Chapter 4

Data Visualisation for Situational Awareness in Industrial Critical Infrastructure: An InfraStress Case Study

By Giuseppe Cammarata, Gabriele Giunta, Lorenzo F. Sutton, Riccardo Orizio, Thu Le Pham, Stefano Sebastio, Piotr Sobonski, Jack Boyd, Filippo Leddi and Carina Pamminger

DOI: 10.1561/9781680838237.ch4

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security* by John Soldatos, Isabel Praça and Aleksandar Jovanović (eds.). 2021. ISBN 978-1-68083-822-0. E-ISBN 978-1-68083-823-7.

Suggested citation: Giuseppe Cammarata, Gabriele Giunta, Lorenzo F. Sutton, Riccardo Orizio, Thu Le Pham, Stefano Sebastio, Piotr Sobonski, Jack Boyd, Filippo Leddi and Carina Pamminger. 2021. "Data Visualisation for Situational Awareness in Industrial Critical Infrastructure: An InfraStress Case Study" in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security*. Edited by John Soldatos, Isabel Praça and Aleksandar Jovanović. pp. 84–106. Now Publishers. DOI: 10.1561/9781680838237.ch4.

now
the essence of knowledge

In this chapter, challenges and approaches for effective Data Visualisation aimed at enhancing Situational Awareness in Sensitive Industrial Sites and Plants (SIPS) Critical Infrastructure are discussed. In the H2020 InfraStress project a set of specific visualisation tools and dashboards have been developed for SIPS, including for real-time events monitoring and augmented reality. These tools have been integrated in a unified environment and with a set of other Cyber-Physical security solutions, aimed at collecting and presenting visually relevant data to users. The dashboards have been tested within the Piloting activities of the InfraStress project. In particular, in the pilot carried out at the De Puy Synthes site in Ireland (DPS), cyber-physical visualization was an important asset to enable operators to gain knowledge on the detected threats as well as to receive advanced mitigation and

reaction strategies and therefore improve the site resilience. In the first part the general dashboard architecture and core visualisation items (and related paradigms) are discussed as well as specifics about the DPS pilot deployment and its interactions with other InfraStress components. The Second part elaborates on deployment experience that is critical in successful operation and critical site infrastructure supervision from the Cyber Physical Systems threats perspective. Finally, main user feedback and conclusions from the InfraStress pilot activities will be presented in particular about enhanced site resilience.

4.1 Introduction

Sensitive Industrial Plants and Sites (SIPS) operators are in charge of complex Cyber-Physical Systems (CPSs) management. The increased interconnections between the cyber and the physical worlds open up to new attack vectors that can lead to safety and security issues. Therefore, SIPS must be adequately protected against adversaries throughout their entire lifecycle. To this end, operators need to have a deep awareness of the current situation in order to be able to adequately address potential issues and threats in a timely manner. The system complexity also prompts for the adoption of assisted automatic mitigation and remediation strategies triggered by the detected anomalies. Detecting early symptoms of deviations from the expected behaviour for SIPS may speed up the incident response process and mitigate more serious consequences on the safety and security. However, obtaining a full understanding of the situation may be challenging, given the complexity of CPSs and the ever-changing threat landscape. In particular, CPSs typically need to be continuously operational. The cyber and physical worlds are often deeply intertwined, operate on different spatial and temporal scales, exhibit multiple and distinct behavioural modalities, and interact with each other in ways that change with context. In order to ensure an accurate identification of attacks, it is very important that the security tools correlate the possible detection events generated in cyber and physical spaces and that such a knowledge is represented to safety and security operators in a clear, effective and timely manner. In this chapter, we illustrate a set of specific visualisation tools and dashboards integrated in a unified environment, including augmented reality, which aim at enhancing Situational Awareness in SIPS Critical Infrastructure. Specifically, the data visualisation fundamentals are presented in Section 4.2 through a visual analytics and augmented reality approach. Moreover, two approaches on how to integrate data and visual analytics into the InfraStress Global Dashboard are reported in Section 4.3. The De Puy Synthes site in Ireland (DPS) is illustrated in Section 4.4 as case study for cyber-physical visualization. Finally, conclusions and future outlook are in Section 4.5.

4.2 Visualisation Tools and Paradigms for Situational Awareness

4.2.1 Dataflow and Data Analysis

The InfraStress framework is equipped with powerful data analysis components performing data processing, attack and anomaly detection, and mitigation decision support. Raw data are collected from various SIPS data sources (e.g., sensors, logs). The framework is constituted by a modular structure in which each component focuses on a specific dimension to develop a comprehensive Situational Awareness (SA) for SIPS. Four SA dimensions have been identified within the InfraStress framework, each with its specific goal and challenges: physical detection, cyber detection, and the combined complex attacks detection (i.e., it detects complex attack combining multiple detected threats from both the cyber and the physical space), and finally the reaction and mitigation engine. Analysis results are shared among components to extract and generate additional knowledge. Thanks to these detections, the SA is built, and a holistic view of the SIPS is provided. Whenever a complex attack is detected, the decision support component is triggered to provide the optimal strategy to mitigate the effects of the threat and to improve the overall resilience of SIPS. Threats detected by any component are presented through the visualization dashboard to the safety and security operators of the SIPS to support further interventions, if needed.

Physical threat detection: The machine learning-based Physical Security Information Management (PSIM) system provides physical threat detection capabilities. An example of physical threat detection tool designed and developed in InfraStress is constituted by the tailgating detector. It provides Access Control (AC) security capabilities to identify tailgating events in real time based on streaming access logs collected by the card reader network. Tailgating events in AC systems are not inherent to the placement of the card readers (whose locations can be optimized by other components designed also within the context of the InfraStress but not discussed here), but rather due to negligence of employees who are followed by an unauthorized person while entering in a restricted area.

The tailgating detection analysis tool works in two steps. In the first, a reachability graph describing the placement of the card readers is inferred through an evolutionary machine learning approach (if not provided in input e.g., in case of very large SIPS like in the DPS example discussed below). In the second, AC logs describing the paths followed by the employee are analyzed. If there is no link connecting two consecutive card readers reported on the AC logs, a tailgating event is detected. Such access logs are generated every time an employee (tries to) access to a restricted area (even within the same building) by swiping her/his badge to a

card reader. Among other information these logs contains timestamp, and identifiers for user and card reader.

Cyber threat detection: Building Management Systems (BMS) can be also the target of cyber-attacks. The cyber threat detection can detect and describe anomalies in real-time environmental sensor measurements (temperature, humidity, light, etc.). Such sensor measurement data constituting time series are analyzed to detect anomalous subsequences of observations representing hazardous events or malfunctioning of the sensors also by taking into account the contextual information (e.g., the external temperature collected from feeds of local public agencies). Anomalies are represented in the dashboard through real-time time series whose severity is represented through a colour scale (i.e., green, yellow, orange, red) according to the deviation from the normal behaviour.

