATIE Simulation Validations took place between Friday, April 23rd and Wednesday, April 28th 2021, as a remote event. The purpose of the events was to validate and verify the SATIE Toolkit on the dedicated simulation platform, using five cyber-physical threat scenarios. These threat scenarios were fine-tuned to be feasible, realistic, and complex as well as to include both physical and cyber-attacks on airports, which are known as critical infrastructures. Such attacks could be performed by an attacker to cause serious damage to the airport operations and human lives. The complex attacks developed had to be feasible based on the involved airport systems as well as any technical constraints from the included tools. Therefore, tailoring of the attacks was done throughout the project before the validation could take place. In the end, these customized cyber-physical threat scenarios were used to simulate such attacks at airports. Invited airport operators used the SATIE Toolkit within the simulations to determine how well the SATIE Toolkit meets their security needs and expectations.

The event was attended by 15 airport professionals in total - including persons with experience in Security Operation Centres (SOC), Airport Operation Centres (AOC) and as police officers - from three European airports (Athens, Zagreb, and Milan). In Human-in-the-Loop (HITL) simulations, the participants were confronted with the threat scenarios, during which they had to use the SATIE Toolkit to combat the attacks. The operators were instructed to use the SATIE Toolkit just like a common airport security system in order to understand what attacks are happening, which assets are impacted, and for practicing the initiation of necessary mitigation procedures as well as informing first responders. The airport practitioners were provided with adequate training materials (the SATIE training handbook, deliverable D7.2) and the event was preceded by training sessions to teach them how to use the SATIE Toolkit. This was achieved through full-day remote trainings with the tool developers. In the time leading up to the conduction of the Simulation Validations, security practitioners were given free access to the simulation platform through a user-friendly web portal. This allowed them to practice using the SATIE Toolkit and to become proficient with it before the validation. During the event, the SATIE Toolkit was validated regarding its acceptance, usability, usefulness, and trust aspects to meet the needs of physical and cyber-security operators (see Figure 1). This was supported by a comprehensive questionnaire. The preliminary analysis of the practitioners' feedback shows a very positive reaction to the unified SATIE Toolkit as well as the individual tools, therefore indicating that all tools were fit for purpose. The participants especially perceive the SATIE Toolkit as a significant improvement compared to their current system, enabling a faster detection of and response to both physical and cyber threats. They also find the correlated cyber-physical alerts generated by the Correlation Engine to be of added value and highly relevant. At the same time, areas for improvement – like a better integration with existing airport systems – were highlighted. Additionally, performance data are currently analysed to calculate objective values for detection and reaction times. The Simulation Validations were an important step towards the final SATIE demonstrations which take place in airport environments. The feedback gathered from the Simulation Validations was used to further refine the SATIE Toolkit for the demonstrations at the three airports.

Demonstration in Athens International Airport

The first of three SATIE demonstrations was carried out on the 11th of June, 2021 at the Athens International Airport (AIA) premises in Spata, Attica, Greece (see Figure 2). It was a hybrid – i.e. both virtual and physical – event. The main objective of the SATIE demonstration at Athens Airport was to communicate the SATIE Solution, present its functionalities and illustrate how it is capable of preventing, detecting, responding and mitigating threats in a holistic manner.

Demonstration operations in Greece were organized and coordinated by Athens International Airport with the active involvement and technical support of all the partners (see Figure 3). In this context several training seminars and workshops were organized with operators to try the system and services, and to be trained on the proposed SATIE Solution. During the demonstration event at Athens Airport, the trained Security Operations Centre (SOC – see Figure 4) and Airport Operations Centre (AOC) operators used and validated the SATIE Solution through the deployment of two realistic cyber and physical attack scenarios:

- Scenario #1: “Cyber-physical attack targeting passengers’ security”;
- Scenario #2: “Cyber-physical attack at airport targeting Automated Border Control Gates, Access Control and Public Announcement Systems”.

