IEEE Open Journal of the Systems Engineering

Received 13 April 2023; revised 5 October 2023; accepted 19 October 2023. Date of publication 25 October 2023; date of current version 17 November 2023.

Digital Object Identifier 10.1109/OJSE.2023.3327524

Security Viewpoint and Resilient Performance in the Urban Air Mobility Operation

RAQUEL HOFFMANN [1], DANIEL PATRICK PEREIRA [2], AND HIDEKAZU NISHIMURA [1] (Member, IEEE)

[1]System Design and Management Graduate School, Keio University, Kanagawa 223-8521, Japan.
[2]Airbus Defence & Space GmbH, 82024 Taufkirchen, Germany.

CORRESPONDING AUTHOR: RAQUEL HOFFMANN (e-mail: raquel.hoffmann@keio.jp)

ABSTRACT The rapid development of urban air mobility (UAM) technologies and their integration into the urban environment brings new security challenges. Threats to aviation and mobility systems continue to evolve. The urban space places additional vulnerabilities to which UAM stakeholders strive to enhance and develop UAM security capabilities. Ensuring the security of UAM operations requires a holistic and integrated approach that considers the complex interdependencies between various stakeholders and components of the UAM ecosystem. This article explores security viewpoints and resilient performance in UAM operations using enterprise architecture modeling methodology through the unified architecture framework (UAF). The ecosystem approach recognizes that UAM operations involve a multitude of actors, including UAM designers, operators, service providers, airspace managers, and regulators. Each actor has a unique role and perspective on security, and their actions and decisions can significantly impact the overall security and resilience of the UAM operation. The approach includes a security viewpoint integrating different actors to identify and assess security risks, strategies to mitigate them, and a discussion about resilient performance in the UAM ecosystem. The security viewpoint considers technical and nontechnical security aspects, including human factors, organizational culture, and cybersecurity frameworks. Moreover, a security state diagram for UAF is proposed, supporting the discussion of how different resilient scenarios can avoid undesirable security states. The results include views defining risk and capability taxonomies, security structure, security states, and ground security processes, showing how the UAM enterprise operates to achieve resilient performance.

INDEX TERMS Resilience, security, unified architecture framework (UAF), urban air mobility (UAM).

I. INTRODUCTION

Security is a critical concern in the aviation industry. Operators and regulators are constantly adapting to new threats and scenarios. The complexity of achieving safe operations by responding to hazards and malicious events is a challenge that moves providers and manufacturers toward new solutions and procedures. Governments and industries work together in civil aviation to harmonize responsive security systems based on data, risk management, and efficient technology [1].

The concept of urban air mobility (UAM) aims to provide transportation to solve challenges in congested urban scenarios [2]. Vehicles capable of vertical takeoff and landing are envisioned to operate at low-level altitudes and attend to flexible air travel demand [3]. UAM intends to integrate manned and unmanned aerial vehicles (UAVs) transporting people or cargo in an urban or suburban environment. Control and navigation of such aerial vehicles can be handled by a pilot, a controller from a remote location, onboard automation, or a ground-based centralized, automated system [4].

The UAM system of systems (SoS) involves a large number of stakeholders, such as service operators, service providers, lawmakers, vehicle designers and manufacturers, human operators, and the public. Integrating UAM operators, technologies, and human interactions creates a complex ecosystem, further complicated by passenger transportation's safety-critical nature. To ensure safe and efficient transportation, numerous concepts of operations are being explored across industry and research domains. The complex nature of the UAM ecosystem presents many opportunities for analysis, exploration, and development of approaches to ensure safe and secure operations.

While some studies have been published on UAM security, most current research relies on autonomous flight and technologies to protect communication and navigation [5], [6], [7], [8], [9]. Although these research areas are important for understanding UAM vulnerabilities, resilient performance in UAM operations has limited related work [10], [11]. Security is essential to ensuring the safety of passengers, crew, and the public, and creating the public's trust and confidence in the UAM's future transportation. In order to achieve its objective of delivering secure air transportation services in urban regions, the UAM idea must establish a durable operating atmosphere that integrates UAM infrastructure and support systems with current air transportation systems. This integration should facilitate the secure exchange of data necessary for UAM operations [5].

The organizational and human operational aspects of the UAM ecosystem are crucial for the security discussion. The process of avoiding, withstanding, and recovering is not limited to systems and technology. To achieve resilient performance, people and processes must be considered among systems and mitigations. The personnel involved in the operation are vulnerable assets that can be affected by malicious events. Personnel plays an important role in achieving security and, most importantly, are agents of resilience performance [12]. With threats and vulnerabilities, situation awareness is also fundamental. Humans can only make the right decisions if they have a good understanding of the environment and are able to avoid unsafe scenarios [13]. In order to design systems and define processes that support resilient performance, human aspects must be considered [14]. Although increased autonomy can contribute to efficiency and safety in aviation, humans greatly increase the probability of resilient performance [15]. Therefore, a method to define and evaluate the resilient performance in the UAM ecosystem should include a holistic viewpoint.

This article proposes security viewpoints, security states, and processes for UAM operation based on resilience engineering (RE) principles. The organizational and operational representations presented in this article provide means to understand how the UAM ecosystem can achieve resilient performance in different scenarios. The rest of this article is organized as follows. Section II reviews security literature to understand the concepts applicable to the UAM context. The objective is to identify the critical security aspects in the UAM concept of operations (ConOps) necessary to understand the problem space. Section III explains the research methodology. The chosen approach is justified after defining the security problem in the UAM ecosystem. The challenges to be mitigated are explored holistically, driving the boundaries of the solution space. Next, the modeling methodology applied in this article is presented. Section IV introduces the enterprise architecture (EA) development. It starts with risk taxonomy and capability's structure. Following the enterprise's strategy to deal with the security risks gives a vision of the enterprise's assets and risks. Then, a state diagram for security is proposed to support the ecosystem's ability to respond to adverse events. Section V explores resilient performance in ground operations. Risk mitigation and security controls are defined and connected with the resource layer. Operational processes are detailed and validated, tracing back to capability and resource coverage. Finally, Section VI concludes this article.

II. BACKGROUND

A. SECURITY

Security is a broad field covering mainly physical, personnel, information, and network security. Security risks are related to the loss of confidentiality, integrity, or availability, and reflect the potential adverse impacts on organizational operations, assets, and stakeholders. Since security risk cannot be eliminated entirely due to limited resources, organizations aim to find the optimal balance between identifying, protecting, detecting, responding, and recovering [16].

Security controls are mechanisms that could be physically or logically employed within a system or organization to protect the system's confidentiality, integrity, and availability from managing the security risk. As security controls impact system architecture, the selection, design, and implementation are essential to realize early in system development. NIST SP 800-53 r5 [17] provides a catalog of security controls. Security capability is the system's ability to achieve a desired effect under specific conditions through a combination of security controls [12]. Proactive security controls comprise a holistic approach that focuses on prevention. On the other hand, reactive security controls focus on detecting and responding to a security threat.

Previous article on security topics of UAM addressed vulnerabilities [5], [6], [7], [18] and discussed the security perimeter for UAM operation [9]. Others focused on authentication risk and mitigations [8], security of autonomous operations [19], and communication enablers, including security concerns [20]. Most of the related work uses autonomous operation as an operational scenario and focuses the effort on communication and navigation security risks. The previous article's motivation is based on assessing vulnerabilities and dense UAM operations that foresee unmanned vehicles. Although some use a cybersecurity framework [5], no one uses an EA to support the security analysis. Moreover, from our knowledge, no studies were found evaluating UAM cyber, physical, and personnel security of piloted vehicle operations.

Security work using EA, specifically unified architecture framework (UAF), is recent. The works [21], [22] provided guidance on using and integrating UAF security views. In addition, UAF security views were explored with the risk assessment and analysis modeling language and the systems modeling language (SysML) in a search and rescue operation [23]. No other work has been published uniting UAF security views and the UAM context.

B. RESILIENCE

Resilience is a concept used in a wide range of definitions and applications. This article will focus on RE principles and

explore resilience *performance* at an organizational level represented by the UAM ecosystem. An integrative review work [24] on RE demonstrated that despite not having a universally agreed definition for the term, the idea involves a collective aspect, is multifactorial, multilevel, and multidimensional, associated with four fundamental principles: anticipation, response, learning, and monitoring.