Complex attack detection: It is responsible for identifying complex attacks affecting a Critical Infrastructure (CI) at any time throughout its standard operations. Complex attacks are characterized by a set of malicious events that often when analysed in isolation could not rise the attention up to an alert level. But when studied as an ensemble could reveal novel threats. In order to be effective, the complex attack detection component needs to have a broad overview of the CI and therefore it analyse heterogeneous information originated from components spread throughout the CI.

The complex attack detector leverages on attack trees defining types of attack (assessed by safety and security expert of the SIPS) and on the anomalies detected by other components deployed in the InfraStress framework (e.g., for cyber and physical events). This component aims at a multisensory data fusion through a complex event-based SIEM (Security Information and Event Management). Event streams related to context information and digital happenings are correlated to infer the threat level. This event processing is in charge of deducing in real-time warning situation deserving additional attention, triggering alarms and countermeasures. More specifically, complex attacks are modelled through a constraint network and used to identify the current state of the CI based on its internal representation and the detected anomalies.

Mitigation decision support: It provides an adaptive decision support service to safety and security managers whenever a (complex) attack is detected. During its decision-making process, the component will trigger the appropriate mitigation by taking into account the potential effects of the detected attack and the current status of the SIPS. In this way, the component can present instantaneously the new response and mitigation decisions based on changes in the environment.

In order to promptly react to unexpected events, it considers all the threat detectors for which one wants to apply an automatically generated optimal mitigation

strategy or receive suggestions on the possible remediation, for example physical trespassing, Wi-Fi attacks, SQL injection attacks. Additional examples in the case of a SIPS are provided in Section 4.4. while discussing the DPS pilot in InfraStress. The mitigation decision support service receives also as input an instance of the context ontology related to the topology and the status of CI. With this information, the mitigation decision support is in charge of: (i) identifying a high-level strategy which is able to mitigate the effect of the detected threat, (ii) computing an optimal medium-level strategy by considering the current status of assets of the attacked SIPS. The optimal mitigation strategy required to tackle the threat affecting the SIPS is generated from: current optimal mitigations threats and complex attack vision of the SIPS, current status of each asset and the potential impact of each mitigation action.

The output of the four components defined above are exchanged through the Kafka message broker and constitute the knowledge to build the situational awareness dashboard which includes also suggested actions according to deliberative/proactive/reactive approaches performed by the safety and security operators of the SIPS. Messages reported in the dashboard will include information about both numerical value and categorical anomaly score (namely, green for normal operation, and yellow/orange/red for threats of increasing risk) with the associated mitigation strategies applied.

4.2.2 Data Analytics and Visual Analytics

Data Analytics is a process of analysis on data sets in order to find trends and relationships with the aim of extracting useful information and knowledge from the same data. Data Analytics technologies and techniques are widely used in all sectors and in many different organizations to support decision makers. It is also used by scientists to verify or disprove scientific models, theories and hypotheses [1].

Data Analytics does not take into consideration specific cases, instead tries to apply algorithms to identify trends and possible solutions to the problem. This type of approach has its issues, since, most often, the best method leading to the solution of the very problem being addressed is not known to the user in advance. Therefore, the applied algorithm might not lead to the desired solution.

To address this challenge an approach can be to use the Visual Analytics. In this case, in the process of knowledge extraction is facilitated through the knowledge of an expert who supports data analysis. Within such approach, the Visual Analytics process should not be seen in contrast with Data Analytics, but, rather, as a tool, which integrated with Data Analytics, allowing the user to facilitate the analysis of data. Visual Analytics aims to synthesize the information coming from the

data, discover patterns within the data, provide timely assessments and effectively communicate such assessments [2].

As part of the analysis security and safety, Visual Analytics are used to study emergency situation and take the right countermeasures as well as to try and predict any catastrophic scenarios. Visual Analytics are also widely used in the field of IT security, since they are able to help identifying any anomalies in the data [3].

The graphical representation of a dataset makes it easy to understand them and their meaning; this means that the sharing of data, even to non-experts in the sector examined, is simplified. It is in fact possible to represent the data through different techniques, such as: graphs, infographics, lists or maps.

The process that starts from the data up to the visualization is usually described through a pipeline, created in Kibana [4] using the visualize tool, which allows you to create the appropriate graphs for browsing the InfraStress data present on Elasticsearch [5].

The main steps used to create a viewing pipeline are:

- **Data modelling:** the data, regardless of the source of origin, must be processed in such a way that important information such as: name, type, range and meaning of each attribute, are easily accessible and editable.
- **Data selection:** In this phase the user has the possibility, also through the support algorithms, to select a subset of data from the original set.
- **Data to visual mapping:** In this phase, the actual mapping of the data in the components that make-up the graphic representation takes place. This phase often involves filtering, sampling, interpolation or subsampling.
- **View transformation:** In this phase, the user has the ability to model the parameters of the view. In particular, it can manage the colours within the representation in such a way that they take on specific meanings.
- **Rendering:** It means the final rendering of the representation, in addition to showing the representation, additional elements are also inserted, such as axes, annotations, legends, etc.
- **Human component:** At the end of the rendering process, it is essential to remember that the information you want to convey must arrive clearly to anyone who approaches the observation of the representation. The user who makes use of the visualization must simultaneously observe the graph and process information through it. To facilitate this process, techniques are put into practice that exploit the use of preattentive attributes, i.e., elements within the representation that serve to direct attention to certain parts of the same representation, and which are based on the so-called Gestalt psychology. which instead introduces rules to facilitate the understanding of the representation. Data Visualization deals with finding representative techniques

for any type of data, in order to be able to carry out an analysis and an effective representation. In case you need to show numerical values, graphs are used.

4.2.3 Data Visualisation for SIPS Critical Infrastructure

Data Visualization is the main tool for Visual Analytics and refers to a set of techniques for graphically representing data and exploring them interactively. The aim is to determine a series of techniques that allow a graphical representation of datasets, which can be more or less extensive. This type of approach arises from the fact that, very often, it is necessary to examine large amounts of data in order to extract information and relationships between the data. The use of graphical representations allows users to: understand data, make predictions and share data.

Extracting information, directly analysing an entire collection of data, would be complex if not impossible. For this reason, some representation is used that can help to grasp their characteristics. The fundamental principle being that the synthesis capacity of an image is far superior to any other representation, and moreover, it tends to be processed more easily by the human brain. Data Visualization can also play an important role in predicting certain events. The analysis of a repetitive trend or of patterns in the data provides the possibility to investigate the causes and to be able to prevent an event before it happens.

The InfraStress Multidimensional Descriptive Analysis is defined as the transformation of raw data into a form that makes it easy to understand and interpret, rearrange, sort and manipulate to generate or highlight information that can be useful for decision makers within SIPS. More specifically, the descriptive analysis represents the starting point of the data analysis process. Therefore, the descriptive analysis aims to provide a set of historical data that can be used to extract knowledge and for further analysis.

This type of analysis is the simplest and most used, and aims to:

- View data in the right context.
- Identify relevant information in the data.