SATIE Tools involved in the Athens demonstration scenarios included Malware Analyser, Incident Management Portal (IMP), Anomaly Detection on Passenger Records (ADPR), Unified Access Control (UAC), Impact Propagation Simulation (IPS)

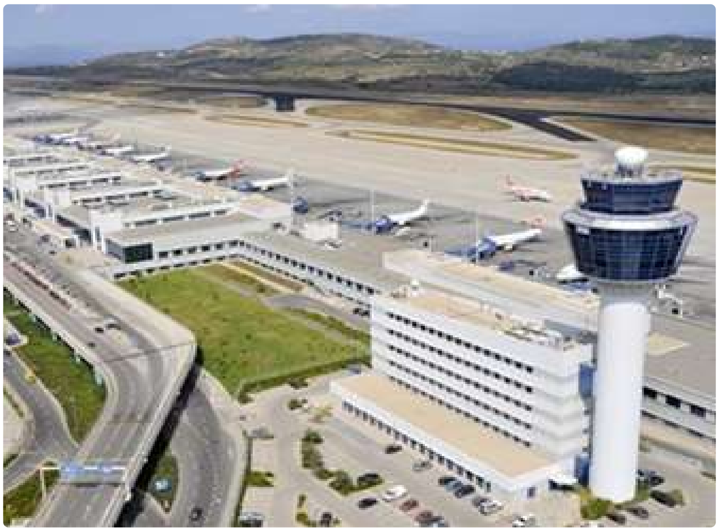


Figure 2: The Athens Airport premises

Figure 3: SATIE project partners’ representatives in the Athens Airport demonstration event

Crisis Alerting System (CAS), Investigation Tool (SMS-I) and Risk Assessment Platform (RIS).

The demonstration event was attended by over 60 participants. Due to the COVID-19 measures and travel restrictions, the audience attended virtually. The hybrid-based demonstration took advantage of the online broadcasting and interactive process (see Figure 5).

The online questionnaires provided during the demonstration event contained an adapted subset of the ones presented to the simulation validation participants. This offered the opportunity to compare the results of the demonstration and simulation validation activities. The responses received were similar. Both, operational experts trained to use the novel SATIE Tools, and security experts just observing the demonstration attack scenarios and the actions of SATIE system operators, evaluated the SATIE Solution very positively.

In conclusion, the similarities of answers and the positive feedback in the different groups of participants are an encouraging reinforcement of the SATIE Solution benefits. In addition, at the end of the event, interviews were conducted with (a) the employed SOC operators to testify their overall experience of the SATIE Solution during the pilot and (b) the project technical partners to gather the added value of the SATIE Solution towards airport's security operations.

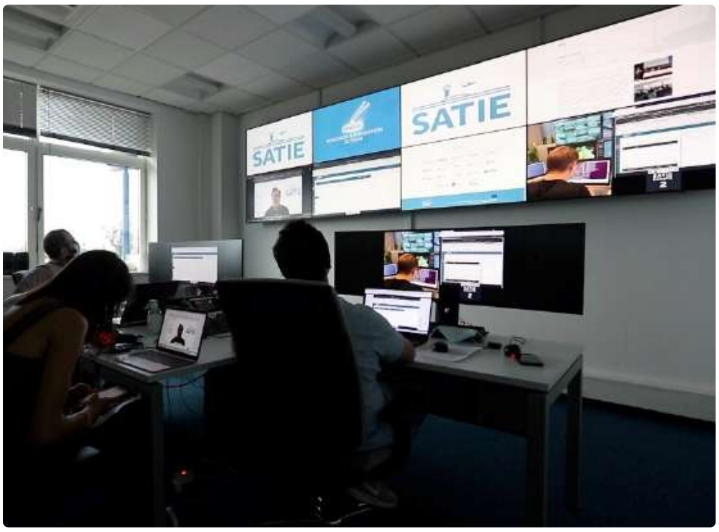


Figure 4: The Security Operations Centre (SOC) activities during the Athens Airport demonstration event

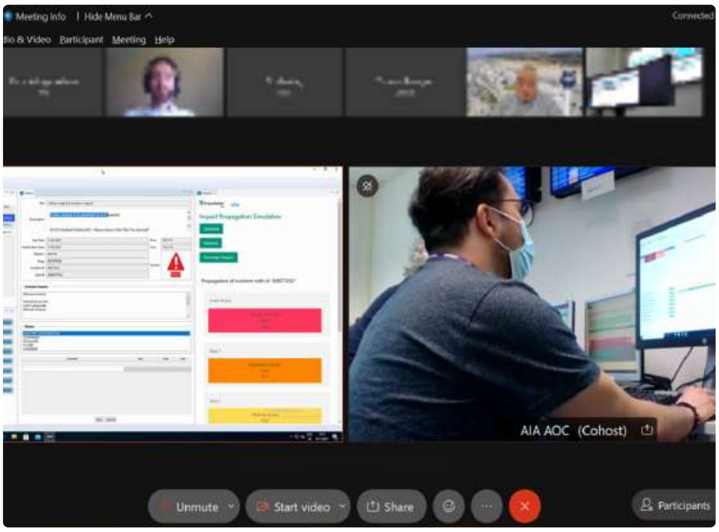


Figure 5: Screenshot from the virtual performance of the Athens Airport demonstration event during the scenario´s execution, showing the AOC activities