RE is a recent topic (2003) and was introduced in the safety domain associated with organizational behaviors [25]. The safety management topic explains the strong relation with organizational resilience, in which a proactive approach involving human factors and cultural behavior are protagonists [26]. Thus, the RE definition used in this article is "a sophisticated approach for managing organizational safety through the development of cognitive, behavioral, and cultural abilities to enable organizational members at all levels to actively anticipate, respond, monitor, and learn to operate close to the boundary of safe operations (…)" [27].

The idea that resilience is not a static property but a performance in constant adaptation and improvement of organizations (or systems) has been defined [28] and explored in different domains. Resilient performance is related to safety more broadly. For the work presented in the following sections, resilient performance refers to the ability of individuals, teams, and organizations to adapt and perform effectively in the face of security threats or malicious adverse events. Some researchers have addressed resilient performance in the security context, focusing on cybersecurity architectures or interfaces [29], [30], [31]. Discussions on performance as cyber resilience metrics were also presented [32]. Despite insightful material [10] on how RE can enable the evolving airspace to adapt and perform resiliently, publications on resilient performance in UAM operations are restricted.

When it comes to exploring RE through modeling, the complexity of a systematic approach still represents an open gap. The literature review in [33] shows an overview of the current effort to advance the RE research agenda into sparse work in different industries with a different focus. This reflects the nature of resilience and safety-critical operations. The inherent complexity of activities involving cognitive, behavioral, and cultural aspects of RE poses a challenge for modeling resilience in an organization. Although quantitative and systematic models have been defined for different objectives, no publications on resilience or resilient performance using EA (or UAF) exist.

C. URBAN AIR MOBILITY CONTEXT

The concept of UAM involves using small aircraft like drones, air taxis, and other aerial vehicles for transportation within urban and suburban regions. UAM aims to offer a rapid and efficient mode of transportation that can bypass ground congestion, thereby reducing passenger travel times. Electric or hybrid-electric vehicles are being considered for UAM as an attempt to lower emissions and noise pollution in urban areas. Authorities, providers, communities, and vehicle designers are currently engaged in developing strategies for UAM operations. The complexity expected for multiple agents interacting in the urban space poses challenges for the UAM ecosystem. Technical limitations, infrastructure, regulatory considerations, and operational challenges, such as safety, security, noise, environmental impact, and public acceptance are potential barriers to UAM operations [35].

In regards to security aspects of UAM operations for passenger transportation, previous works have started by analyzing the existing security incidents and vulnerabilities of commercial aircraft and UAVs [5], [18], [35]. There are two main sets of operational considerations: 1) cybersecurity considerations relating to control and communication, navigation, and surveillance (CNS); and 2) considerations relating to physical security. Most of the works mentioned previously have contributed to the first set of security considerations. The first set is commonly approached for the in-flight phase and is often related to autonomous operation. In [18], a list of vulnerabilities that can compromise the integrity of the UAM system was provided. The same article evaluates alternatives and potential solutions for protection from the attacks of such vulnerabilities. It is important to note that fully autonomous operation was suggested as one of the solutions for those vulnerabilities.

A similar approach focusing on identifying the cybersecurity and CNS operational risks was presented in [5]. Using the NIST cybersecurity framework [16], the baseline of this analysis was the airspace pillar of the UAM ConOps [2]. Research areas, i.e., CNS, C2 link, and vehicle, were assessed regarding cybersecurity risks. The findings and research guidance showed the importance of performing systemic threat mitigation and adapting to a threat landscape that is constantly changing.

Another work [7] analyzed three types of attacks (via system access, wireless, or sensor attack). It proposed a vehicle recovery system in case of intrusion. The intrusion detection system was considered an important asset to support event detection and trigger recovery after an attack. The unmanned vehicle (and autonomous operations) is also the object of study in this article.

While physical security is not included in most publications, in [35], it was considered an important public acceptance factor. Mitigations suggest personnel and passenger background checks. Concerns about sabotage, terrorism, and violence against passengers in vehicles without crew (autonomous scenario) were also raised. Last, the physical security of the vertiports, aircraft, charging/refueling, other physical infrastructure, and cargo must also be ensured.

The FAA's UAM ConOps [2], [36] describe the envisioned operational environment in phases to support the anticipated growth of flight operations. EmbraerX ConOps [3] also cover this concern with a similar approach, projecting different scenarios with increasing vehicles sharing the airspace and more passengers using UAM transportation. UAM phases were then defined according to the horizons projected. Although autonomous flight is expected to evolve UAM operations, the work presented in this article is based on the early stage of

UAM operations in which the pilot will be on board controlling the vehicle. The proposal presented in Section IV considers the physical security of passengers and crew. Likewise, the physical security of vehicles and infrastructure is also included with the cybersecurity pertinent to the UAM ecosystem. The systematic approach combining UAM ecosystem elements like organizations, personnel, infrastructure, and systems contributes to this article. The purpose is to address existing gaps by exploring a comprehensive viewpoint of cyber and physical security concerns and discuss resilient performance in UAM operations.

III. RESEARCH METHODOLOGY

A. PROBLEM SPACE

Increased airspace traffic, augmented need for communication (with other vehicles and traffic controllers), vertiports in congested urban areas, public proximity to information systems and networks, and reduced and easily accessible crew contribute to a set of vulnerabilities in the UAM operation. UAM security is strategic and vital for UAM safety operation and public acceptance. Manned (and unmanned) aerial vehicles will heavily depend on computers, software, and automation. Organizations will use databases to store sensitive data and share data through networks as providers or operators, making them vulnerable to cybersecurity threats. Ground staff, controllers, and pilots are also susceptible to security risks. Intentional damage to a vehicle or network can target UAM personnel to start an attack.

The problem space in UAM security is an extensive set of elements and concerns. Vulnerabilities of the urban space (easy access and how data will be exchanged near the public areas), vulnerabilities of the personnel involved in UAM operations, risks related to data and information systems, risks to passengers and the pilot, and evidently risks related to controlling and CNS during flight. Threats and attacks can be diversified. Physical assets might be the ultimate target of a malicious event. However, people can be used to achieve an intrusion or even perform sabotage. There are different ways of affecting the confidentiality, integrity, or availability of UAM operations. The problem space encompasses all elements that are associated with those risks.

B. SOLUTION SPACE

Understanding the vulnerabilities more broadly supports a comprehensive approach in the solution space. Security viewpoints, including physical and cyber aspects, must consider different threats and behaviors that lead to a more protective and resilient ecosystem. For a complex operation like UAM, different perspectives are necessary to understand how systems and personnel can act together, not only protecting but adapting and learning from events. A systemic approach is required in the solution of the security problem. UAM operational concepts need to explore the critical functions able to avoid, withstand, and recover from threats. This strategy may be compromised if the solution lacks an ecosystem-level perspective.

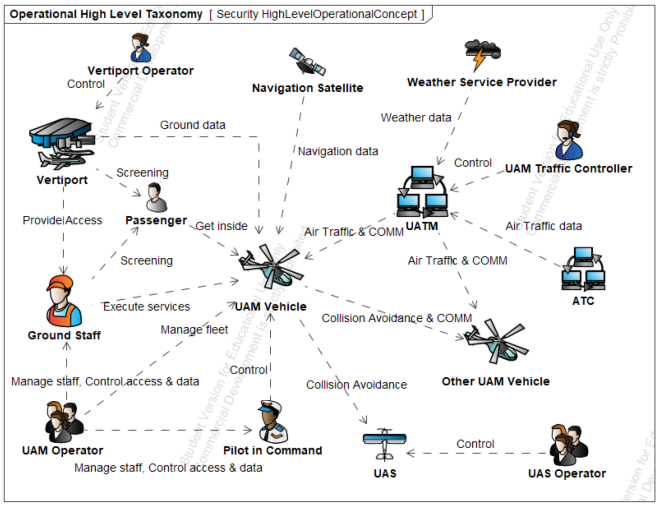

FIGURE 1. Operational high-level taxonomy diagram (St-Sr).

Protective technologies are necessary but not enough to avoid attacks. Operational procedures must be aligned with the daily operations and human operators' performance. Assets are integrated with people and might be vulnerable through this relationship. Fig. 1 depicts the high-level operational taxonomy where the main assets are represented. Identifying and exploring security capabilities by understanding how assets are organized within the ecosystem is the base for a strategic solution. This article's comprehensive solution space embraces security viewpoints and resilient performance in the UAM ecosystem.