Extracting value from data requires tools and technologies suitable for this scope. The following Figure 4.1 shows the architectural draw of the module in its complex highlighting the main tools and technologies utilized in it.

In the InfraStress project, the ALIDA micro-services platform, develop by ENGINEERING R&D was adopted [6]. ALIDA offers a catalogue of Big Data Analytics (BDA) services for ingestion, preparation, analysis, visualization of data allowing to exploit their potential, in order to gain value. Furthermore, ALIDA

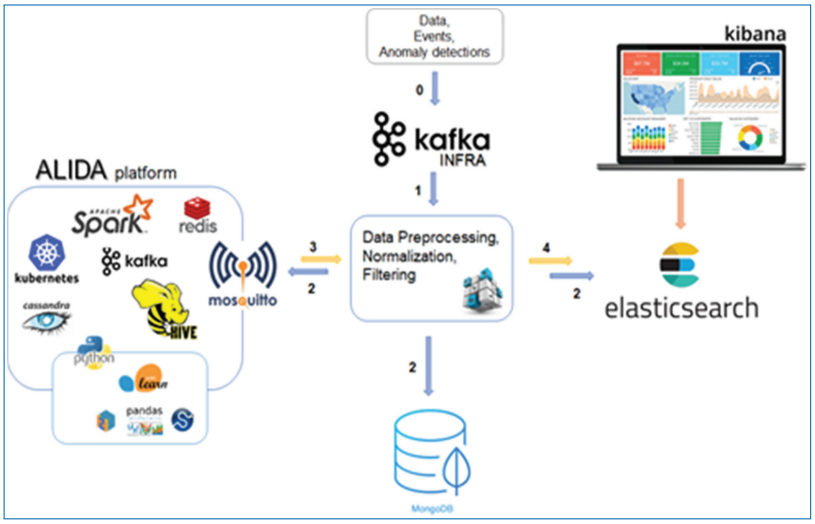

Figure 4.1. Schema of the InfraStress multidimensional descriptive analysis.

provides a catalogue of services useful for the management of applications that guide the user from data acquisition to results visualization. For the scopes of InfraStress a specific python service was implemented for processing data coming from the situational picture component and concerning the situational state of the SIPS. The results of this processing are historicized on Elasticsearch and are available through Kibana.

The data produced by situational picture component, before being historicized and sent to the ALIDA platform, needs to be pre-processed according to a data-preparation process, through which only the significant features are selected from the set of data and used for the elaboration of multidimensional analytics. The data flow shown in Figure 4.2 highlights how the data is manipulated before being displayed as graphs.

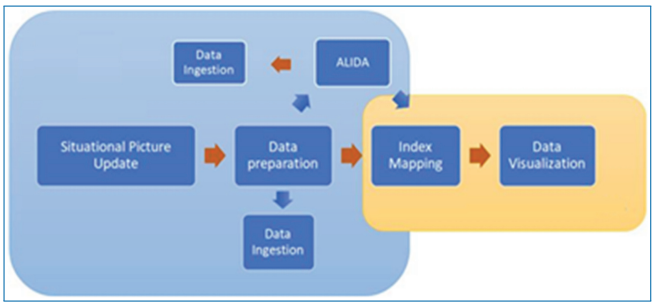

Figure 4.2. Diagram representing the process of creation and analysis of the descriptive analytics.

Once data have been selected and prepared, they must be presented to users in a suitable way. The selection of the best way to present data depends on the type of information that we want to communicate.

The identification of the graph to be used depends on the type of data. The data that can be represented in a graph can typically be divided into three categories: quantitative, qualitative, and temporal.

In the case of quantitative data, we want to represent numerical data, which in this case can be continuous or discrete. In case of categorical data, they represent categories and can be ordinal (low, medium, high) or non-ordinal (chemical, intrusion, fire). Finally, in case of temporal values, they can be represented as a discrete quantity (e.g., succession of temporal instants expressed in hours, days, months, years) or as a continuous quantity (e.g., considering a specific time interval), although the time is a continuous quantity. In Figure 4.3, a graphical representation of this classification is provided.

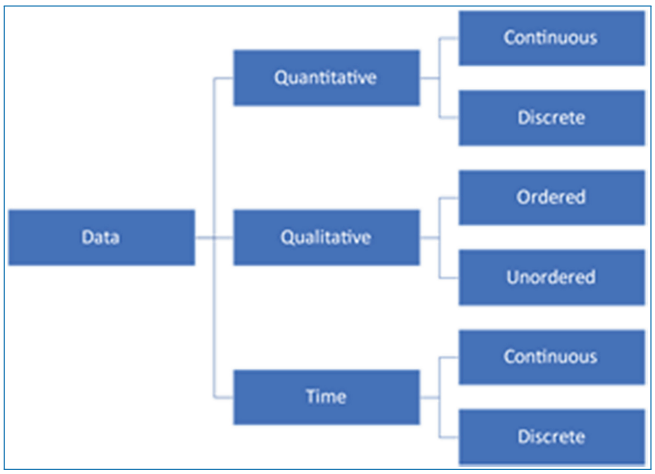

Figure 4.3. Categories of different type of data to be represented through a graph.

In the InfraStress, three groups of graphs for each class of information to represent, or features to highlight, have been selected. These groups include:

Graphs for Composition: This group includes any graph suitable to show composition of data. The following figure shows two examples of graphs belonging in this group, built in context of InfraStress.

Graphs for Distribution: This group includes any graph suitable to show the distribution of a dataset parameter against time (Time series) or space (Tile maps). The time series chart shown for each day of the considered interval, the amount of time the SIPS was in critical state (critical situation) and in which it persisted in each of the assigned severity levels. The tile map shown in following figure shows

Figure 4.4. Graphs for composition used in InfraStress (on the left a pie chart shows the percentages of events of specific category occurred in the SIPS. On the right, instead, the pie chart shows the percentage of time during which the SIPS situation has the specified severity level in respect to the considered time interval).

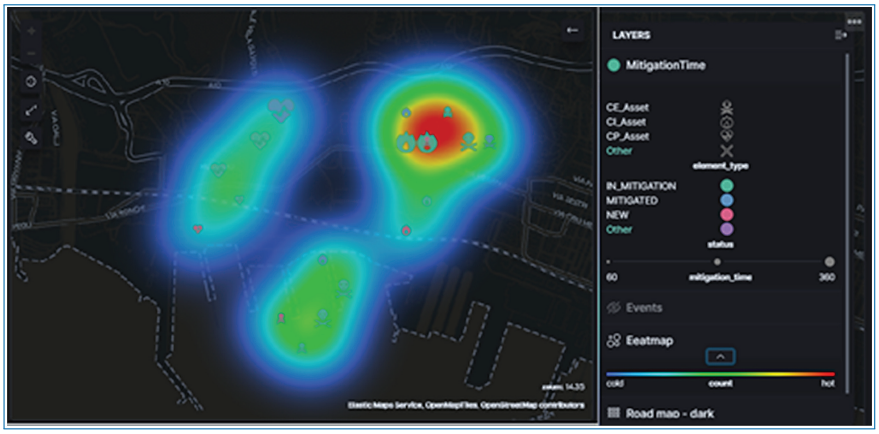

Figure 4.5. Heat map used in InfraStress for distribution.

georeferenced data about the infrastructure assets, differentiated by type of asset (shape of the symbol), by status of the latest event in which the asset was involved (colour of the symbol) and cumulative time needed to mitigate each event that has involved it (size of the symbol). The heat map layer highlights the zones where the identified events (heatmap) were concentrated.

