JDST, vol. 5, no. 1, p1-p28, 2022
https://doi.org/10.46713/jdst.05.001
www.jdst.eu, ISSN 2534-9805, e-ISSN 2534-9813

Research Article

FOLDOUT project: Towards an enhanced and innovative architecture for border protection

Aggelos Vassileiou [a], *Vasiliki Mantzana* [a], *Abdelkader Magdy Shaaban* [b], *Andreas Kriechbaum-Zabini* [b], *Cristina Picus* [b], *Luis Patino* [c], *James Ferryman* [c], *Gaetano Pastore* [d], *Giovanni Alberti* [e], *Claudio Papa* [e], *M.Rosaria Santovito* [e]

[a] *Center for Security Studies (KEMEA), P. Kanellopoulou 4, 101 77 Athens, Greece*

[b] *AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria*

[c] *University of Reading, Department of Computer Science, Polly Vacher Building, Whiteknights, Reading RG6 6DH, United Kingdom*

[d] *Thales Alenia Space Italia, Via Saccomuro 24, Rome 00131, Italy*

[e] *CO.RI.S.T.A. Consortium for Research on Advanced Remote Sensing Systems, Corso Novara 10, Naples 80143, Italy*

ABSTRACT

The objective of the European Union (EU) in the field of external border protection is to safeguard the freedom of movement within the Schengen area, and to ensure efficient monitoring of people who cross EU's external borders. To achieve an effective and efficient border management, there is a need for applying enhanced technologies and methods that support personnel to ensure the national security interests of states while allowing the cross-border flow of legitimate trade and commerce. The paper initially discusses and analyses technologies used in EU external borders and research projects in border surveillance areas. We will further analyze the FOLDOUT research project, which focuses on through foliage detection in the inner and outermost regions of the EU. Based on the outcome of the aforementioned analysis, border guards' need for innovative and modern technologies (e.g., maintenance systems, drones, wearable

✉ Corresponding Author: Tel.: + Fax: + ; E-mail:

devices etc.) that will support border surveillance processes will be highlighted. Finally, a novel and enhanced FOLDOUT architecture will be developed and incorporated with the technologies described earlier. These innovations (a) could play a significant role in the daily activities organizational and planning tasks of border management, as well as other involved stakeholders federal agencies, and (b) might also enhance EU external borders security.

ARTICLE INFO

Received: 09 Oct 2021
Revised: 10 Nov 2021
Accepted: 30 Nov 2021
Online: … ……12 Dec 2021

KEYWORDS

4-8 comma separated Index Terms, in alphabetical order; Acronyms can be included if they are defined in the paper.

I. INTRODUCTION

Border surveillance may be described as the complex mission of monitoring the geographical areas comprising border crossing points outside the fixed opening hours as well as areas of borders between border crossing points so as to prevent irregular movement of persons and goods. Border surveillance has been defined as "the surveillance of borders between border crossing points and the surveillance of border crossing points outside the fixed opening hours, in order to prevent persons from circumventing border checks" [1].

The EU is geographically close to several areas of the Middle East and North Africa, that are characterized by economic, political and demographic instabilities and where large pools of potential migrants are located (e.g. Libya, Syria, Iraq, and Afghanistan). Likewise, the lack of economic opportunities in the countries of origin (Africa, Asia and Latin America), and demographic pressures drive movements towards the EU. More specifically, the total number of clandestine migrants and asylum seekers who arrived in Europe in 2019 was 123.920,00; 144.282,00 people arrived in 2018; in 2017, that number was 186.788,00; where in 2016, 390.456,00 people arrived [2]. The vast majority of migrants and asylum seekers who arrived in 2019 using irregular migration routes entered the EU mostly through Mediterranean passages. The Eastern Mediterranean route displayed the highest total in detected irregular border-crossings since 2016. Behind the intention of the EU border's authorities to detect irregular trespassers and block their transportation in the Schengen Area, their responsibility also involves their attempt to prevent incidents (like migrant vessels capsizes) that caused the death of more than 18.000,00 migrants during the past few years (only in the Mediterranean Sea) [2]. According to an EMN Focused Study from 2016, family reunification was the reason behind more than 30% of new arrivals in 21 Member States, even exceeding 50% in some Member States [3].

In addition, according to Europol, the Serious and Organized Crime Threat Assessment (SOCTA), published in 2021, it has been reported that approximately 5000 international Organized Crime Groups (OCGs) are active and under investigation in the EU Member States and somehow related to illegal border activities [4]. Frequently, the related activities are categorized into 11 distinct classes including drug and weapons trafficking, human and organ trafficking, trafficking in cultural property, counterfeiting, illegal wildlife trade, illegal fishing, illegal logging, illegal mining and crude oil theft. In terms of retail values, drugs and human trafficking are the most profitable amongst the relevant activities with US$500 and US$150 billion in annual basis, respectively.

In terms of prevention, the EU policies involve multiple initiatives towards securing the EU external borders in many levels. On one hand, EU has focused on reinforcing border management rules, such as the Schengen Borders Code, and strengthening and upgrading the mandates of EU agencies, such as Frontex, eu-LISA, Europol etc. [5] To enable and enforce the agency to successfully complete its objectives, the foreseen budget for 2014-2020 increased slightly from €3.7 to €3.8 billion [5]. On the other hand, over the same period, almost €0.17 billion were earmarked for Information Systems (IS) (Visa Information System and Schengen Information System) that allow national authorities to cooperate on border management by sharing relevant information. Moreover, EU has invested in enhancing the operational capacity of these agencies by purchasing novel systems such as long endurance unmanned vehicles and advanced sensing systems. Overall, improved methods, technologies, solutions and products for border surveillance are necessary to ensure an effective and efficient EU border management and internal security, which are explained in the following Chapter.

II. REVIEW OF BORDER SURVEILLANCE TECHNOLOGIES

A border surveillance system usually consists of one or multiple Command & Control Centres and a set of Sensor Stations forming a hierarchical architecture. The sensor stations are deployed across the surveillance area and can be fixed, mobile or airborne (manned or unmanned) stations. Sensor systems normally consist of the sensor and a ground station that does the primary data processing and possibly some exploitation.

Depending on their application and use, surveillance sensors can be classified in several groups. Based on the environment of deployment, sensors can be installed on aerial, ground, marine and space platforms. Aerial or air-born platforms can refer to balloons, UAVs, zeppelins, helicopters or other flying and hovering systems that can carry one or more operating sensors. Ground sensors are deployed in land set ups and can be either on mobile or fixed platforms. Examples of such systems are optical and radar sensors installed either on fixed locations (e.g. masts) or operating on vehicles. Marine surveillance can be performed using sensors installed on vessels (e.g. patrol boats) or on autonomous marine platforms capable of operating without human intervention, serving also as docking and charging stations for UAVs or other systems. Another division of sensor technologies can be made regarding their need for a human operator's presence. Unattended Ground Sensors (UGS) are devices that automatically gather sensor data on a remote target; interpret the data; and communicate information back to a receiver without interaction with a human operator. In contrast, Unattended Tactical Ground Sensor Systems (UTGSS) are designed to detect and classify targets, such as vehicles, animals or persons. UTGSS can report alarms over great distances, even using satellites, and human operators are normally not present. All sensors, irrespectively of the technology they implement, may come as fixed devices to be installed permanently, as mobile devices that operate on moving platforms (e.g. cars, vessels, UAVs) and as handheld equipment that can be carried by the personnel during surveillance operations.