C. MODELING METHODOLOGY

Modeling methodologies representing an SoS (UAM ecosystem) is fundamental to providing comprehensive material like the solution space envisions. Modeling eases the burden of dealing with complex systems and provides tools for analyzing behaviors and relationships. Moreover, modeling can systematically represent decision alternatives, evaluate their consequences and tradeoffs, and support decision-making processes [37]. The benefits of modeling methodologies for cross-cutting concerns like security in the UAM ecosystem have been explored in [13]. More specifically, EA and the UAF have been proven effective for building different and complementary perspectives of the UAM ecosystem.

EA is a discipline with a holistic approach to handling an enterprise's intricacies while ensuring that its responses align with its desired business objectives and outcomes [38]. To develop and use enterprise models that include business processes, data, applications, and technology components, an enterprise modeling methodology offers a structure. EA views aim to comprehend the enterprise and its interactions thoroughly. This approach supports the enterprise by aiding decision-making and aligning the enterprise with its strategic

objectives [39]. The framework applied in this article is the UAF, which is built on top of SysML and used to define the overall goals, strategies, capabilities, interactions, standards, operational architectures, and systems patterns [41].

UAF domains' breadth and depth features provide a unified environment for defining security goals, requirements, technical aspects, capabilities, human interactions, personnel organization, roles, and responsibilities. The methodology includes the EA guide for UAF [39], the UAF modeling language [40], and the UAF metamodel [41] specifications. The UAF functions as an EA framework that adheres to EA modeling principles while providing room for adaptability and personalization. However, this methodology has a drawback because it allows for the creation of inconsistent or incoherent architectural elements. To address this issue, validation is strongly recommended, particularly when working with multidisciplinary teams and stakeholders. Another recommended practice is to tailor the modeling process, which can enhance the quality of the work.

Regarding security methodology, the NIST cybersecurity framework [16] is used for defining risk taxonomy, security capabilities, and security controls. The framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. Section IV will present the definitions used for the security viewpoint based on the NIST framework. Section V also considers the same framework when defining ground processes and resilient performance.

This article addresses security viewpoints and resilient performance in the UAM ecosystem. The novelty is the holistic approach applied to cyber, physical, and personnel security, considering potential risks for the future UAM operation. The security state diagram is nonexistent on the current UAF grid [39] and is another contribution of this article. The viewpoints proposed in the following sections consider both technical and nontechnical aspects of security, including human factors and organizational culture. Exploring the ecosystem entities' perspectives provides a means to plan for an integrative, resilient operation.

IV. UAM SECURITY VIEWPOINT

The UAF was created as a combination of the architecture frameworks from the U.S. Department of Defense Architecture Framework (DoDAF) and the British Ministry of Defence Architecture Framework (MODAF). Although DoDAF and MODAF do not provide security views, it was added to the UAF profile. UAF's security viewpoint is based on Canada's Department of National Defense Architecture Framework and the North Atlantic Treaty Organization Architecture Framework version 4.

The UAF security views are intended to depict the security assets, enclaves, constraints, controls, families, and measures required to address specific security concerns. Their objective is to define the security constraints and information assurance attributes that exist on exchanges between systems and operational elements and the elements themselves. The stakeholders who benefit from these views include security architects, security engineers, systems engineers, and operational architects [22].

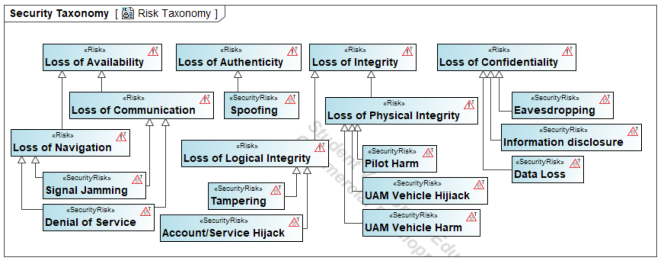

FIGURE 2. Security taxonomy (Sc-Tx).

The diagrams presented in the following sections use UAF version 1.2 [41]. The authors entirely created the diagrams in this article based on the security concepts and aspects discussed in Section II. High-level operational concepts were extracted from existing UAM ConOps [3]. All diagrams were validated by cybersecurity and architecture modeling experts. Consistency and coverage validation were performed using model traceability and verification tools. An example of a traceability matrix is presented in Section V-C.

A. RISK TAXONOMY

The first step in the security architecture elaboration process is defining the security taxonomy [39]. This step includes identifying risks, affected assets, security controls, security enclaves, and security constraints. *Risk* in UAF is a type that represents a situation involving exposure to danger of affectable elements like assets, processes, or enterprise goals. The effects of such exposure can be characterized in terms of the likelihood of occurrence of a given threat and the potential adverse consequences of that threat's occurrence. *Security risk* is a specific type of risk related to the impact on enterprise operations, assets, or individuals resulting from the potential impact of a threat given an information system. This element was defined in UAF according to the NIST cybersecurity framework [16].

Fig. 2 presents the *risk taxonomy* diagram. There are four main categories of risks: loss of confidentiality, loss of integrity, and loss of availability. Loss of availability concerns the disruption of access to, or the availability of, information or an information system. Loss of authenticity is the lack of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or a message originator. Loss of integrity is the unauthorized modification or destruction of the information. Loss of confidentiality is related to unauthorized disclosure of information.

The diagram of Fig. 2 defines generalization relationships between <<Risk>> and <<Security Risk>> in the context of the UAM by the solid line with the white triangle arrow pointing to the generalized risk. Loss of availability was divided into two categories better to accommodate the security

views in the following sections. Either loss of navigation or loss of communication can happen when there is signal jamming or denial of service (DoS). Signal jamming is an attack that blocks or interferes with radio or wireless signals. DoS is when traffic is used to flood a network or server, overwhelming its capacity and causing it to crash or become unavailable to legitimate users. Spoofing is a specialized risk of loss of authenticity. It happens when an attacker impersonates another entity or user to gain access to sensitive information, perform unauthorized actions, or deliver malware.

The loss of integrity can be logical or physical. Logical comprises tampering and account/service hijack, while physical comprises pilot harm, UAM vehicle hijack, and UAM vehicle harm. Tampering is intentionally modifying or manipulating data, systems, or other assets for malicious purposes. An account or service hijack is when an attacker is able to access and control a user account or service without authorization. In the physical integrity, it is possible to harm the vehicle through a malicious attack using physical parts (like sabotage during replacements) or through external connectors during unauthorized maintenance activities. Vehicle hijack refers to the act of taking control of a vehicle for malicious purposes. Pilot harm is when the target is the pilot, which can happen when hijacking the vehicle or affecting the service.

Last, there are three ways to lose confidentiality. Eavesdropping refers to the interception and monitoring of communication between two parties by an unauthorized third party. Information disclosure involves unintentional or intentional exposure of sensitive information to unauthorized individuals or systems. Data loss is when there is unintentional or intentional destruction, deletion, or corruption of digital data.

The main reason for starting with the risk taxonomy is that it prompts the need for security controls and other security aspects. Unlike in systems engineering, where requirements drive system development, in security engineering, the driving force risks [22]. The security taxonomy can be defined after identifying all types and subtypes of risks. It includes the hierarchy of security assets and asset owners available to implement security, security constraints (policy, guidance, laws, and regulations), and details of where they are located (security enclaves). With the security taxonomy complete, it is possible to understand which and how the assets can be affected, how to mitigate them, and, consequently, build the enterprise security strategy. The complete security taxonomy is not depicted due to limited space in the article. Still, in the security structure diagram below, some elements defined in the taxonomy are represented along the relationships between them.

B. SECURITY STRUCTURE

Creating the security structure is the second step. The objective is to capture the allocation of assets (operational and resource, information and data) across the security enclaves and show applicable security controls necessary to protect organizations, systems, and information during processing, storage, and transmission. This view also defines the hierarchy

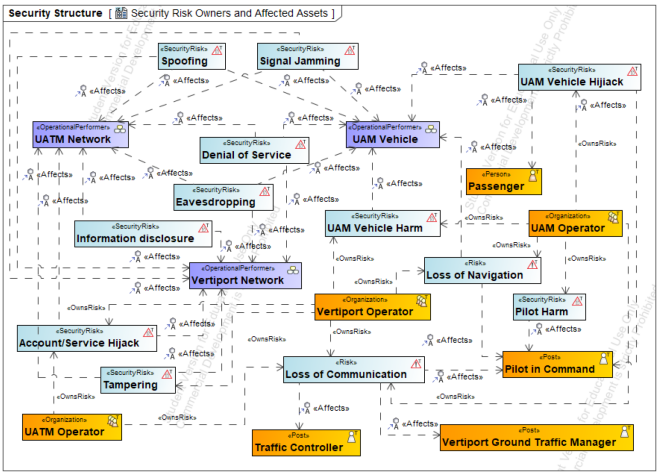

FIGURE 3. Security structure (Sc-Sr).

of security assets and asset owners that are available to implement security, security constraints, and details about security enclaves.