Graphs for Comparison: Graphs belonging in this group are used to show comparisons among data. The heat map shown in the left part of the following figure, shows the total amount of time in which each event involving specific types of assets persisted in "Mitigated" or "In Mitigation" status. Instead, the heat map on the right side of the following figure, shown the number of events, included in the dataset (events occurred in a specific time interval), to which was assigned a specific severity level value, during its persistence in each of the event statuses.

Figure 4.6. Heat map used in InfraStress for comparison.

The bar chart is another type of chart that can be used to show a comparison among data. For instance, the one shown in the following figure was used in InfraStress to show the amount of time a mitigated SIPS situation persisted in critical and normal status.

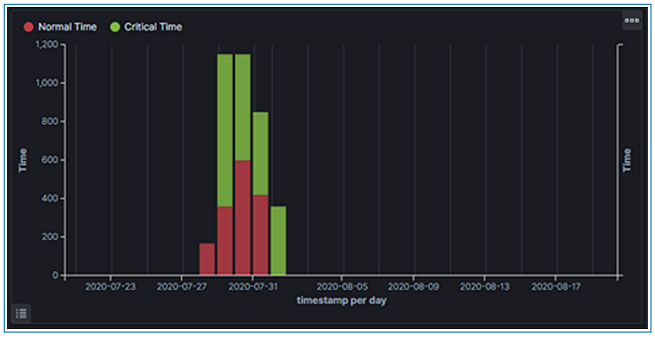

Figure 4.7. Bar chart used in InfraStress for comparison.

Finally, the Tag Cloud is another type of chart not included in the previous classification. This chart is used to provide an immediate perception of predominant values of a feature. In Figure 4.8, two examples of tag cloud charts implemented within InfraStress are shown, representing severity and criticality levels that prevail in situation occurred in the SIPS.

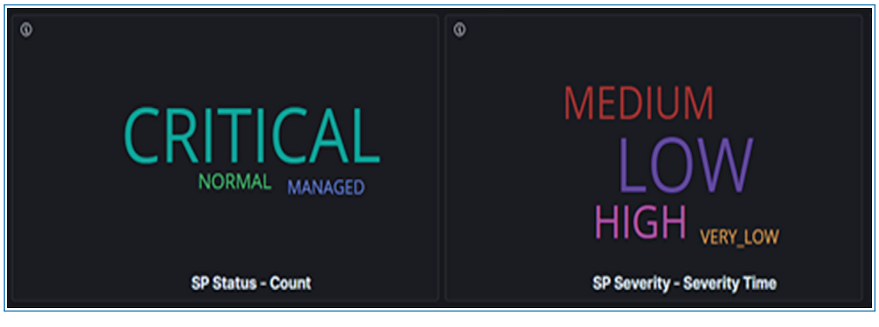

Figure 4.8. Tag cloud chart used in InfraStress for comparison.

4.2.4 Augmented Reality and Virtual Reality Technology for Data Visualisation

The past few decades have seen great technological advances in almost every field. Things are now possible that were originally thought of as science fiction. If there is any doubt about that, simply watching the documentary "How William Shatner Changed the World" can clarify this. However, up until recently, both worlds – digital and real – were strictly separated for most people.

To make this separation a thing of the past, great effort has been put into new technologies. Though the field appears to be relevant only since the 21st century, actually, the work started much earlier. In 1968 Ivan Sutherland bore the first fruits of this effort, when he completed The Sword of Damocles [7] – the first head mounted AR device [8]. The Sword of Damocles allowed the projection of a digital 3D cube into a room. As you can see in Figure 4.9, this was an impressive machine and the first step towards an integration of the digital into the real world.

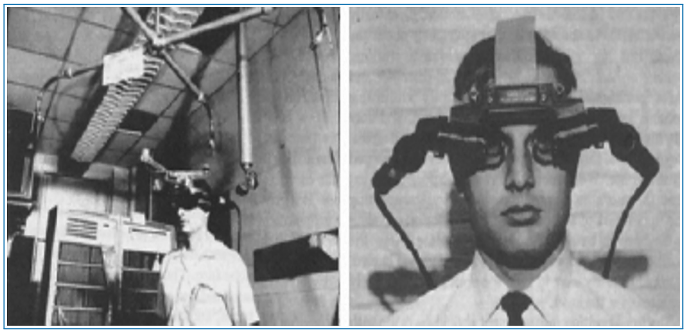

Figure 4.9. The Sword of Damocles created by Ivan Sutherland.

At that time, there was no clear separation between the different approaches. A complete immersion into the digital world was equated to the display of digital elements within a real world, i.e., room. This has, of course, changed over time and various forms of integration appeared. Paul Milgram and his colleagues, who published the paper "Augmented reality: a class of displays on the reality-virtuality continuum" [9] showed the most commonly used split between the methods.

As visible in Figure 4.10, which is an updated replica of Milgram's graph which also includes different types of AR interactions, there are plenty of methods to allow the merging of both worlds. Digital elements can be projected into the real world – similar to The Sword of Damocles – real world elements can be integrated into a virtual world, or an experience can be entirely virtual.

Though all methods and technologies are interesting, in InfraStress we focused on Augmented Reality (AR) and Virtual Reality (VR) applications for Situational Awareness purposes. In this context, a 2D dashboard can be enhanced with a 3D model display. The remote controller, using the HoloLens, can be at any location,

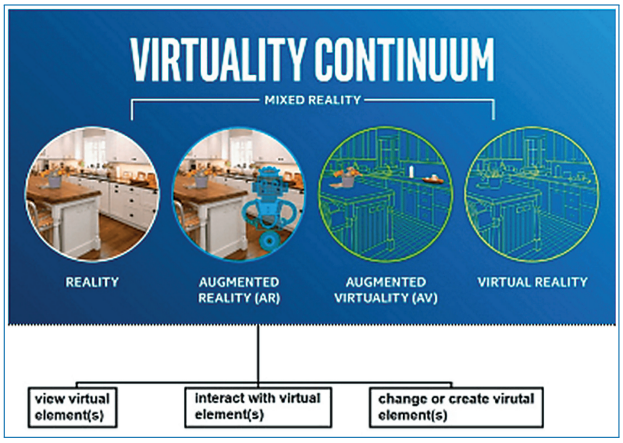

Figure 4.10. Reality-virtuality continuum.