Further to the aforementioned categorizations of sensors according to their deployment specific attributes, they can primarily be grouped with respect to the individual technology they employ in order to make detections of targets. In this respect there are four main sensor categories, namely imagers, radars, Radio Frequency (RF) detectors, and seismic/acoustic sensors.

Imagers are cameras that provide to the user a visible picture of the surroundings by receiving the emitted electromagnetic radiation. There are cameras that operate in a specific part of the spectrum e.g. the electro-optical cameras (EO) that operate on the visible part of the spectrum and infrared (IR)/thermal cameras that operate at the corresponding part as well as multispectral and hyperspectral cameras that take advantage of larger portions of the spectrum. Further to these categories there is also monochrome, colour, low light and long range cameras offering different capabilities to the operator depending on the operational needs.

Radars are typical systems used for the surveillance of an area and they operate by radiating electromagnetic energy and detecting the echo returned from reflecting objects. Multiple types of radars exist today e.g. the Perimeter Surveillance Radar (PSR), the Frequency Modulation Radars (FMCW/FMiCW), the Phased Array (SIMO) & Holographic Radars, the Multiple Input – Multiple Output Radar (MIMO) and the Synthetic Aperture Radar (SAR) addressing the diverse operational needs and environments of the border surveillance.

Another technology available to border surveillance is the Radio Frequency detectors. Such kind of systems can detect and even localize radio transmissions from various devices (e.g. mobile phones, transceivers, wifi, drones etc.) in a wide frequency range. An RF monitoring and localisation system may incorporate a spectrum analyser, relevant software for the automatic detection and localisation of signals and one or more antennas. Further to the aforementioned categories there are numerous additional technologies in service such as the seismic - vibration sensors, magnetic sensors and fibre-optic sensors, that address specific needs of the border surveillance tasks.

Border surveillance incorporates usage of Command and Control centres, within state of the art implementations for nationwide surveillance tasks. Hierarchically there are two levels of Command and Control centres: (a) Central Command and Control at the Central Headquarter and (b) Regional (Mobile) Command and Control centres at Regional Headquarters that are usually temporarily placed on an area of interest. The system facilitates the following tasks for Central Command and Control center: (a) strategic planning; (b) access to ongoing and historical operations; and (c) access to Regional Control and Command centres. For the Regional Control and Command centres, the following tasks are usually performed: (a) Operational planning; (b) dispatching patrols; (c) maintenance planning and (d) access to ongoing and historical operations.

Important role in the operation and security of the system has the communication network, which interconnects all the subsystems. Border surveillance systems should allow both scalability and flexibility in their implementation, as the number of sensor stations and systems should grow up to much evolving needs and any commercial sensor subsystem should be integrated (open standards approach).

Research activity regarding the development of similar tools has been very intense during the last years and several projects (as displayed in Table 1) have investigated relevant research problems and/or integrate novel capabilities in existing infrastructure.

Project	Description
Protection of European seas and borders through the intelligent use of surveillance (PERSEUS)	PERSEUS was a large pilot project (FP7-SEC 261748) that had the purpose to develop and test modern technologies and adapt their use aiming to contribute to protect the European seas and control the external borders of the EU.
Low time critical Border Surveillance (LOBOS)	LOw time critical Border Surveillance Testing and validating the low time critical components of the CONOPS) aimed at testing the low time critical scenarios of the European Concept of Operations (CONOPOS).
SEABILLA	Seabilla project progressed towards European Maritime surveillance implementation, being a cornerstone between preparatory actions like Operamar project and final demo as Perseus Project. It aimed to identify key issues to improve interoperability and reduce the information gap arising from heterogeneous surveillance systems, legislations, mandates and modes of operation.
C2 Advanced Multi-domain Environment and Live Observation Technologies (CAMELOT)	H2020 project (2017-2020) develop and demonstrate different advanced command and control service modules for multiple platform domains, based on a SOA architecture that specifies internal and external interfaces, allowing the development of a modular and scalable command and control station, customisable to the user needs.
Early Warning For Increased Situational Awareness (EWISA)	This project will provide assessment and the management of illegal migration flows at the land border, through the increase of knowledge degree of operational situation and the enhancement of reaction capacity of the participating authorities responsible for land border security
An End to end Interoperability Framework For MaritimE Situational Awareness at StrategiC and TacTical OpeRations	The project aims to enhance maritime surveillance, improve decisions support, and foster collaboration of maritime stakeholders by implementing an Interoperability Framework and associated Data Fusion and Analytics services for Maritime Surveillance and

(EFFECTOR)	Border Security and exchanging enhanced situational awareness pictures at tactical and strategic level

Table 1. EU Research Projects

In the following paragraphs, an overview of an EU funded programme related to border security called FOLDOUT is presented [2]. The main goal of FOLDOUT is to develop, test and demonstrate a system and solution to detect and locate people and vehicles operating in illegal cross-border activities under the coverage of trees and other foliage over large areas. Overall, in order to achieve FOLDOUT' s main goal, a multi-sensorial platform will be designed and developed. This platform shall incorporate end-users' requirements by integrating, ground, air, space and in-situ sensor systems.

III. FOLDOUT PROJECT SOLUTION

To design FOLDOUT system, we used Service Oriented Architecture (SOA) architecture, which is more flexible and suitable for large and complex systems. In this term, we did not have to describe each single component of the System of Systems (SoS) at structural level but just to define a set of services (e.g. Command and Control (C2) service, Data Fusion service, Sensors service), the interfaces among them and how they collaborate to provide the final service to end users. In this way, the different system components had been described like services. As a matter of example, each sensor was not seen with respect to its structure, but as an object providing some functions/services to other objects (i.e. C2 service, Fusion service, etc.) through well-defined interfaces.

Overall, in order to achieve FOLDOUT's main goal, a multi-sensor platform was designed and will be developed. This platform shall incorporate end-users' requirements by integrating, ground, air, space and in-situ sensorial techniques. More specifically, FOLDOUT's architecture design focus is on detecting and tracking activities in foliated areas, in the inner and outermost regions of the EU. FOLDOUT will build a system that combines various sensors and technologies and intelligently fuses these into an effective and robust intelligent detection platform, as illustrated in Figure 1. To support detection and tracking activities of Border Guards in foliated areas, the FOLDOUT system consists of the following main sub-systems:

(a) Sensors layer that will receive information from registered visual and non/visual sensors. This concept for border surveillance includes mobile platforms equipped with or without wireless connection to ground sensors (Radio spectrum, RADAR, LIDAR, EOS, RGB, visible and thermal cameras, acoustic sensors). These platforms are fully autarkical, providing also computational resources for the processing and automatic analysis of the sensor data. Further miniaturization of specific sensors (camera, acoustic) will facilitate deployment of resource limited lightweight smart ground sensors, which are used temporarily and complementarily, in dense forests. StratobusTM is finally introduced to border surveillance as a quasi-static platform able to operate over longer timespans at altitudes above 20km by that filling a gap between satellites and UAV;

(b) Fusion platform that is a high-level processing component responsible for performing data fusion algorithms based on machine learning and providing sensors' fused detections, tracking and alarms to the C2 platform and;

(c) C2 sub-system that combines the information received from the sensors layer, and the fusion platform with external data sources (such as weather conditions and maps) and provides alarms and relative information to C2 operators through a GIS-based real-time web platform. The sub-system includes modern command and control tools and provides a live action map with terrain and environment information continuously updated with real time information. Moreover, through this sub-system, border guards can also (a) register and manage (when possible) sensors and (b) plan interception of targets by utilizing assets from the C2 system.