Fig. 3 shows the diagram *security risks owners and affected assets*, which presents an overview of the security risks and the enterprise assets at risk. <<SecurityRisk>> blocks were already defined in the risk taxonomy diagram of Fig. 2. There is *loss of communication* and *loss of navigation*, general classifiers of *signal jamming* and *DoS*. Furthermore, there are more specialized risks like *spoofing*, *signal jamming*, *eavesdropping*, *information disclosure,* and so forth. From the asset representation perspective, there are elements from the operational domain like the <<OperationalPerformer>> blocks and from the personnel domain like <<Organization>> and <<Post>> blocks.

The resource layer in this diagram aims to point to risk owners and assets affected by threats related to the risks. In the UAM ecosystem, three main operators share space and work with interdependent processes. The <<Organization>> *vertiport operator* is responsible for managing and controlling the vertiport facility, which includes takeoff and landing pods, embarking/disembarking area, maintenance area, and battery recharging area. It also provides ground communication and surveillance. <<Organization>> *UAM operator* is the organization responsible for the travel service, owns the vehicle, provides the flight plan, passenger and crew list, and is responsible for vehicle maintenance and operations. <<Organization>> *UATM operator* is the service provider responsible for integrated airspace traffic management, including providing authorizations and airspace awareness.

When it comes to risk ownership in complex operations like in UAM, having a single entity is not always simple and straightforward. The <<Security Risk>> UAM vehicle harm, for instance, is a risk owned by the asset owner and shared responsibility with the vertiport operator, since, most of the time, the vehicle will occupy the vertiport facilities. The same applies to loss of communication or any other risks

affecting networks. Losing or using a compromised communication link is a risk that affects all three operators. Despite not showing the relationship <<OwnRisk>> to all of the risks (to keep the figure's clarity), it is expected that operators share the ownership and responsibility.

There are also two levels in the personnel elements. The <<Organization>> *UAM operator* owns integrity risks that affect people and vehicles. However, the <<Post>> pilot in command is part of the *UAM operator* organization. The vulnerability of the pilot is represented by different risks affecting the post in different operational phases. Single pilot operation is expected in the early phases of the UAM services. Planning for the pilot's security is crucial. The organization-level effort should be considered when protecting and preparing for responding to events. The ground operation explored in Section V further explains the security controls and mitigations related to the pilot's vulnerabilities.

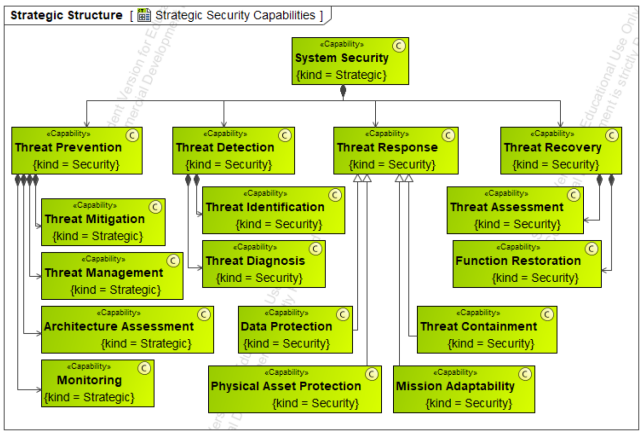

FIGURE 4. Capability structure (St-Sr).

C. CAPABILITY STRUCTURE

Capability is a high-level specification of the enterprise's ability to execute a specified course of action [41]. In DoDAF, a capability is further described as the ability to meet performance standards and conditions by combining activities and resources to achieve the desired effect. Defining capabilities is crucial to architecture conceptualization because it is closely related to operational, resources, personnel, and services definitions. The system's purpose and the model's objective can be understood by defining architecture capabilities.

UAF offers a set of views for defining capabilities. Traceability and association relationships can be established across different views, including the operational architecture. The operational architecture provides a solution-independent expression of the system intended to be used during operations. Thus, the system views can determine how the capabilities and operational architecture will be realized [22]. The strategic taxonomy view is used to identify all the capabilities referenced across one or more architectures. It can create high-level use cases and user requirements as a source document. The strategic structure can be used to show the relationship between the capabilities, and the strategic connectivity describes the dependencies between planned capabilities.

The next step is defining capabilities to achieve a secure and resilient operation after identifying the risks and security structure. Fig. 4 shows the structure organized from the top-level capability of *system security* using composition and generalization relationships. The composition notation is the solid line with the tail attached to the part and the black diamond arrowhead attached to the whole. Composition relationships demonstrate that it is necessary to fulfill all four capabilities to achieve system security: *threat prevention*, *threat detection*, *threat response*, and *threat recovery*. These parts were defined considering the NIST cybersecurity framework [16] functions and then tailored to explore security views and resilient operation in the UAF model. These functions are identify, protect, detect, respond, and recover. The functions assist an organization in articulating its approach to managing cybersecurity risk by structuring information, facilitating risk management decisions, mitigating threats, and enhancing its practices through learning from prior experiences.

Threat detection (second block from left to right in the second line) is about the ability to identify and diagnose threats. It has two parts represented by the capabilities *threat identification* and *threat diagnosis* (the two blocks below the *threat detection*). *Threat identification* refers to the mechanism of detecting an event. A good performance of this capability is not only to detect known or expected threats but to bring awareness when something does not seem right, even about unknown threats. *Threat diagnosis* is about knowing the threat profile, where and how the event threatens the system's health, which is essential to address a more effective response.

Threat response (third block from left to right in the second line) can address protection or contingency measures to respond to a threat. The generalization arrow links four types of responsive capabilities. Protecting the system provides a means to avoid attacks getting adverse outcomes in the system. Two possible types of assets in the security domain require two protection types: *data protection* and *physical asset protection* (blocks below the *threat response* on the left side). *Data protection* refers to the protection of logical data exchanged by the UAM system. *Physical asset protection* is related to physical and environmental security, such as operational procedures. Contingency is about the ability to control attacks to the most negligible effect possible. There are two ways of doing it (blocks below the *threat response* on the right side). *Threat containment* refers to isolating the attack or controlling its boundaries to minimize its functioning or make it harmless eventually. The other way of contingency is *mission adaptability*. Inactivating the area where the attack harms and adapting the system's mission also makes it possible to control the threat. System redundancy is a good example of contingency by adapting the mission.

Threat recovery (the last block from left to right in the second line) is a combination of *threat assessment* and *function restoration* (blocks below *threat recovery*). It is about the ability of the system to resume a safe operation after a threat occurs and generates outcomes to the system's normal functioning. *Threat assessment* includes the reconnaissance and analysis of the threat, assessment of the potential harm, and additional vulnerabilities. This assessment is needed to restore the function initially affected by the threat. Therefore, *function restoration* refers to the measures necessary to restore the system's operation. These measures have a high level of variability and depend on what type of attack occurred and how was the sequence of events and facts. The organization and systems are expected to be able to assess threats and have the flexibility to act toward recovery.

Threat prevention (first block from left to right in the second line) was proposed to address risk management and the capability to assess the architecture and promote adaptation in the face of events. In order to know events, system monitoring is essential. After events occur, with or without adverse outcomes, it is important to manage them by controlling and performing assessment (threat management). These activities can lead to an architecture assessment or a new/improved mitigation plan (threat mitigation). The four capabilities composing threat prevention are not independent or linear parts that occur as a simple flow of actions. Their behavioral aspect is highly coupled with other capabilities in the diagram.

The proposed representation in Fig. 4 results from iterative work during the definition of mitigations, security controls, security state, and processes. Allocations to capabilities in further diagrams are a method to verify coverage and consistency. It allows the architecture designer to revisit definitions and best accommodate the representations. Moreover, the UAF views allow traceability relationships from resources and processes to capabilities. The following sections provide a few examples of how this model feature can support the architecture to achieve the desired security effect.