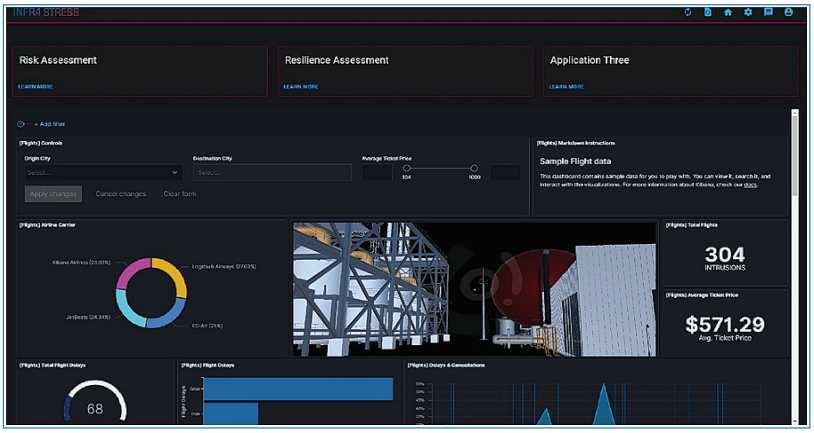

Figure 4.11. 3D model visualisation within the InfraStress Global Dashboard.

e.g. control room or in any other place at the SIPS. The flexibility comes through the video stream of the used AR or VR device. In case of emergency the remote controller can:

- establish a connection to the security feed and immediately view the precise location of the incidence at the site.
- investigate the surrounding area, to assess the risk of the incidence and communicate exit paths with agents on site.
- if available, the investigation can even be enhanced through a live video feed.

Figure 4.11 displays a possible 3D model dashboard extension. The extension is hosted in a cloud environment and used with a Mixed Reality (MR) device, for example HoloLens. It is designed to allow interaction with one or multiple 3D mesh

file(s), highlight areas and display the feed on the board. This extension allows the controllers to better analyse the impact of an incidence. A user can view a specific section of a building, cut through walls using spheres to view i.e. adjacent pipelines, or preview and share escape routes and much more. A user can view the model in bird-view or zoom into any level of the building. As mentioned, the 3D model can be interacted with and therefore will only display the relevant details.

In Figure 4.12 is shown a simulation of SIPS operators monitoring the security using AR/VR technologies.

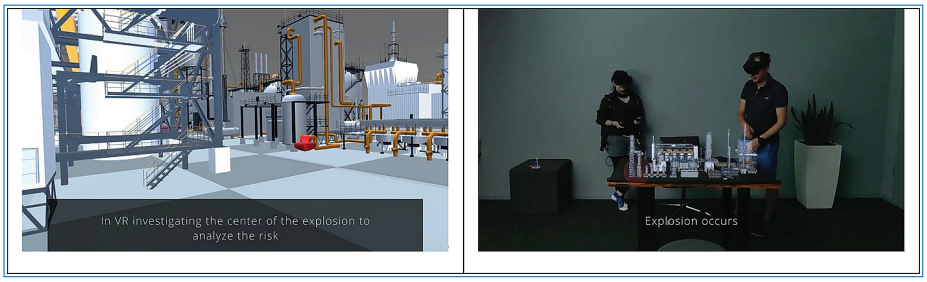

Figure 4.12. VR investigation displaying possible exit route (left); SIPS operators interacting with AR module (right).

4.3 InfraStress Global Dashboard

Dashboards created with Kibana can be easily shared and integrated in the InfraStress Global Dashboard. In the project, two modalities have been followed to integrate the visual analytics, described in 4.2.3, into the InfraStress Global Dashboard.

In the first modality, the individual panel of the data analytics is integrated as a set of independent sections called frames. Some of these frames will be displayed by default on the main page of the dashboard (Figure 4.13); others, instead, can be chosen by the user from a pre-set views (Figure 4.14) and added into the Global Dashboard clicking on button (Figure 4.15). The choice of the panels to be displayed will be decided a priori and personalized for each pilot.

In the second modality we integrate the full dashboard in the InfraStress Global Dashboard in a full screen mode (Figure 4.16).

In Figure 4.17 is shown a custom User Interface (UI) to represent the most important monitoring features for each detector component. Top left corner represents the asset inventory of the SIPS under monitoring e.g., sensors, access card readers and Internet of Things (IoT) devices. Clicking on each inventory asset leads to a separate view containing detailed information about its current status (an example will be shown in Section 4.4 while discussing the case of one of

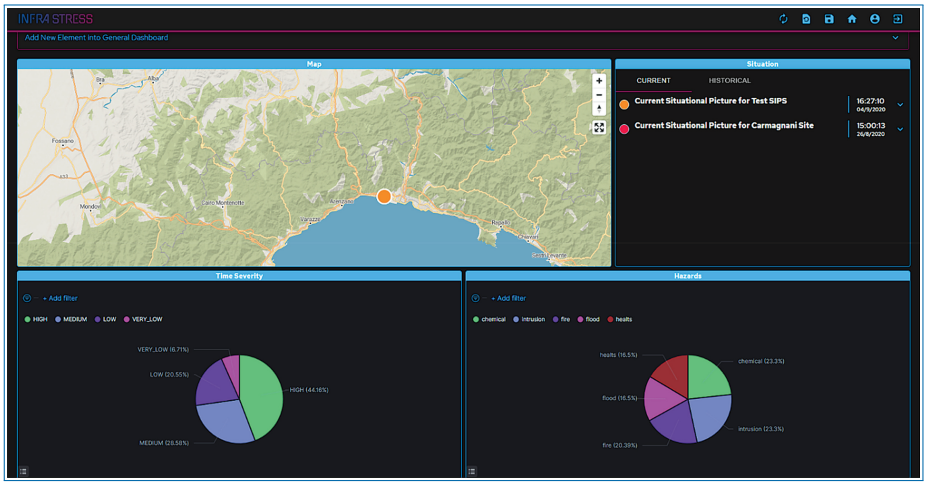

Figure 4.13. Default individual panel of MDA in the InfraStress Global Dashboard.

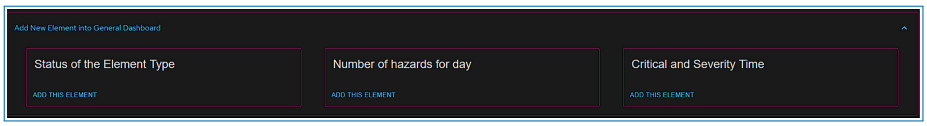

Figure 4.14. Example of pre-set views of individual panel of MDA.