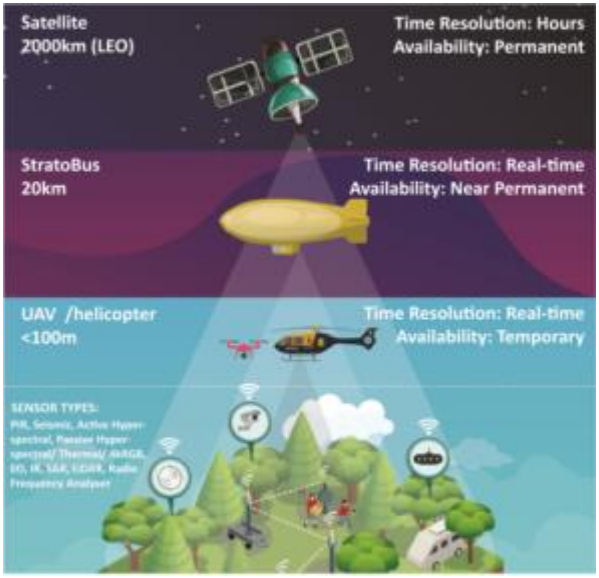

Satellite
2000km (LEO)
Time Resolution: Hours
Availability: Permanent
StratoBus
20km
Time Resolution: Real-time
Availability: Near Permanent
UAV /helicopter
<100m
Time Resolution: Real-time
Availability: Temporary
SENSOR TYPES:
PIR, Seismic, Active Hyper-spectral, Passive Hyper-spectral/ Thermal/ AiRGB, EO, IR, SAR, LIDAR, Radio Frequency Analyser

Figure 1: FOLDOUT platform and architecture

In the following paragraphs, the architecture design of FOLDOUT system and its main subsystems using the Capella tool (Arcadia method), is described. Arcadia is a system engineering method based on the use of models, with a focus on the collaborative definition, evaluation and exploitation of its architecture (6). According to the Arcadia method, the logical architecture method is used to define the conceptual level of how the system and subsystems operate to reach the necessary objective. In the Figure below, the subsystem parts of the FOLDOUT system architecture design are displayed.

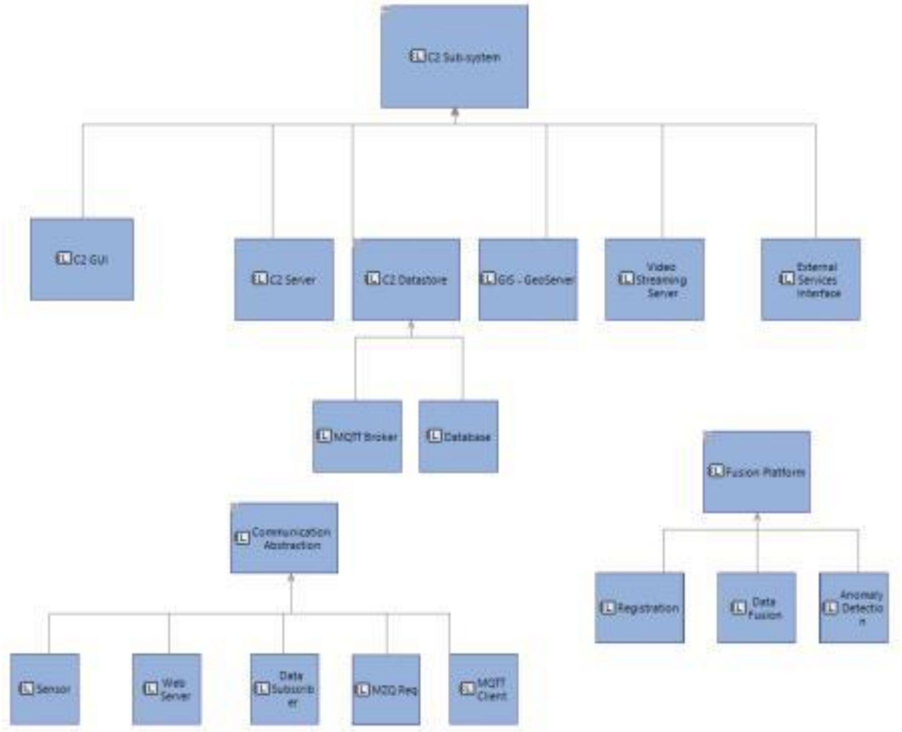


Figure 2: Logical Components Breakdown of the FOLDOUT System

FOLDOUT reinforces the decision-making process and provides operation dispatching capabilities thus allowing end-users to set and monitor activities, send and receive event related messages but also to include ad-hoc information from sensors or sensor networks. In this paper, we aim to enhance the system behavior and performance by adding alternative IoT technologies that could be integrated with the architectural design of the FOLDOUT project to improve its functionalities in the borders.

IV. PROPOSED MODEL

In this Section, an enhanced conceptual model for border surveillance design is presented that incorporates new and commonly used IoT technologies to improve the border surveillance process. We develop a series of distinct hierarchical layers that interact to provide an automated/semi-automated mechanism for controlling borders and detecting any intrusion scenarios on the border side. The suggested paradigm is divided into four basic levels, inspired by the Cloud Web of Things (CloudWoT) concept presented in [6]. The conceptual design of our proposed approach is illustrated in Figure. 3.

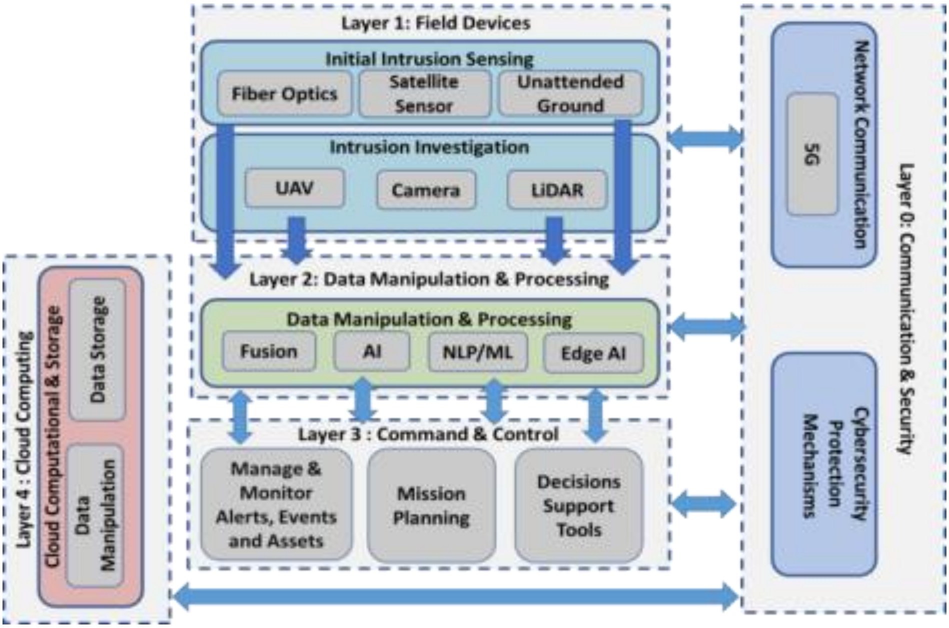

Layer 1: Field Devices
Initial Intrusion Sensing
Fiber Optics
Satellite Sensor
Unattended Ground
Intrusion Investigation
UAV
Camera
LiDAR
Layer 2: Data Manipulation & Processing
Data Manipulation & Processing
Fusion
AI
NLP/ML
Edge AI
Layer 3 : Command & Control
Manage & Monitor Alerts, Events and Assets
Mission Planning
Decisions Support Tools
Layer 4 : Cloud Computing
Cloud Computational & Storage
Data Storage
Data Manipulation
Layer 0: Communication & Security
Network Communication
5G
Cybersecurity Protection Mechanisms

Figure 3: The conceptual proposed borders surveillance model

Multiple IoT technologies are gathered and proposed to be included in this model to define an advanced border surveillance architectural design based on related work. We adapt the CloudWoT model to apply to border control. The model can manage multiple technologies that support monitoring border surveillance activities. Figure 3 depicts a preliminary design of integrating the

CloudWoT with the FOLDOUT project. The following sections overview each proposed layer, and the kind of technologies suggested to be part of the surveillance task.