SATIE Work Package eight (WP8) Summary

WP8 spans over the whole length of the project and is divided into several tasks. The first task consisted in carrying out a legal state of the art on privacy and cybersecurity, to establish the requirements and principles that SATIE should follow. Human rights, data protection and cybersecurity standards were analysed, and two national case studies were examined. Based on these, recommendations were made to the consortium both in terms of the system and validation activities. The second task consists of operationalizing the data protection and privacy by design requirements into recommendations. Thus, an Ethics Briefing Pack was created for the consortium, aimed at explaining ethical requirements in research activities and how to apply them in SATIE. Aiming to provide an ethical standard for the development of technologies within SATIE, WP8 has provided a guide consisting of the operationalization of the privacy by design principles. This guide considers the individual data life cycle of subcomponents, carries out an impact assessment and determines potential risks that would undermine privacy by design principles. WP8 has been working closely with other tasks and work packages, especially those involving the scenarios and demonstrations, providing consent forms and information sheets making sure that the work in SATIE remains compliant with privacy and data protection regulations wherever external and internal participants are involved. In this context, a GDPR checklist has been provided to be used as part of the demonstration assessments and to update the progress and applications of the technologies being developed.

To this end, a series of online workshops have been organised providing partners with the necessary tools to fill in the checklist as well as input updates on how the privacy by design recommendations have been applied to the systems and subsystems. All of this will be incorporated in the last WP8 task which is about societal impact assessment. This will cover results and potential changes that have occurred during the project and which could affect its social desirability.

As part of the WP8 responsibilities an Ethics Advisory Board (EAB) was organized with experts in the ethics and security fields. The EAB held an internal meeting focusing on the review and comments of the WP8 deliverables, and advisors were provided with all the necessary documents in order to analyse the work done so far in regards to data privacy and GDPR compliance. The EAB also held a meeting with SATIE WP leaders, end users and tool developers where they were able to better assess the integration of the ethical and Privacy by Design recommendations into the SATIE Tools. Following these meetings the EAB and SATIE partners agreed that the taken measures assure compliance to ethical standards.

Partner Profile – ITTI

ITTI is a SME IT company providing software solutions for the companies and institutions in Poland and in other countries. The company has been operating since 1996 and is located in Poznan, Poland. Currently, ITTI has a team consisting of ca. 90 persons.

The main goal of ITTI is to develop and provide innovative applications and dedicated software solutions which are adjusted to customer needs, e.g. systems supporting management of warehouses and production process, solutions for crisis management and telemedicine, as well as systems supporting space situational awareness and space missions. ITTI has over 15 years of experience in international R&D projects that have been done in the following programmes: Horizon 2020 (formerly also FP7, FP6 and FP5), European Defence Agency (EDA) programmes (e.g. Joint Investment Programme on Force Protection, Joint Investment Programme on CBRN) as well as Action Grant CIPS II and NATO Industrial Advisory Group

iTTi

100
EMPLOYEES

25
YEARS OF EXPERIENCE

850
PROJECTS

2
OFFICES

studies. The company has also been active in Polish applied research projects co-funded by industry and the Polish Ministry of Science and Higher Education or National Centre of Research and Development. Moreover, ITTI collaborates with such organisations as European Space Agency (ESA) and European Union Agency for Cybersecurity (ENISA). In R&D activities the company cooperates closely with numerous universities and research institutes based in Poland as well as around Europe. Main competences and experience of ITTI cover such areas as: software development, communication networks (including PPDR and 5G networks), cybersecurity, crisis management (decision support and simulations), critical infrastructure protection, sensor systems, and internet of things. ITTI is an institutional member of the Public Safety Communication Europe (PSCE) Forum, Integrated Mission Group for Security (IMG-S), and NetWorld2020 SME Working Group. ITTI is also one of the co-founders of Polish Space Industry Association. In the recent years ITTI was several times awarded with the prestigious "Cristal Brussels Prize" for being the most active and successful Polish company participating in EC FP programmes.

THE 3S CLUSTERING EVENT

COMBINED WITH SATIE'S AND SECUREGAS'S FINAL CONFERENCE

HERALKLION / GREECE + ONLINE
12-13th OCTOBER 2021

Disclaimer: This 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.