D. SECURITY STATES

Motivated by the strategic state view, used to capture effects that the implementation of capabilities is expected to deliver, a security state view is proposed in this section. The existing UAF grid [41] does not provide the security state view. The security viewpoint is limited to taxonomy, structure, motivation, connectivity, processes, constraints, and traceability. The security state diagram in Fig. 5 intends to identify the states related to RE: avoid, withstand, and recovery.

Given the unavoidable circumstance of facing evolving threats, protection is not a real and viable solution for the entire ecosystem (assets and operations). How an organization or system can cope with threats, recover, and learn from them? How do we transition from an undesirable state into a controlled one? In which process should the effort be strengthened? Are the defined capabilities coherent with the security states transitions and behaviors? Those are questions that drive the diagram in this section.

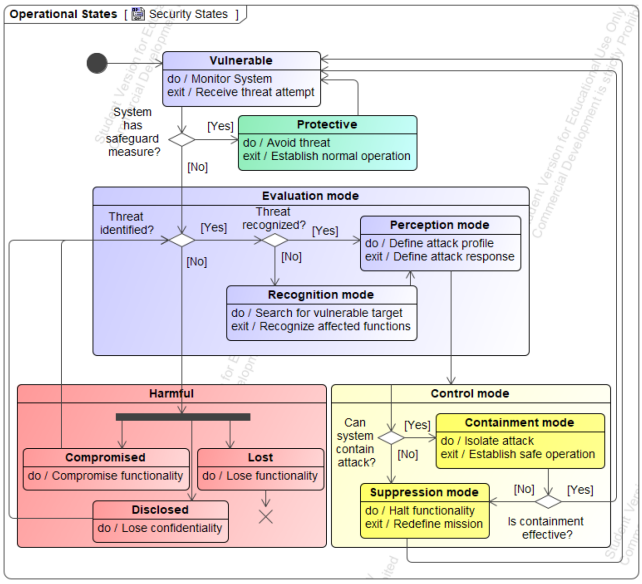

FIGURE 5. Security states.

The first state, applicable to all systems and operations, is vulnerable (the first state at the top). Risks, hazards, and threats are inherent in any system. Safety and security are dynamic properties that complex systems must be designed to handle. Furthermore, recognizing that humans are an integral part of ecosystems and that their abilities and limitations must be taken into account in designing and managing systems is one of the resilient engineering principles [10]. This state requires continuous and real-time monitoring, which traces to the capability of monitoring (bottom left block in Fig. 4). The *monitoring* capability is an extensive ability that comprises physical, logical, and personnel entities.

When a threat is attempted, the best transition would be to a protective state (second state from top to bottom in Fig. 5). It means the system is adequately prepared to avoid the threat. *Data protection* and *physical asset protection* capabilities are related to this state (bottom center blocks in Fig. 4). *Protective* is a desirable state because it returns to normal operation without causing any adversity to the system. Data encryption, firewalls, verification layers, and controlling authorized access are examples of protecting data and physical assets.

When the system does not have effective protection upon a threat attempt, it transitions to the *evaluation mode* state (center state). Detecting a threat starts with knowing if an event happened and then recognizing its profile. *Threat identification* and *threat diagnosis* capabilities (from Fig. 4) allow the *perception mode* substate (right side state inside the *evaluation mode* state) to define the attack profile and search for a response. If the system is not able to recognize the threat event knowing the existence of the attempt, the other substate possible would be *recognition mode* (bottom state inside the *evaluation mode* state). The flow within the *evaluation mode* state shows the system's importance in being prepared for

monitoring and performing screening during an attack. Furthermore, the capability *threat assessment* is also related to both substates within the *evaluation mode* state.

The control mode state (bottom right state) is entered when the threat is acknowledged and the response is known. The first option for controlling the threat is isolating the attack and resuming safe operation. If the system has means to contain the attack, the containment mode substate (right side state inside the control mode state) is activated. Suppose the strategy is not effective, or the system does not possess the containment means. In that case, the suppression mode substate (bottom state inside the control mode state) is also a possibility. The other way of controlling the attack is by redefining the mission and halting the functionality that is being attacked. Redundancy of resources or suspending operations are examples used to suppress the threat. The *control mode* state represents the measures to withstand or to respond to an attack. The state is associated with capabilities like *threat containment*, *mission adaptability*, and *function restoration* (Fig. 4).

If the system cannot detect any event, the transition moves to the harmful state (bottom left state). This state is the most undesirable in the diagram. Not knowing a threat occurred can lead to catastrophic events. Once the state is active, there are three possibilities. Compromised substate (left side state inside the *harmful* state) is when the threat affects one or more functionalities. Operating without knowing the system has compromised integrity and can bring unsafe outcomes. Disclosed substate (bottom state inside the *harmful* state) concerns the unauthorized disclosure of confidential information. Disclosing unauthorized data can range from jeopardizing national security to disclosing private customer information. For instance, if a flight plan is disclosed, it can facilitate other attacks with worse outcomes or even affect the organization's reputation and business. The third state is lost (the state on the right side inside the *harmful* state) and symbolizes when functionality is wholly lost. If an attacker can take control of a system and shut it off without being noticed, it can also bring catastrophic effects. Compromised and disclosed states can transition to control mode again. The system can and should detect the threat even after some time has passed since the first attempt. This could lead to the threat diagnosis and eventually a recovery and learning behavior.

The harmful state represents the risks being consolidated in a real fact. The lost state is associated with the risk of loss of availability (from Fig. 2). The disclosed state can represent an event that produced a loss of confidentiality or a loss of authenticity (risks from Fig. 2). Last, the compromised state is when the risk of loss of integrity or loss of authenticity happens. Loss of authenticity is a risk that occurs in both states because losing confidence in the validity of a transmission, a message, or a message originator can also compromise the system's functioning.

The state diagram is proposed to represent the primary states and the common transitions. Some specific behaviors or transitions require a more elaborated logic between states and substates. There are cases in which the threat attempt would be detected, and still, the protection exists and is effective. However, some protection systems avoid threats without recognizing attack attempts. Another example of a situation not detailed in the diagram is when an attack can hit different targets and present different profiles. This scenario could lead to controlling part of the threat and keep trying to evaluate another part. When the harmful state is active with compromising functionality for a while, and the system can detect the event, the diagram transitions to the control mode state. However, irreversible harm could have been done, and the controlling state would deal only with new targets.

The state diagram has limitations. Security states experience complex transitions and require more depth to cover various scenarios. Triggers and effects in security states can compel more elaborate notations. Nonetheless, the level of detail to increase the coverage of the diagram would affect the visualization and compromise the understanding aimed at this article. The intended purpose of Fig. 5 is to support understanding of how a system or organization can behave while facing its threat landscape. As presented in Section V, the diagram helped define functions, mitigations, and processes.

V. RESILIENCE IN GROUND OPERATION

The security motivation and taxonomy views define *which* security control and risk mitigations are necessary. The UAF security process (Sc-Pr) view addresses *how* security controls will mitigate risks. Functions, processes, and resources are aggregated to elaborate the structure and behavior of the processes. *Security resource performers* comprise mitigations and security enclaves. Mitigations can be defined as resource elements or operational activities. *Functions* performed by those security resource performers will perform an *Sc-Pr* that implements *security controls* for protecting enterprise assets to *mitigate* expected *risks*. Different views can describe operational behavior, structure, and exchanges required to exhibit capabilities.

The security architecture is often viewed as primarily concerned with safeguarding assets. This involves implementing security measures that align with established security control tactics, techniques, and procedures, as well as adhering to relevant security policies, directives, and limitations. Mitigations for operational and resource security can be defined and implemented to achieve these objectives [39]. Despite the need to protect various assets, the security architecture must also provide countermeasures and means to withstand and learn from events. This section will focus on the UAM ground scenario to discuss how Sc-Pr supports resilient operations.