1. Layer 0: Communication & Security

This layer exchanges data throughout the Internet connection from different sides. 5G technology is proposed to be defined in this infrastructure that needs a fast and reliable Internet connection all the time. This technology is considered one of the leading mobile technologies developed for people, systems, and machines [11]. The 5G becomes more common in mobility topics, indicating that it will improve communication performance among different Unmanned-Aerial System (UAS) terminals [7]. On the other hand, that will help in reducing the data latency of sending data to a centralized cloud unit for more investigation or storage.

Data transfer over an open network is prone to multiple cyberattacks. There are multiple forms that attackers could seize existing cyber vulnerabilities for compromising data over a network. We can classify these attacks into six categories according to the STRIDE (i.e., spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege). STRIDE was invented in 1999 and adopted by Microsoft[1] in 2002 [8]. Each classified category of threats violates a particular security property. The threats categories are discussed in [9] as follows: (a) **Spoofing**: Get unauthorized access by false identification by violating authentication; (b) **Tampering**: Modify or damaging data in an unauthorized way by violating integrity; (c) **Repudiation**: Denying an activity that a legal/illegal user makes by violating non-repudiation; (d) **Information Disclosure**: An undesirable manner could reveal data by violating confidentiality**;** (e) **Denial of Service**: An unauthorized action could lead to a specific service, system, or application unavailable by violating availability and (f) **Elevation of Privilege**: A restricted authorized user could claim a higher privilege than they hold by violating authorization.

Each one of these categories could violate a particular security mechanism in the system design. Therefore, it is essential to consider these security issues while developing the proposed model and its communication infrastructure. Accordingly, the IEC 62443 [10] could be proposed to be adapted and integrated

[1] www.microsoft.com

into the surveillance systems design in order to provide a complete cyber protection framework in borders. The IEC 62443 provides a cybersecurity framework for addressing existing cybersecurity issues. Each security requirements in this standard have a security level is called Security-Level Capability (SL-C). This level describes the security level that the system units of fulfilling the main security objective without additional measures [11]. Each security requirement is defined in the IEC 62443 security standard with a range of capability levels varying from 1 (i.e., casual exposure) to 4 (i.e., sophisticated means). The standard describes security requirements into seven Foundational Requirements (FRs). These requirements are discussed in [11], as follows: FR1 - Identification and Authentication Control (IAC), FR2 - Use Control (UC), FR3 - System Integrity (SI), FR4 - Data Confidentiality (DC), FR5 - Restricted Data Flow (RDF), FR6 - Timely Response to Events (TRE), and FR7 - Resource Availability (RA)). Each FR has a particular security objective that aims to provide protection mechanisms to cope with the violation of security properties due to cybersecurity threats (i.e., IAC provides authentication, UC supports authorization, SI provides integrity, DC supports confidentiality, RDF support security zones, TRE supports non-repudiation, and RA supports availability).

2. Layer 1: Field Devices

This layer accommodates multiple sensing technologies able to receive information from the environment and detect any intrusion events. This layer contains two sub-layers of detection; the first identifies and detects any vibration or movement indicating a human or vehicle movement. Then the second layer contains UAVs with LiDAR and camera for imaging and captures objective evidence about this situation.

a. Initial Intrusion Sensing

In this layer, we propose to use satellite sensor technology. The concept is defined for very long distances to alarm quickly or even provide pre-warning of border authorities by complementing terrestrial sensors. It is based on a P-band SAR instrument dimensioned with radiometric performances aimed at detect in day and night, all weather conditions and with several characteristics of forested areas. The P-band with respect to C and X-Band sensors, allows **application of penetrating the canopy to reveal hidden metal objects under the foliage** and the application to forests mapping. The satellite system products are geo-located images (2D) and target detection metadata. The system is based on constellation of LEO orbit (around 600 Km) satellites. The satellite SAR works at low frequency, 435MHz, which permits Foliage Penetration capabilities and the detection of metallic objects (car, trucks, structures) with a footprint up to 80x80 Km^2 (swath-width) covered by vegetation. The layout of the system architecture and interfaces is depicted in the following figure:

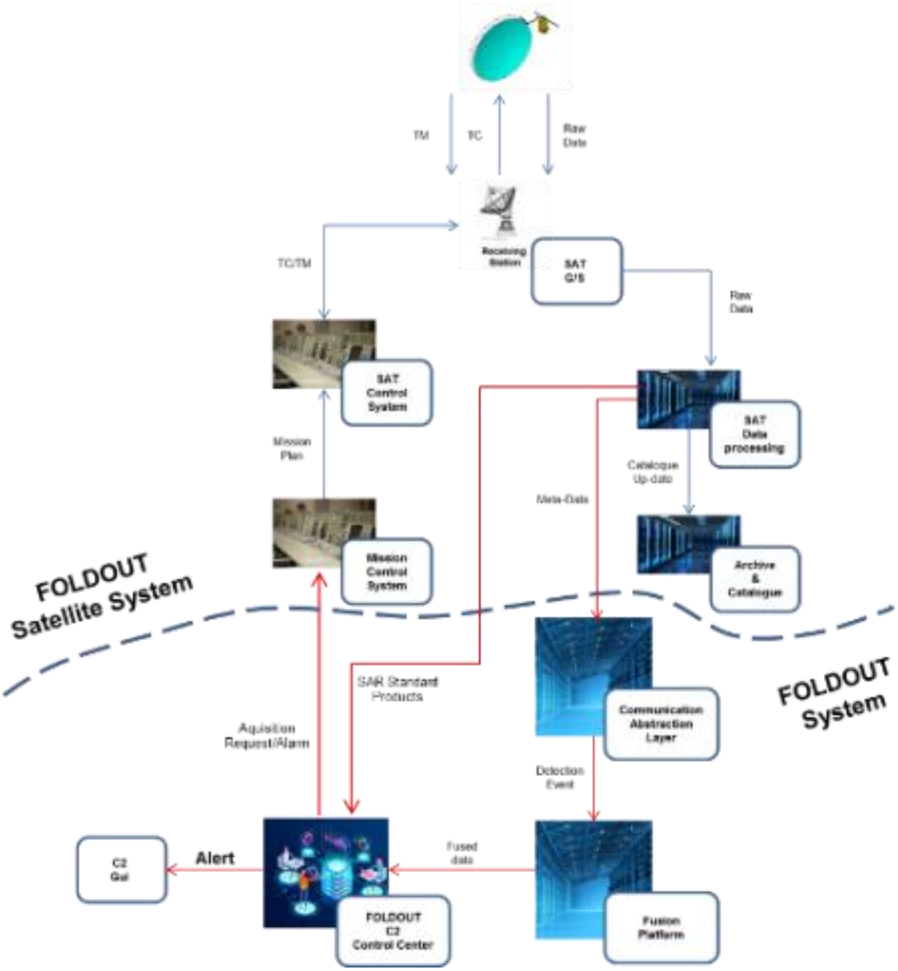


Figure 4: E2E Earth Observation Satellite Subsystem Architecture Layout

The **Ground Segment (G/S)** aims to perform the main functions/operations, at ground level, needed to manage the FOLDOUT mission, both in terms of satellite control and data management: (a) **Satellite Control System (SCS)** performs routine activities on the satellite and execution of planned payload operations (mainly, instrument data acquisitions and transmission to the ground); **(b) Mission Control System (MCS)** is mainly devoted to the development of planning activities. The activities include the preparation of the mission plans, solving the possible conflicts on the spacecraft, the commands to be uplinked (safety on board, attitude and orbit maintenance, sensor operative mode setting, on-board S/W patches to be uplinked); and (c) **Data Processing System** is the core element which is charge of the processing of the satellite raw data with the aim to provide Level 1 (images) and Level 2 (metadata) products to the FOLDOUT interface. Images and metadata are stored in the Archive and Catalogue system.

The following options are envisaged for the Ground Segment configurations. The first option is the **Centralized Architecture** that envisages the use of a single data receiving ground station located near the polar region in order to maximize the contact time per day. The data acquisition ground station will be located in **Svalbard** (or Kiruna). The Data Processing and Data Distribution are located in the same center and are common for all countries/border authorities. The second option is the **Distributed Architecture** that envisages using of dedicated Data Processing and Distribution Center per each country in order to allow an autonomous data processing and storage. This configuration also permits to reduce the system **response** time of around one orbit duration (1,5 hours) . Indeed, upon acquisition of the data above a country they can be immediately downloaded to the Ground Station positioned on that country.

S**pace Segment** analysis have been conducted in terms of orbit parameters, coverage and system time response. Mission requirements and Instrument performance are among the main drive for orbit determination with either single satellite or satellite constellation scenario. The mission requirements analysis shows that some characteristics of the FOLDOUT orbit are mandatory, i.e.: Global coverage; and Frozen Sun-Synchronous Orbit (SSO) with down-dusk local time at either ascending or descending node (LTDN). Frozen SSO allows to have an optimal solar illumination over the solar panels of the satellite and therefore to optimise solar power availability and to minimise the duration and number of eclipse. One more advantage of SSO is that they are polar orbit; it guarantees frequent and good visibility of artic ground station. The orbit chosen for FOLDOUT mission is described into Table 2. Chosen orbit has 12 days repetition cycle, with total number of 179 orbits for each cycle, hence every twelve days passes on selected area, repeats. Separation between adjacent ground tracks is 224 Km at equator wrt 300 Km of access area. Access area is the maximum observed area with required instrument performance.

Orbit type	Sun-Synchronous Orbit dawn-dusk
Inclination	97.758°
Revolutions per day	14+11/12
Eccentricity	0.0010621
Period	96.72 minutes
Semi-major axis	6970.87 Km
Altitude	592.73 Km
Argument of perigee	90°
RAAN (21 March)	275°

Table 2: summary of main orbit parameters

Coverage analysis example on Greece/Bulgaria border area.

For the scopes of mission analyses several AOI have been considered according to FOLDOUT end user needs. As a matter of example, in the following are described the performance results relevant to the Greek/Turkish and Bulgarian/Turkish borders. The simulations have been performed with MatLab tool. The reference site to collect satellite passes statistics has been positioned on Komotini area. Chosen orbit allows a total number of 7 passes over Komotini test area. Those passes are collapsed into 4 different days, hence sometimes two pass per day occurs (Figure 5-a). This analysis takes into account both ascending and descending passes. Upgrade to a constellation of three satellites lead to more frequent pass on selected area as shown in Figure 5-b. Figure 6 shows access area achievable on Komotini area with **one satellite**. The whole boundary line between Greece and Bulgaria is covered with three passes. Three satellites have the same orbit with difference in LTDN only, which is 258°, 275° 291°. Figure 7 shows coverage map of **three-satellite constellation** after a complete repeat cycle (12 days). In conclusion, to obtain a more frequent passes on a selected area, satellite constellation is necessary.

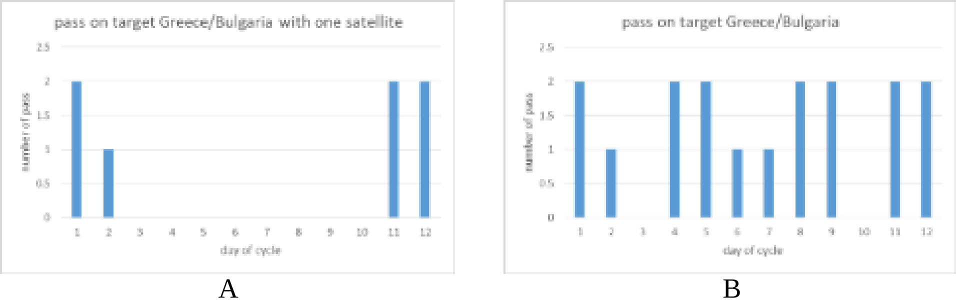


Figure 5: passes on Komotini Area: single satellite (a), three satellites (b)