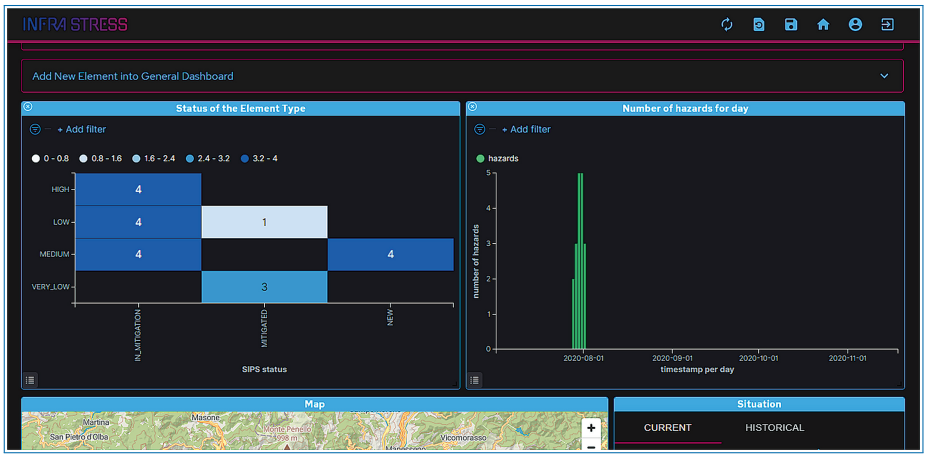

Figure 4.15. Select panels adding in the main page of the InfraStress Global Dashboard.

the InfraStress pilot). Top right panel shows the detections of complex attacks. Figure 4.17 represents the case of a (periodic) simulated attack (the red-line plot), whereas during normal operations this graph should be flat. The second row of panels illustrates the number of detected anomalies and their severity with respect to the SIPS status. The panel at the center of the dashboard illustrates the time series

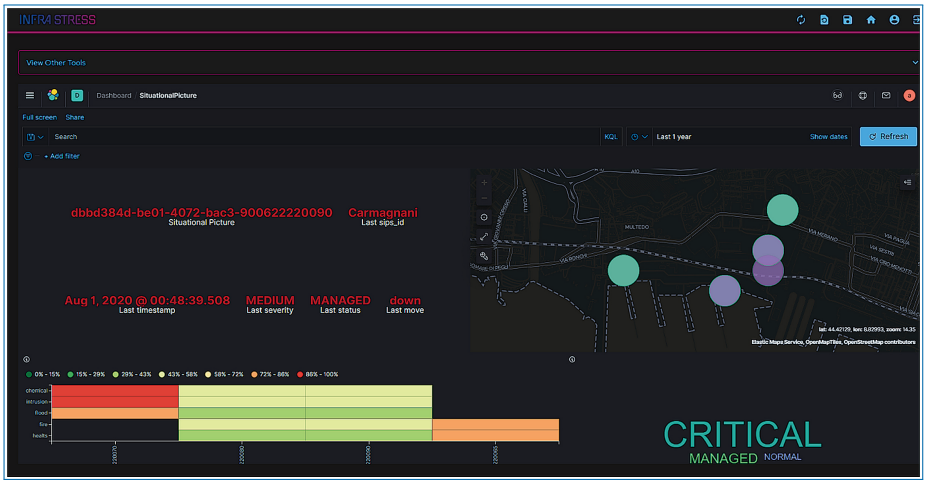

Figure 4.16. Full Dashboard.

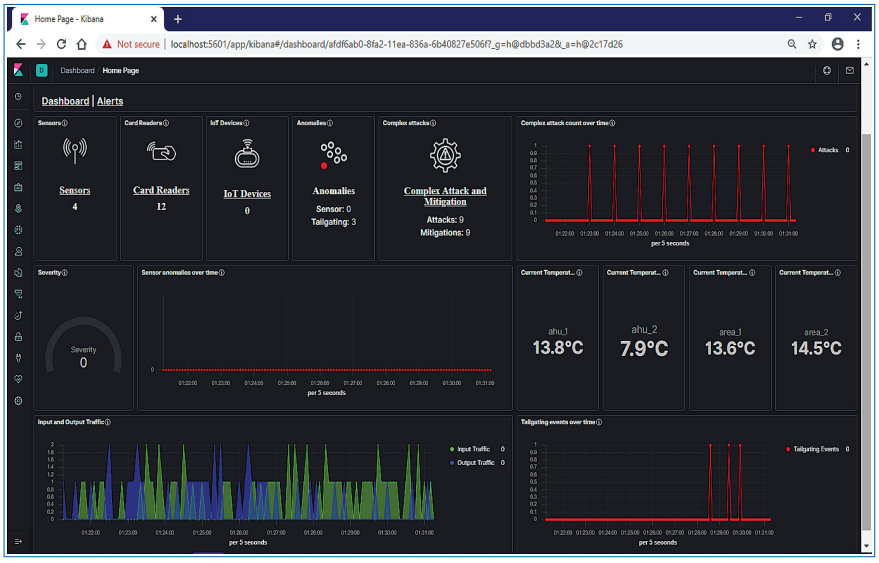

Figure 4.17. Situational awareness Dashboard – main view.

of physical anomaly detections over last 10 minutes. Most right middle panel shows temperatures read from supervisory control and data acquisition (SCADA) BMS. The last row is devoted to the AC and the card readers monitoring. The left panel displays incoming and outgoing traffic employees through the different restricted areas. In right panel, the tailgating detections are illustrated. More examples about the situational awareness dashboard are reported in the next section while discussing the DPS Pilot in InfraStress.

It is worth to highlight that the SA dashboard represented here constitutes only an example (tailored to the needs of one of the project pilots) of what can be obtained with technologies and data analytics developed in InfraStress. Indeed, the ELK stack allows a fast and easy customization of the dashboard.

4.4 The InfraStress Pilot Case: DePuy Synthes

DePuy Synthes (DPS) established its manufacturing facility in Cork (Ireland) in 1997 where it manufactures orthopedic knees and hips. The company has since expanded to include a Global Supply Chain Operation in 2002 and in 2008 DePuy established an Innovation Centre which was created to develop next generation orthopedic products and processes for a global market. In 2015 the Cork site carried out a €53.2 million expansion to open a new 320,000 square foot state-of-the-art facility (Building 2) similar in size to the existing facility (Building 1). This building primarily provides additional manufacturing capacity but also features a Medical Device Test Methods Center of Excellence laboratory to advance quality testing methods across the Johnson & Johnson (J&J) family of medical device companies, while also creating potential expansion opportunities for other J&J companies. Building 2 also houses DePuy's new 3D Printing Innovation Centre.

In InfraStress, this pilot showcases a heavily automated line involving AIV (Autonomous Intelligent Vehicles) robots, and advanced PSIM and BMS. By taking an effort in improve its performance and efficiency and the one the workforce operations, DPS is focusing on enlarging its fleet of AIV robots, and automatizing the physical access to the site (from the main barriers to the doorways around the line) and the control of the site through BMS solutions.

At DPS, the PSIM system has to deal with approximately 1000 employees, a large perimeter area (part of which open to the sea) and runs 24/7. The facility includes two building housing manufacturing spaces characterized by special heating, ventilation, and air conditioning (HVAC) systems and cleanrooms. The site is considered a Sensitive Industrial Plant (SIP) due to a number of dangerous industrial processes involving high voltage/temperature/pressure, and volatile and toxic chemicals. The proximity of other pharmaceutical plants exacerbates the hazards.