A. GROUND SECURITY PROCESSES

The first Sc-Pr diagram (Fig. 6) presents the functions necessary to perform mitigations. After the security structure and motivation were clear, security controls were defined to mitigate risks related to the ground operation. A *security control* (as the first line of blocks with the notation <<SecurityControl>>) is a prescribed safeguard

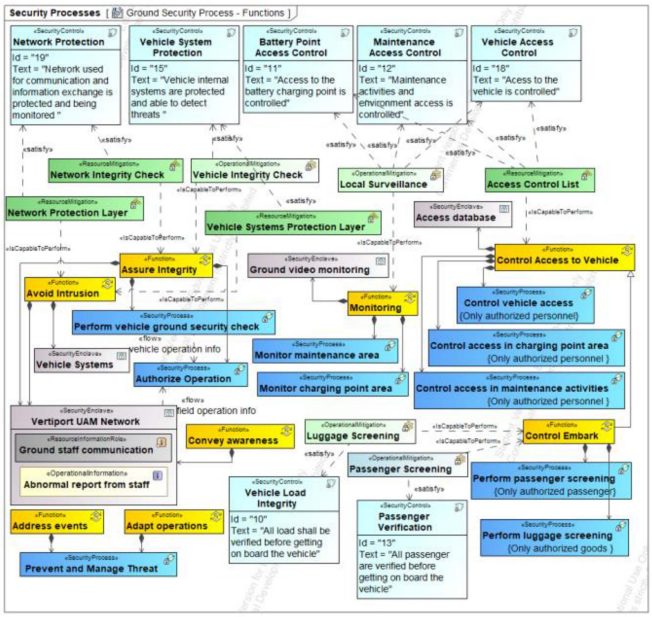

FIGURE 6. Security processes (Sc-Pr)—functions view.

or countermeasure for an information system to protect the confidentiality, integrity, and availability of the system and its information. In this step, the environmental context and the high-level operational concept are considered to have coherent security controls. In the diagram below, the security controls are satisfied with one or more mitigation elements. Below the <<SecurityControl>> blocks are the mitigation blocks defined for satisfying the security controls. <<ResourceMitigation>> represents a set of resource performers intended to address specific risks. <<OperationalMitigation>> represents a set of operational performers intended to address specific operational risks. In other words, it is possible to define mitigation based on function performance or operational activities.

The security control network protection (top left block) is satisfied by two mitigations: network integrity check and network protection layer (blocks under network protection). They are digital resources to enhance network protection. The purpose of these resources is to protect and monitor the network, as stated in the security control text. Vehicle system protection (second block from top left to right) is a security control requiring two different mitigation types. Like the network protection layer, the <<ResourceMitigation>> *vehicle system protection layer* is a digital resource that protects the vehicle's interfaces. In addition, an operational mitigation element is needed to satisfy the security control completely. The <<OperationalMitigation>> vehicle integrity check is a set of elements (personnel, process, and systems) performing an activity.

Two key functions are common to the security control and mitigations mentioned above. Avoid intrusion is a <<Function>> (block on the center-left side) performed by the network protection layer and vehicle system protection layer, two different resource performers. Assure integrity (block near avoid intrusion) is performed by network integrity check and vehicle integrity check, a combination of resource and operational elements. When defining which processes deliver the function assure integrity, there are two Sc-Pr and one security enclave. A <<SecurityEnclave>> block represents a collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The <<SecurityEnclave>> vertiport UAM network (big block on the left side) is a network for communication and information exchange. Integrity checks must be planned within the network and can be further detailed in the resource architecture. *Perform* vehicle ground security check (<<SecurityProcess>> block in the center-left side) is a process to ensure that the vehicle is intact and nothing is affecting its integrity. Last, the Sc-Pr authorize operation (block below the *perform* vehicle ground security check) is the last integrity check before vehicle takeoff. It represents a comprehensive vision of the ground operation and is described in the activity diagram in Section V-B.

The same process of defining functions performed by mitigation elements was done for the other security risks. Access to the vehicle on the vertiport facility is a sensitive aspect of the security properties on the ground operation. Concerns with unauthorized access during maintenance or battery recharging are legitimate, considering how the vehicle is vulnerable to malicious attacks. The vertiport is expected to settle in urban areas surrounded by the public and where the space is limited.

Another concern is regarding passengers and the embarking process. As a single crew, the pilot is exposed and vulnerable in the vehicle. A pilot or vehicle hijack is not locally constrained by protecting the crew with a cockpit door. Commercial flights count with airport security barriers, checking crew, passengers, and luggage through a series of processes and resources. However, the time spent in the embarking process, from when the passenger arrives at the airport to take off, is long and can take hours. Considering UAM flights are short (not more than 60 min), it may not be practical, or even acceptable from the business perspective, to have a long embarking process. Security and passenger experience must be considered in the ground operation. Current discussions are taking place to find a suitable solution for the UAM stakeholders. Regulatory authorities have yet to decide the ground standards for vertiport and UAM operations. Suppose authorities apply a similar approach to helicopter flights, where private transportation does not require passenger or luggage screening. In that case, it is important to understand the accepted risks and consequences. Alternatively, loyal passenger programs are also being discussed in a way to reduce the risk and still have a more agile embark and attractive transportation service.

The Sc-Pr view is also used to introduce personnel elements and define which resource (who) is capable of performing which Sc-Pr (what). The diagram in Fig. 7 shows an example of the relationships between Sc-Pr, security enclaves, organizations, posts, and capabilities. Processes are mapped

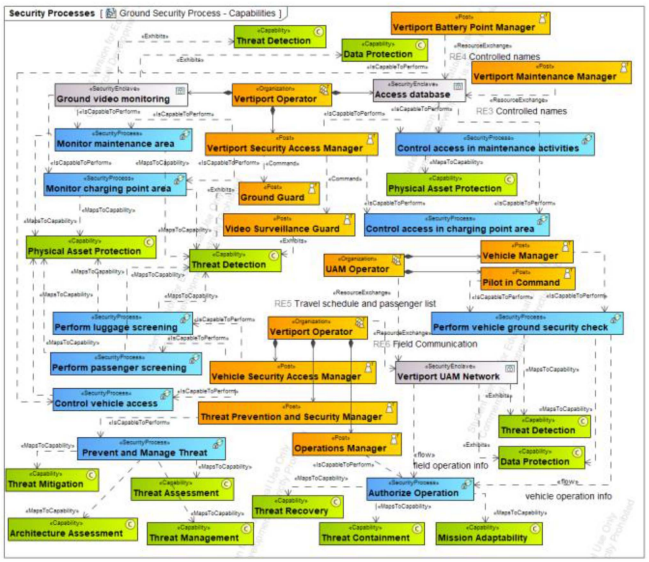

FIGURE 7. Security processes (Sc-Pr)—capabilities and posts view.

to capabilities supporting the model's consistency with the enterprise's taxonomy.

Relationships within the personnel domain are explored to represent different organizational levels performing Sc-Pr. Resources like organizations, posts, and security enclaves *perform* Sc-Pr. Fig. 7 shows blocks <<Organization>> and <<Post>> (blocks in the center) linked to <<SecurityEnclave>> (same blocks defined in Fig. 6 and presented in Fig. 7). The dotted line with the notation <<IsCapableToPerform>> shows the resources' capability of performing processes. At the organization level, the <<Organization>> vertiport operator (block in the top center in Fig. 7) is composed of posts (staff) and security enclaves like ground video monitoring and access database. People and systems are capable of performing Sc-Pr at different hierarchy levels. For instance, the <<Post>> vertiport security access manager (block below vertiport operator) is the element responsible for the processes monitor maintenance area and monitor charging point area (<<SecurityProcess>> blocks on both of its sides). Still, two posts are commanded by the security access manager: ground guard and video surveillance guard (<<Post>> blocks below vertiport security access manager). The combination of the entities linked to the mentioned Sc-Pr will exhibit the capabilities of physical asset protection and threat detection (<<Capability>> blocks in the center). Each post's responsibilities can be defined in detail, considering the structure and behavior explored in the process view. The UAF personnel viewpoint organizes data about organizations, posts, and responsibilities.

Resource exchange is another essential definition in this step. Identifying and understanding the exchange between resources is crucial for detailing the process flow of each Sc-Pr. The security enclave access database can only perform the Sc-Pr control access in maintenance activities if it receives the proper controlled names (RE3 and RE4 on the top right of Fig. 6) from posts vertiport battery point manager and vertiport maintenance manager. The definition of the resource exchange can result in systems requirements, operational performance, or personnel responsibilities.

In the ground scenario, the effort for monitoring and safeguarding the environment is more evident. The resources, functions, and processes focus on protecting the vehicle as the ultimate sensitive asset. Since the vehicle is on the ground, the ecosystem's behavior to secure the operation differs from during flight, when time is a critical resource. On the ground, the most critical boundary to avoid unsafe scenarios would be the flight authorization of an insecure vehicle. Most countermeasures and prevention rely on organizational processes and people's behavior. To address this scenario, the process authorize operation (block on the bottom right in Fig. 6) has its flow detailed in the following section.