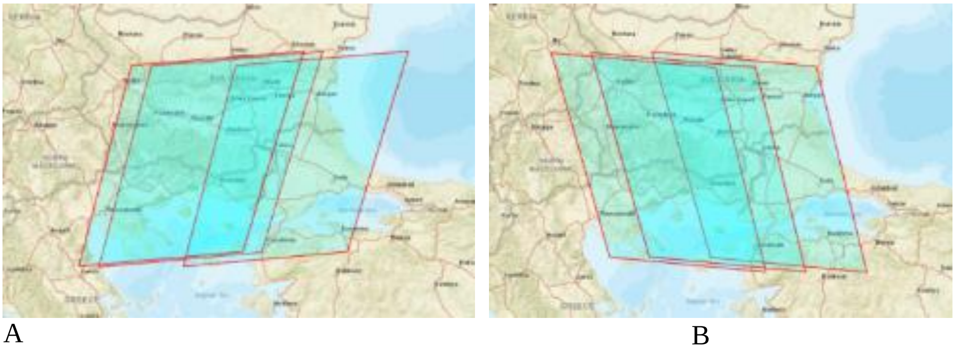


Figure 6: achievable access area on Komotini AOI

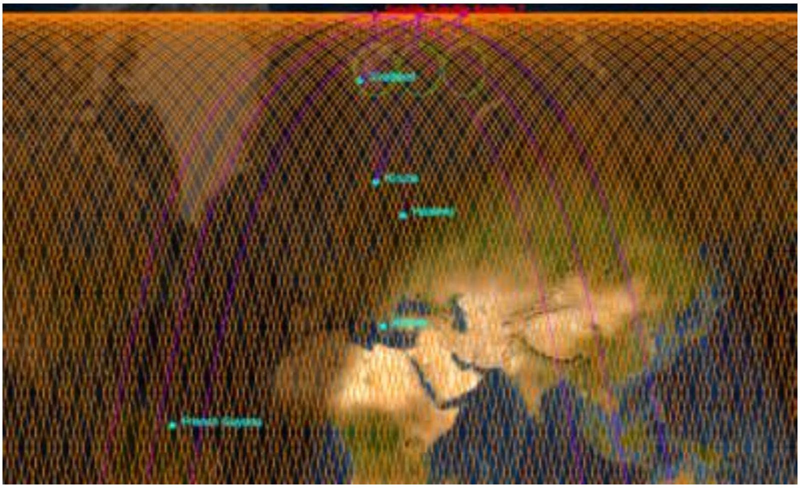


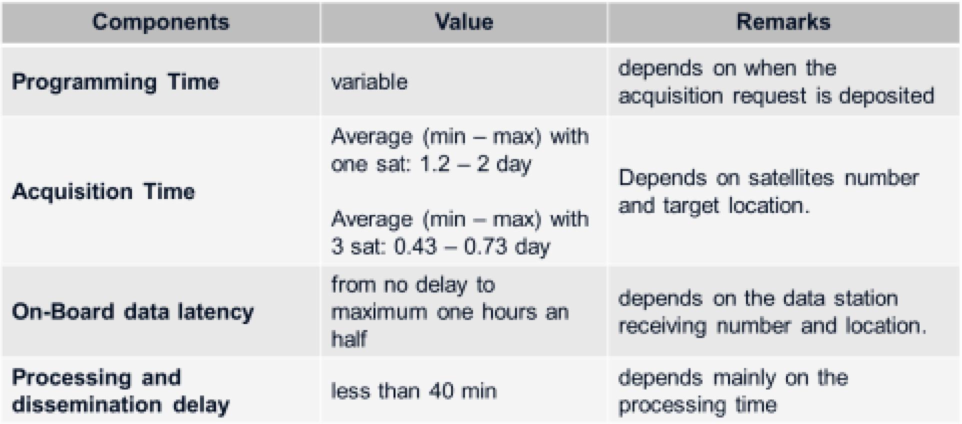
Figure 7: coverage map with three-satellite constellation

System Time Response

In order to evaluate the readiness of the system to respond at the requests of the users the system response time as been used as an indicator of the performances. After receiving the user request, the control center of the satellite send a tele-command to the satellite when it is in visibility ground station. Then when the satellite pass over the target area it takes the image of the required border area and, after reaching ground station, downloads the data. Overall system response depends on several factors, such as number of satellite (coverage), ground station visibility, processing time. Ground station visibility depends on theirs geographic position; **Table 3** shows visibility time and number of contact for each ground station for the completely repeat cycle. The acquisition time is the interval of target visibility, when the observation can be done. **Table 4** shows a summary of averaged system time response for each repeat cycle.

Ground station visibility (minutes)	**Athens**	**Kourou**	**Helsinki**	**Svalbard**	**Kiruna**
min	2.2	9.2	4.4	7.2	4.4
max	12.41	12.01	12.62	12.6	12.41
average	9.17	10.84	9.85	10.88	10.2
Number of contacts for repeat cycle	7	4	9	179	139

Table 3: Ground-Station visibility time for each contact.



Components	Value	Remarks
Programming Time	variable	depends on when the acquisition request is deposited
Acquisition Time	Average (min – max) with one sat: 1.2 – 2 day Average (min – max) with 3 sat: 0.43 – 0.73 day	Depends on satellites number and target location.
On-Board data latency	from no delay to maximum one hours an half	depends on the data station receiving number and location.
Processing and dissemination delay	less than 40 min	depends mainly on the processing time

Table 4: System Response Components summary

The **satellite SAR** performancesDesign of satellite SAR payload, especially at low frequency, requires an accurate trade-off analysis of main system parameters, such as:

- Orbital determination: Choosing the orbital altitude presents the first trade-off between a low orbit that, by being closer to the observed targets, reduces the power required by the radar and the need to minimize atmospheric friction, which increases at lower altitudes and translated to the need to carry more fuel (hydrazine) to maintain orbit;
- Incidence angle: The incidence angle affects the radar cross section of target area (a smaller incidence angle results in more backscattered power) but also the ground range resolution (which improves for larger incidence angles) and the swath of the system; and
- Sensitivity: The sensitivity is usually specified in terms of the noise equivalent σ^0 (NESZ). The sensitivity can be improved in several ways, such as increase the average power by increasing either the peak power, which is technology-limited, or the pulse duration. It is upper-bounded by the total available power; Reduce the range to the target, which for an orbital case implies lowering the orbital altitude; Increase the antenna gain, which implies increasing its physical size and either degrading the azimuth resolution or the swath width; reduce the required geometric resolution; reduce the noise introduced by the system (either receiver noise or quantization noise). It is worth stressing that the noise power is lower bounded by the noise temperature of the antenna, which for a SAR system is usually in the order of 300K; Reduce overall system losses.
- Range Resolution: Within legal and technological limitations, the range resolution can be made arbitrarily fine by increasing the pulse bandwidth at the cost of losing sensitivity. The resolution also improves for increasing incidence angles, but this also increases the range and tends to reduce the normalized radar cross-section.
- Azimuth Resolution: The azimuth resolution of a SAR system is strictly depended on the azimuth dimension of the antenna. To improve the along-track resolution it is necessary to decrease the antenna length in the along-track dimension.
- Antenna: The key antenna parameters affecting the SAR performance are the antenna gain and its beam pattern. The antenna gain is directly proportional to its effective area. A first lower bound on the required antenna (effective) area can be derived from a zero order analysis of

range-azimuth ambiguities, which sets the minimum area of a SAR antenna. The minimum area depends by the carrier wavelength, the incidence angle, and the orbital velocity, which is set by the orbital height and almost constant for the range of useful orbital altitudes.

- Pulse Repetition Frequency (PRF): The range of PRFs values is established by the maximum acceptable range and azimuth ambiguity-to-signal ratios, as well as the transmit and nadir interference. At some look angles, there may be no acceptable PRFs that achieve the minimum requirements. In general, as the off-nadir angle is increased, the PRF availability is reduced and the ambiguity requirements must be lowered to find acceptable PRFs.
- Frequency Band: A fundamental system parameter is the center frequency of the system. Its choice depends on the applications, the required resolution, and on technological aspects. Further constraints can be imposed by ITU regulation in force.

System trade-off analysis includes also ionosphere and ground vegetation attenuation (estimated as 8 dB as maximum two-ways value). Transmitted signal bandwidth is limited to 6 MHz by ITU regulation as well as the transmitted peak power (150 W) and duty cycle (12 %). The incidence angle of 35° has been chosen as in the middle of required system access area. **Figure 8** shows the values of NESZ as a function of incidence angle taking into account previous restriction on system parameters. SAR system is able to reach -26 dB of NESZ up to about 30° of incidence angle. In this access area, the system can achieve a maximum swath of about 80 km. Summary of system parameters values and performance figures are reported in **Table 5**, as results of system definition and trade-offs performed along previous paragraphs.