Given the sensitivity of the infrastructure, the plant is subjected to a potential set of both cyber and physical attacks, despite none of the ones described below has been registered in reality. On the physical side, being the site located on the shore, it could suffer from natural hazards (such as extreme weather, ocean tides). Moreover, its location opens to the possibility that the site's perimeter is reached by sea without using the road. In addition, due to a recent effort devoted to the reduction of the carbon footprint, DPS employees can reach the campus even through public

Figure 4.18. DPS J&J Site in Cork, Ireland.

transportations thanks to a few bus stops located close to the campus. This scenario eases the possibility for unauthorized people to reach the site and look for weakness in the surveillance systems.

On the cyber side, the DPS facilities exploit advanced information technology (IT) and operational technology (OT) for automating some manufacturing procedures from the perspective of Internet of Things (IoT). DPS performs a number of dangerous and highly complex processes. Attacks to those operations could cause damages to machineries and products or in the worst cases to the surrounding SIPS and environments. In the site there are also sensitive data and confidential product specification whose access is restricted only to personnel on a need-to-know basis. DPS already adopts advanced cyber security techniques to monitor its infrastructure. On the other hand, there are always new threats that hackers could try to exploit given the complexity of the infrastructure.

Physical threats: An intruder could potentially violate the DPS perimeter and access to the site with the aim of reaching critical assets by concealing herself with the regular employees. Moreover, given the large size of the site, the number of employees and the number of jobs carried out by contractors (e.g., for maintenance of some special equipment) it is not possible to identify easily the presence of an unknown people. DPS already has in place perimetral defense, video surveillance and access control systems.

Disloyal contractors or simply distracted employees can have an oversight and not respect the DPS security policies. In such circumstances a person with knowledge of critical parts of the manufacturing system could enter the zone of interest through the use of social engineering techniques (e.g., by performing tailgating) and

cause damages to the production processes. This can be done directly by destroying part of the production line (e.g., by machine misuse or by causing fire) or indirectly by injecting malicious code to machines of interest or network to have delayed effect and not to raise an immediate suspicious.

Cyber threats: DPS introduced new manufacturing lines supported by a number of automated solutions which include AIV and robot technologies working together. If on the one hand this opened the way for a future with more sophisticated and autonomous production lines, on the other hand the more pervasive adoption of IT/OT solutions potentially exposes the infrastructure to cyber and cyber physical attacks on the line.

Currently the cyber infrastructure of the production line is being heavily monitored through cyber-security solutions. Nevertheless, the fast pace at which new cyber threats are discovered suggests that monitoring and detecting early signs of compromise to the integrity of the cyber infrastructure or anomaly is a good security practice.

Cyber-Physical threats – Complex Attacks: Given the high degree of automation and the use of IT/OT in the site, accidental changes or malicious configurations to the supervisory control and data acquisition (SCADA) of the BMS controlling the temperature settings of the production area could bring to halt of the production and/or to product damage.

The attackers can work in a few steps: intrusion to the IT/OT of the site, lateral movement to area of interest (e.g., a specific production line) and control/tampering of the infrastructure. An adversary could get closer to the area of interests and reach the wireless infrastructure of the site through small and easy to hide devices (e.g., thanks to a drone). Then the attacker could gain remote control to inject attacks via Wi-Fi to intercept, analyze and inject malicious traffic to machines and robots.

Situational awareness and threat reaction: Given the complexity of the SIPS at DPS having at one's disposal a clear, meaningful and timely overview on the site status and potential threats covers a pivotal role in protecting the CI and to apply the optimal counter measures. According to the attack in progress, countermeasures could foresee halting the production of a specific line to avoid further damage, restarting to a previous known good and safe state the affected machines, or activating fire extinguishers, alarms or even the immediate call of the firefighters if appropriate (given the chemicals managed in the site).

The designed situational awareness dashboard is able to provide a compelling and real-time view on the status of the whole infrastructure, including the automatic mitigation actions undertaken. In the context of the InfraStress project it has been evaluated at the DPS pilot through a series of simulated cyber, physical and cyber-physical threats. Mitigation strategies have been presented to the safety and

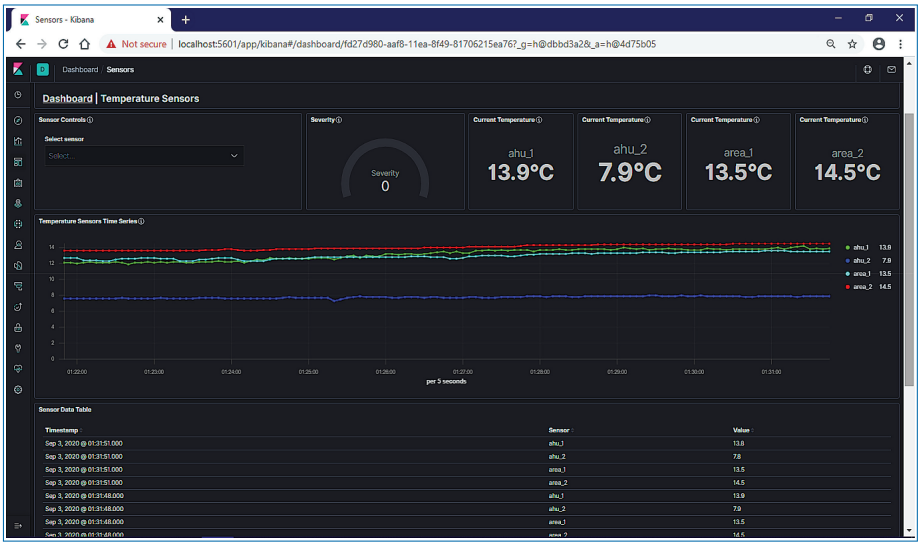

Figure 4.19. Situational awareness Dashboard – BMS view.

security operators of the site and evaluated with respect to promptness and correctness of the proposed solution. The following screenshots show how attacks and automatic mitigation actions are represented through the InfraStress dashboard.

Figure 4.19 illustrates the output monitoring of the BMS temperature sensors on the pilot site. Top right section represents current temperature measurements while below a 10 minute time series is displayed followed by a data table acquired from the Kafka broker. It is important to note that the top middle section of the BMS view includes a detection panel showing information about current anomaly detections being performed by the data analytic services.

Figure 4.20 shows the detection view of the PSIM component (some parts of the screenshot have been purposely blurred for confidentiality reasons). From there anomalies on the access to restricted areas of the buildings are reported. Number of incoming and outgoing employees for the area of interest are monitored in the top panel. On the right, the number of transactions per area is reported. The SIPS traffic of last 10 minutes is represented through two graphs: the number of tailgating detections is reported through a red line (left side), whereas the time series of incoming and outgoing total site traffic are in the panel at the right. The bottom part of the dashboard shows how the restricted areas are connected and the allowable transactions (the reachability graph discussed in Section 4.2.1). Raw datasets received in real-time by the Kafka broker are reported at the right-bottom of the dashboard.