B. GROUND SECURITY PROCESS FLOW

UAF Sc-Pr flow diagram represents the flows within an Sc-Pr. The security behavior of the architecture can be defined, including process flows and their security measures of performance. Fig. 8 shows an activity diagram to represent the behavior of the authorize operation Sc-Pr. The activity diagram describes operational or resource-level processes that apply (operational level) or implement (resource level) security controls to assets. In addition, the input and output for each action are specified consistently with the resource exchange defined previously.

The core process for *authorize operation* is represented in the last column from left to right in the diagram of Fig. 8. The performer of authorize operation is the post operations manager (<<Post>> in the header of the last column from left to right). The activity starts in the initial black dot and follows the control flow (dotted line) inside the swim lane allocated to the operation manager. The first actions are related to context awareness and happen in parallel. Monitor ground operation, confirm vehicle integrity, and confirm embark integrity (<<OperationalActivityAction>> blocks) are actions that depend on other performers' information. The vertiport UAM network (<<SecurityEnclave>> column left to operations manager's column) is a central resource in this scenario. Its function is to provide operational awareness (<<FunctionAction>> block in the same column) to the operation manager. Additionally, there is a resource action of provide ground network and report threat in the network (blocks without notation in the same column) performed by the network itself. All other posts perform the <<FunctionAction>> report any event using the network as a communication resource.

Some actions are directly related to other Sc-Pr. The allocation of the elements <<SecurityProcessAction>> into posts using swim lanes is consistent with the Sc-Pr view in Fig. 7. The relationship between resources and processes was defined in Fig. 7 with the notation <<IsCapableToPerform>>. For instance, the <<SecurityProcessAction>> *prevent and*

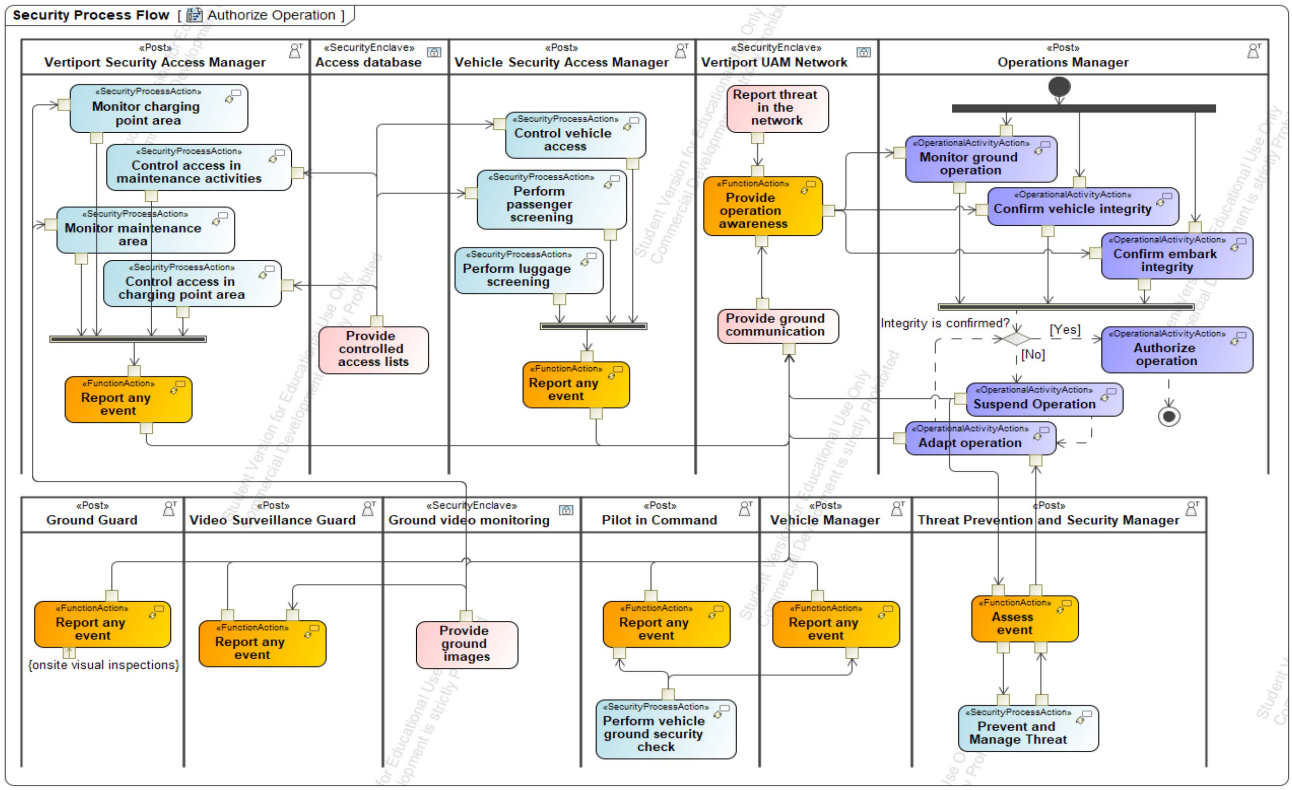

FIGURE 8. Security process flow (Sc-Pr).

manage threat allocated to <<post>> *threat prevention and security manager* (bottom right column in Fig. 8) is an action resulting from the Sc-Pr *prevent and manage threat* (depicted in the bottom left of Fig. 7). Last, resource actions (blocks without notation) are provided by security enclaves, like provide ground images and provide controlled access list.

The process flow performed by other posts is detailed in different diagrams. When all processes are defined, the output and inputs can be specified and called references among processes. The representation above is a sample of how different processes are related and dependent on each other. Using different elements to show the contribution of other resources in authorize operation was intentional. <<SecurityProcessAction>> <<FunctionAction>>, and resource actions are possibilities to explore the behavior of Sc-Pr flow. Sc-Pr flow can and should be tailored to present the intended perspective.

The activity diagram of Fig. 8 shows the extent of the operation awareness necessary to authorize a flight operation. Without the performance of posts realizing other processes and reporting events, the integrity of the ground operation could not be confirmed. Resources (staff and systems) are working to monitor and control the environment. Identifying threats is a collective and integrated performance. Using views with higher abstraction levels helps understand the ecosystem behavior toward the security goal. In addition, the usage of the process flow view includes requirements capture, the definition of roles and responsibilities, support task analysis to determine training needs, operational planning, and information flow analysis.

C. RESILIENT PERFORMANCE ON GROUND

The security architecture elaboration presented at this point, starting from risk taxonomy (Fig. 2) until the structure and behavior of security processes (Figs. 6–8), is an iterative and recursive process. The analysis to achieve and sustain resilient performance supports the architecture elaboration. At the same time, the architecture resources affect the ability to perform resiliently, enabling and enhancing it in the best case. Resilient ecosystems are able to respond, monitor, learn, and anticipate adverse conditions. Additionally, resilience must be managed, which requires more than just monitoring and learning about the system. It also involves considering how the world responds or changes in response to the system's modifications and how these responses may impact the changes made. This recursive form of anticipation is the highest level of resilience management and must be considered to ensure optimal outcomes [42]. To address resilience in the ground operation scenario, the security states of Fig. 5 presented in Section IV-B were used as a reference to understand how the UAM ecosystem can avoid undesirable states or transition into controllable states.

Two high-level functions are associated with the protective state in ground operation: avoid intrusion and control access to the vehicle (<<Function>> blocks on the right and left sides of Fig. 6). The first means that networks, information systems, and vehicle systems must be protected against malicious attacks and intrusion attempts. Systems and technologies can be designed to perform the protection for this case. Resource architecture details the measures defined for security protection. The other primary function is related to direct contact with the vehicle. The vehicle needs physical protection while on the ground as a physical asset. Sabotaging during maintenance, dangerous loads, unauthorized pilots, or malicious passengers are threats to flight operations. Controlling the embarking process is a way of controlling vehicle access and requires luggage and passenger screening, verification of pilot authorization, and local surveillance.