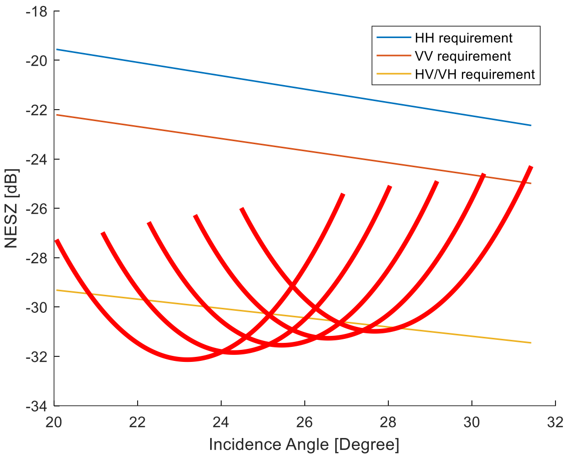


Figure 8: NESZ values as a function of incidence angle with ITU requirements and vegetation attenuation margin

Parameter	Unit	Value	Comments
Spacecraft altitude	[Km]	600	Assumption
Antenna overall efficiency		0.8	
Polarization		SINGLE/DUAL/QUAD	
Receiver noise figure	[dB]	3	
System losses	[dB]	8/10 (with vegetation margin)	
Transmitted bandwidth	[MHz]	6	ITU requirement
Number of looks (max)		5	System definition
Transmitted peak power	[W]	> 1300 150 (full ITU compl.)	
Tx duty cycle	[%]	20-45 (DUAL-POL) 37-44 (QUAD-POL) Max 12% (full ITU compl.)	
Oversampling factor (Doppler)		1.45	
Doppler bandwidth	[Hz]	1087	
PRF	[Hz]	1460-1660 (DUAL-POL) 3050-3175 (QUAD-POL)	
Antenna tapering coefficient		1.06	
Antenna side-lobe level	[dB]	< -24	
Antenna area	[m^2]	99.5	
Antenna dimensions (range x azimuth)	[m^2]	6.7 x 14.8	
Antenna range aperture	[deg]	6.2	
Antenna azimuth aperture	[deg]	2.8	
Antenna gain	[dB]	32.3	
Range resolution	[m]	35-73	
Access area	[deg]	20-45	
Antenna pointing	[deg]	21.3-37.1	
Azimuth resolution (single-look)	[m]	7	System performance
Range resolution	[m]	35-73	
Radiometric resolution	[dB]	< 1.7 (SNR > 10 dB)	
Swath	[km]	30-100 (DUAL-POL) 45-60 (QUAD-POL) < 80 km (full ITU compl.)	
NESZ	[dB]	-36/-48 (DUAL-POL) -45/-50 (QUAD-POL) <-26 dB (full ITU compl.)	
AASR	[dB]	-22/-54(DUAL-POL) -20/-50 (QUAD-POL)	
RASR	[dB]	-20/-70(DUAL-POL) -20/-65 (QUAD-POL)	

Table 5: Summary of main system parameters and expected performance of satellite SAR instrument

In order to validate and refine the satellite SAR performances the acquisition of airborne datasets which are representative of the satellite system took place . The campaign is based on an airborne P-band SAR that has been developed by CORISTA in the framework of the Italian Space Agency (ASI) technological project (contract ref. I/062/10/0 and ref. 2015-029-I.0). The campaign has been performed at the beginning of November 2021 at Bulgarian border area at the military base of Zmeyovo, near Plovdiv, with the support of the Bulgarian Defense Institute "Professor Tsvetan Lazarov", which is part of the Ministry of Defense of the Republic of Bulgaria. The figure provides a snapshot of the CORISTA radar system antenna (kindly granted for publication by Italian Space Agency) mounted on board the Bulgarian helicopter.

Figure 9: CORISTA team and SAR demonstrator antenna mounted on board

Airborne SAR Demonstrator, properly tailored in order to be a scaled version of the Satellite Radar System will permit to verify scaled performance of the radar system in terms of Foliage Penetration (FoPen). The campaign has been performed in a relevant scenario: airborne SAR specifications are reported in the following table. The data collected will be used to set the parameters of Satellite Radar System. At the time of publication, the analysis of the collected data is in progress.

Parameters	SAR-Low
Carrier	450 MHz
Tx bandwidth	40 MHz
Tx steps	1
PRF	1000 Hz
Pulse width	2 µs
Mode	Pulsed
Antenna type	Planar array 4 x 1 patch dual polarization
Antenna gain	17 dBi
Elevation pointing	45°
Azimuth pointing	0°
Range aperture	75°
Azimuth aperture	20°
ADC Sampling frequency	200 MHz
Peak power	200 W
Power consumption	500 W
Rack Weight	30 Kg
Rack Dimension	50x50x65 cm
Antenna Dimension	10x45x165 cm
Antenna weight	15 Kg
Operating altitude (agl)	1500/2000 m

Table 6: Airborne SAR specifications

b. Intrusion Investigation

This layer aims to gather more evidence concerning previously detected events by capturing images about one of the major technologies for border surveillance improvement: the unmanned aerial vehicle (UAV) or drone. That it is capable of scanning a large coverage area and detecting unauthorized tracks efficiently [12]. UAVs can be utilized in a complex territory with multiple road bumps and detours to make the border control process more difficult. The UAV helps identify abnormal border activities between Russia and southern Finland, as mentioned in [13]. Recently, around 100 UAVs were installed by the US on Mexico's borders. As discussed in [14], the United States Border Patrols use three types of drones as defined: (a) **AeroVironment Raven**: this type of drone has about a maximum of 80 Kmh speed with 90 minutes endurance flight time; (b) **Aeryon Skyraider**: it has about 50 kmh maximum speed with 50 minutes max flight time. The Skyraider can fly for a maximum of 1500 feet; and (c) **Lockheed Martin Indago 3**: it has a 40 kmh maximum speed and can flight in variant altitude ranges from 10 up to 500 feet. The total flight time by the Indago 3 could be reached up to 50 minutes. The different types of drones and their classifications lead them to be an essential part of modern and smart border surveillance applications. The Light Detection and Ranging (LiDAR) is proposed to be integrated into the border surveillance systems as presented in [14]. This technology works by emitting laser light pulses; the reflected energy of these pulses is measured to identify hit objects. The integration of LiDAR in border surveillance with AI algorithms for object and tracking detections helps in improving the detection system and reduce the total costs [15].

A further technology to be adopted here is the use of specialized cameras with integrated intelligence functionalities. In the FOLDOUT system a smart sensing platform is integrated which provides different complementary visual sensors targeting ground-based surveillance. The sensor combines high resolution RGB, thermal and low-light cameras with zoom option. The combination enables operability day and night and under strongly varying weather conditions. An additional element is the transportability of the lightweight system, which can be deployed to remote areas, as well as potentially self-sufficient if operated by battery. The typical sensor range is about 100-200m, for ad-hoc surveillance of specific areas. Further, the sensor provides advanced detection functionalities by novel AI based algorithms for object detection and classification under partial occlusion, such those originating by objects partially hidden under vegetation. Independent detectors based on CNN perform video analytics for object and event detection on each video stream [16]. The platform integrates an NVIDIA Jetson AGX Xavier board including a CPU and integrated GPU units, for onboard data processing. This enables sending to the wireless network only detection results and not raw data, both to avoid overloading of the network and also to fulfill basic privacy by design requirements. Streaming is performed only upon explicit request by the operator. The sensor is automatically geo-localized for accurate target localisation and visualisation on a map of the area, useful to provide the operator with a visual feedback in a GUI.