The threat mitigation decision support system and policy enforcement view of the DPS Pilot is shown in Figure 4.21. Top elements display number of attacks

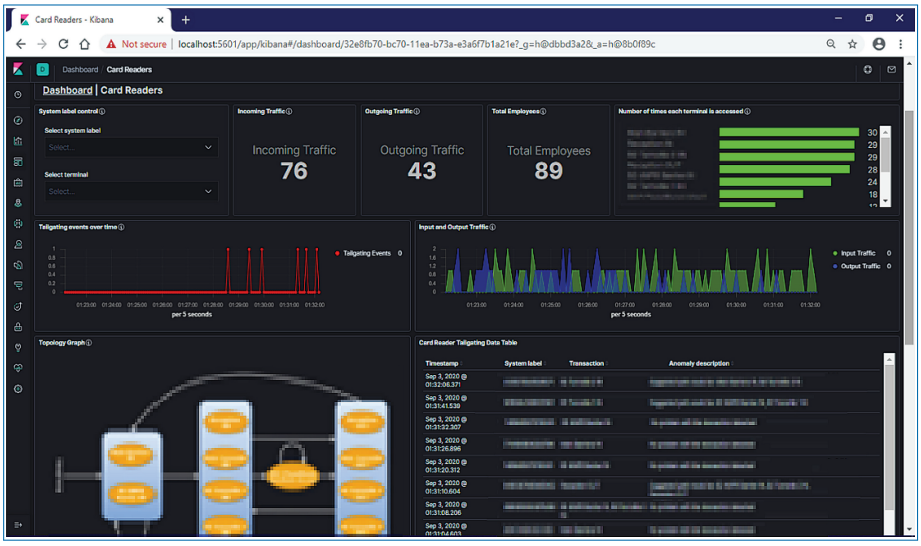

Figure 4.20. Situational awareness Dashboard – AC view.

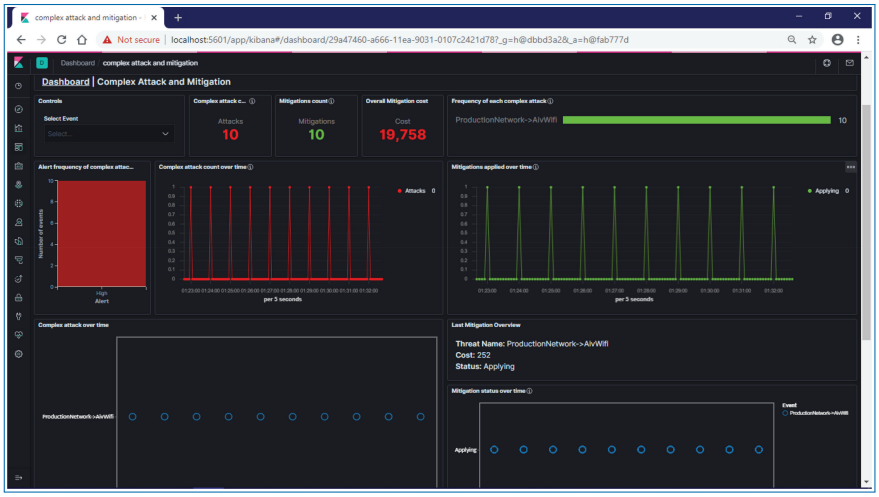

Figure 4.21. Situational awareness Dashboard – Threat mitigation view.

observed and number of mitigations applied to the CI, as well as their enforcement cost. As a matter of fact, not all mitigation strategies have the same cost on the operations of the SIPS for example production slow down and disconnecting or blocking devices from standard operation have different impacts to the SIPS operations. Moreover, the number of attacks mitigated is displayed on the top right bar. Below, in the middle section of the dashboard view the three graphs represent, respectively, starting from the left side: a bar chart with the number of alerts vs. alert relevance (low, medium and high); time series for complex attack detected over

time and safety and security mitigation policies applied to the CI. These policies aim to automatically prevent that malicious activities cause harms to production process and equipment and more importantly protect employees working in the area of attack. Bottom elements illustrate time series of type attacks and mitigations applied against them. In Figure 4.21 the Man-in-the-middle (MITM) type of attack over the WiFi network is being detected and promptly mitigated.

4.5 Conclusions and Future Outlook

In this chapter we have presented some of the Data Visualization tools and paradigms applied within the H2020 InfraStress project. InfraStress is dealing with the security of Sensitive Industrial Plants and Sites (SIPS) and therefore addressing complex attach scenarios where operators require clear awareness of the situation and capability to react to potential threats of different nature, be them physical, cyber or cyber-physical. In this context a set of comprehensive data analysis components are employed and follow a complete dataflow which starts with Physical- and Cyber threat detection and further includes Complex attack detection and Mitigation decision support. Data are then exchanged through a message broker which feeds a situational awareness dashboard which suggests SIPS operators deliberative/proactive/reactive actions.

A core part of the dashboard, providing users with intuitive and effective ways to read data and react accordingly, is Data Visualisation. In the context of SIPS and CIP, as in similar applications, effective visualisation od data makes it easy to understand them and their meaning. In this chapter we have particularly focused on Visual Analytics and AR/VR technologies as they are being applied within InfraStress. In order to be effective for SIPS a set of quantitative, qualitative and time-based visualisations have been selected and described: they include composition, distribution, comparison, maps and tag clouds. To further enhance operators' capabilities within SIPS we also presented the main AR/VR solutions employed in InfraSterss and including mixed reality devices (such as HoloLens) which allow to directly interact with VR models which represent the site/building, for instance viewing in AR escape routes or relevant a part.

Finally, we presented one of the InfraStress Pilot cases at the DePuy Synthes site in Cork (Ireland) and in particular the specifically designed situational awareness dashboard incorporating some of the visualisation tools provided by InfraStress (including in real-time views), and evaluated through a set of simulated cyber, physical and cyber-physical security and safety related events.

Acknowledgements

This work is supported by the European Commission within the project InfraStress, Grant Agreement No. 833088.

References

[1] Chambers J. M., Cleveland W., Kleiner B., Tukey P. (1983). Graphical Methods for Data Analysis. Wadsworth International Group.
[2] Tukey J. W. (1977). Exploratory Data Analysis. Boston: Pearson, Addison-Wesley.
[3] J. K. G. E. F. M. Daniel Keim, Mastering the Information Age Solving Problems With Visual Analytics, Eurographics Association.
[4] Kibana, https://www.elastic.co/kibana
[5] Elasticsearch, https://www.elastic.co/
[6] ALIDA, https://alida-demo.alidalab.it/login
[7] The Sword of Damocles, https://www.youtube.com/watch?v=NtwZXGprxag
[8] Poetker, B. (2019, September 26). The Very Real History of Virtual Reality (+A Look Ahead). Retrieved from Learning Hub: https://learn.g2.com/history-of-virtual-reality
[9] Milgram, P., Takemura, H., Utsumi, A., & Kishino, F. (January 1994). Augmented reality: a class of displays on the reality-virtuality continuum. Proceedings of SPIE – The International Society for Optical Engineering, 282–292.