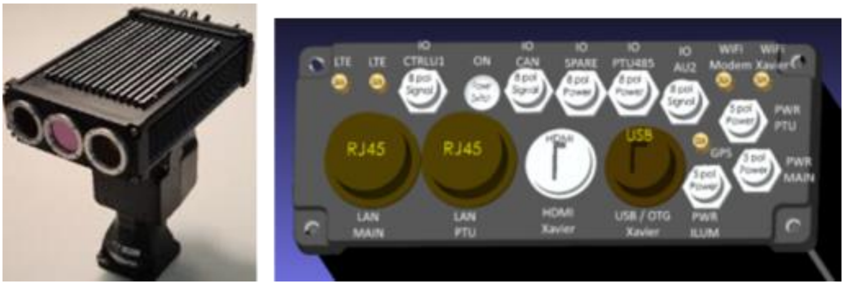


Figure 10: Images show the front and back of the camera platform with main connectors.

3. Layer 2: Data Manipulation & Processing

Data processing on border sites is one of the main challenges that need more attention to succeed providing meaningful information to border guards. Data processing in border surveillance has to deal with a huge amount of data to be processed at the Command & Control centre. Most of the surveillance towers at border sites are managed by human beings for investigating collected images to give appropriate decisions of different situations [14]. Human observations could be prone to errors or inaccurate decisions. Moreover, border guards can be overwhelmed by having to monitor systems corresponding to different types of sensors I.e. thermal cameras, RGB cameras, seismic, LiDAR, SAR sensors just to mention a few; and integrating or making the mental or manual correspondence of alerts from those systems becomes a very demanding task for the border guard.

Integrating AI with its different techniques (i.e., NLP, ML, etc.) would provide a more efficient surveillance solution on borders instead of a group of people sitting in front of screens [14]. In FOLDOUT we will develop different key components that can employ AI features to:

- provide the automation of digital and physical tasks and considering the information management process.
- Provide an integrated overview of the location of the alerts by registering all different sensors into a single map.
- process and manage a large amount of collected data which combines the quantity of data and quality of results. Particularly, data corresponding to objects triggering sensor modalities can be intelligently fused.

- combine Natural Language Processing-like (NLP) and Machine Learning (ML) techniques to deliver human-like reports of warnings and alerts to border guards that give a complete situation awareness

Therefore, FOLDOUT aims to provide a fast and reliable action against multiple critical events [6], triggered in border surveillance by an heterogeneous set of sensors. Critical AI-based components analyse data collected from all different resources to perform complete situation awareness. The technology aims to be efficient working with smart sensors processing as much data near to the source as possible. This technology also does not need to be connected to the Internet all the time, which reduces power consumption and data costs [17].

4. LAYER 3: COMMAND & CONTROL

In several cases on borders, the human decision is still required. Border patrols can do more investigation on the collected data for decisions toward multiple events. Therefore, a human can interact with the whole system terminals through user interfaces (UI) to observe any malicious behavior activities in borders. In addition, a human can monitor, investigate and manage alerts and events that indicate border intrusion.

5. LAYER 4: CLOUD COMPUTING

This layer is concerned with data storage, data processing, and in-depth investigation. The collected events could be used for future dataset training for the used AI algorithms for enhancing the identification algorithm and improve the overall system decisions for handling existing threats.

In doing this, the daily activities, as well as organizational and planning tasks of border management, as well as other involved stakeholders federal agencies, will be more efficient and effective. Moreover, it will improve decisions support, and foster collaboration of involved stakeholders and therefore external borders security will be improved. In addition, the public will benefit from the enhanced capability and efficiency in how threats are prevented, detected, mitigated and reacted to, meaning that it will contribute to citizen protection via controlling of illegal activities and saving lives.

VI. CONCLUSIONS

In this paper, the technologies used in EU external borders and research projects in border surveillance areas are presented and FOLDOUT research project, which focuses on through foliage detection in the inner and outermost regions of the EU is analysed. Based on the outcome of the aforementioned analysis, border guards' need for innovative and modern technologies (e.g., maintenance systems, drones, wearable devices, etc.) is highlighted and a novel and enhanced FOLDOUT architecture is proposed. These innovations (a) could play a significant role in the daily activities organizational and planning tasks of border management, as well as other involved stakeholders federal agencies, and (b) might also enhance EU external borders security.

ACKNOWLEDGEMENTS

The work presented in this paper has been conducted in the framework of FOLDOUT project, which has received funding from the European Union's H2020 research and innovation programme under grant agreement no 787021. 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.

REFERENCES

[1] European Commision, "Regulation (EU) 2016/399 of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification)," 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0399&rid=3 (accessed May 05, 2021).

[2] International Organisation of Migration (IOM), "IOM- UN Mighration." https://migration.iom.int/europe?type=arrivals (accessed Feb. 05, 2021).

[3] European Commission, "EMN Focussed Study 2016 - Family Reunification of TCNs in the EU: National Practices." https://ec.europa.eu/home-affairs/sites/default/files/08a_estonia_family_reunification_final_en.pdf (accessed Feb. 05, 2021).

[4] EUROPOL, "European Union serious and organised crime threat assessment 2017," 2017. https://www.europol.europa.eu/socta/2017/ (accessed Jan. 05, 2021).

[5] FRONTEX - Research and Development Unit (RDU), "Border Surveillance Best Practice and Guidelines," 2017.

[6] A. M. Shaaban, C. Schmittner, T. Gruber, A. B. Mohamed, G. Quirchmayr, and E. Schikuta, "CloudWoT - A Reference Model for Knowledge-Based IoT Solutions," in *Proceedings of the 20th International Conference on Information Integration and Web-Based Applications &amp; Services*, New York, NY, USA, 2018, pp. 272–281. doi: 10.1145/3282373.3282400.

[7] L. Huxtable, "Artificial Intelligence-based capabilities for the European Border and Coast Guard," p. 167.

[8] N. Shevchenko, "Threat Modeling: 12 Available Methods," *Carnegie Mellon University - Software Engineering Institute*, 2018. https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html (accessed Sep. 27, 2020).

[9] M. Abomhara, M. Gerdes, and G. M. Køien, "A STRIDE-Based Threat Model for Telehealth Systems," p. 16.

[10] IEC, "Security for industrial automation and control systems - part 4-2: Technical security requirements for IACS components," International Standard, Feb. 2019.

[11] *IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*. 2013.

[12] Z. Sun, P. Wang, M. C. Vuran, M. A. Al-Rodhaan, A. M. Al-Dhelaan, and I. F. Akyildiz, "BorderSense: Border patrol through advanced wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 3, pp. 468–477, May 2011, doi: 10.1016/j.adhoc.2010.09.008.

[13] J. Rajamäki, "Studies of satellite-based tracking systems for improving law enforcement: Comprising investigation data, digital evidence and monitoring of legality," p. 222, 2014.

[14] S. Ghaffary, "The 'smarter' wall: How drones, sensors, and AI are patrolling the border," *Vox*, May 16, 2019. https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai (accessed May 19, 2021).

[15] "How Technology is Ramping Up Border Security," *Innovation & Tech Today*, Oct. 18, 2019. https://innotechtoday.com/border-security/ (accessed May 24, 2021).

[16] J. Pegoraro, R. Pflugfelder, "The Problem of Fragmented Occlusion in Object Detection.". Proc. of the Joint Austrian Computer Vision and Robotics Workshop 2020. s.l. : arXiv preprint arXiv:2004.13076, 2020.

[17] "Enabling Artificial Intelligence (AI) Solutions on Edge - Akira AI," *AkiraAI*. https://www.akira.ai/ (accessed May 23, 2021).