Monitoring in ground operations is a critical and central function necessary for evaluating threats. The Sc-Pr and, consequently, the people involved in the ground operation are organized to monitor and report events effectively and efficiently. The action *monitor system* in state *vulnerable* of Fig. 5 represents the system's monitoring capability. Without monitoring, the system remains vulnerable. The monitoring performance can also identify and recognize threats in the ground operation scenario. The human aspect, safety culture, and organizational culture lead to the monitoring performance and detection capability. Communication resources like the vertiport network and process adherence support the monitoring behavior. Another function is associated with the monitoring effort: assure integrity (<<Function>> block on the center-right of Fig. 6). When the vehicle performs preflight checks, or the operation's manager checks the integrity of other processes, an ultimate effort is made to monitor the environment and detect possible threats. Therefore, if the ground monitoring performance is deficient, the evaluation mode state cannot move to the control mode state and avoid the harmful state as presented in Fig. 5.

Regarding controlling threats, the ground scenario responds differently than the flight operation. The ground staff is not as pressured by time as a pilot during a flight. There is always a possibility to suspend operations until safety is restored. The authorize operation process flow demonstrates how the organization can contain or suppress threats. If the integrity is not confirmed, the operation is suspended until the mission can be adapted and restored. The possibility of suspending the operation gives time to the organization assess the threat and respond to it safely. The same may not be possible during the flight. In extreme circumstances, the flight could go to an emergency state and land as safely as possible.

The *prevent and manage threat* process (<<Security Process>> block on the bottom left of Figs. 6 and 7) supports assessing the threat during operation. An organized and effective risk prevention and management structure is the foundation of resilience. Planning is crucial to understanding risks and responding properly. Monitoring and assessing is the key to learning about the effects on the

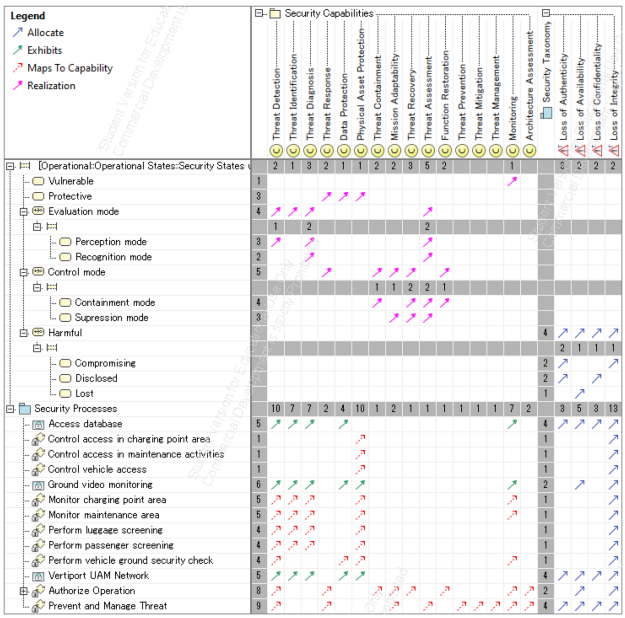

FIGURE 9. Security traceability matrix.

operation. Monitoring is a capability that is exhibited collectively and depends on staff behavior and culture. Constantly adapting to the changes in the environment and anticipating them is necessary to reach the outcome desired by this process. Anticipation is only possible if the system's behavior is known through monitoring activities and with the engagement of the people involved in those activities.

Situation awareness, already addressed in the UAM safety context [13], is essential for achieving security. As a collective cognitive process distributed at different enterprise levels, sharing information about events can improve the response capacity of the organization. Resilient performance is also related to nonsecurity events. Learning from actual operation (work as done) can improve security and safety efficiency and make opportunities evident. Active management enables the learning and anticipation capability of the ecosystem. The action common to all posts in the activity diagram in Fig. 8 is to report any event (<<FunctionAction>> elements). Training people to observe and report all sorts of events, even nonthreat or harmless events, can improve the capability of monitoring and provide means to assess opportunities and actual threats.

A system can be considered resilient if it has the ability to adapt its performance before, during, or after events, such as alterations, disruptions, and opportunities and, as a result, maintain necessary functions even in predicted or unforeseen circumstances. Security states, in conjunction with capabilities, provide a reference for analyzing the Sc-Pr coverage and verification in terms of resilience. The abstraction of capabilities can be refined with the behavior of security state transitions. The state diagram's narrative can serve as a background scenario for defining effective processes. The

matrix in Fig. 9 shows the security traceability between states, processes, risks, and capabilities.

The top part of the matrix is how the states relate to capabilities and risks, as explained in Section IV-D. The relationship used to trace the states to capabilities is the realization (pink arrows). Realization is a specialized abstraction relationship between two sets of classes, used in this case for model stepwise refinement. States and risks were traced using the allocate relationship (blue arrows), a mechanism for associating elements of different types or hierarchies at an abstract level. The harmful state is the only tracing to risk element because it represents the consolidation of all risks. All other states are associated with detection, protection, response, and recovery capabilities. Some capabilities from the prevention structure are not traced to any security state. This gap was significant in defining the ground processes.

The bottom part of the matrix shows the relationship among Sc-Pr, capabilities, and risks. Security enclaves *exhibit* capabilities (green arrows), while the Sc-Pr is mapped to capabilities (red arrows). The strong presence during threat detection and protection is coherent with the ground scenario. Controlling measures rely on the *authorize operation* process, given that monitoring and threat detection were realized. The *prevent and manage threat* process was created to combine field information with proper assessment and support the responding capability.

Furthermore, as discussed earlier, risk prevention (with response planning and enablement) and resilience management must be performed. The *prevent and manage threat* was simplified in the diagram as a single process. However, it represents an integrated and complex operational process. The *prevent and manage threat* process represents the enterprise's mechanism to manage security states and achieve security goals. Protection, or using the *protective* path (from *vulnerable* to *protective* state in Fig. 5), can only happen if the enterprise is constantly monitoring and spending resources to assess threats and avoid them preventively. Using the *evaluation mode* state to improve the detection capability and learn from threat behavior is driven by the same mechanism. Likewise, the *prevent and manage threat* process enables containment and suppression measures; consequently, the ability to control threats is possible. Besides, the resources and process definitions involved in preventing threats, cultural aspects, and individual behavior must be included if the organization needs flexibility and constant learning.

The allocation to risks on the bottom represents which processes or security enclaves are actively working to avoid or contingence the risks. *Loss of integrity* (risk defined in Fig. 2) is the primary target due to the nature of the ground operation. The availability can always be affected if the integrity is not confirmed. However, business interruption is less critical than ensuring safe operation.

VI. CONCLUSION

RE takes a holistic view of organizational functioning. This article used the UAF viewpoints to address security and resilience in UAM operations. The elaboration of the security structure started with the risk taxonomy and how the enterprise can build its security strategy once the affected assets are defined. Before integrating the resource architecture, the security capabilities were discussed and proposed according to resilience principles. Since UAF does not provide a security state view, this article proposed a diagram with agnostic security states. The second part of this article focused on the UAM ground operation to define Sc-Pr and process flow. Finally, resilient performance in the ground operation was discussed using the security states and traceability matrix.

During the process of determining security controls and mitigations, the strategy must be comprehensive to address different scenarios and vulnerabilities. The UAM ecosystem has multiple service providers and operators sharing spaces and operational processes. The perspective necessary to define operational and resource mitigations must include personnel, infrastructure, and daily operation processes. Vulnerabilities are inherent to the ecosystem and are not exclusive to digital or physical systems. Processes and people are also vulnerable and must be included in the holistic approach.

Regarding the ground scenario, the article demonstrated that monitoring and controlling the environment is crucial to protecting assets at the vertiport. The most evident asset is the vehicle, which is vulnerable and can be the main target of different malicious attacks. The vehicle is also the most safety-critical asset that can lead to catastrophic outcomes. Nonetheless, all the people engaged in the UAM operation is also a target that can be used to attack the vehicle. The mitigation and processes must consider the ecosystem as a complex and integrated environment. The resources used to convey awareness, like the vertiport network, must consider the mission of reporting events by the ground staff. The effectiveness of this behavior will drive the capacity to detect events and respond efficiently. Functions in the security mitigation strategy must be included in the early stages of the system design.

An organization's resilience can be assessed by examining its response, monitoring, learning, and anticipation capabilities. These four fundamental capabilities should be viewed in combination rather than individually. The integration and dependency of processes and resources involved in resilient capabilities were explored using EA views. The resilient performance in ground operation was discussed and proposed using the security viewpoint. Furthermore, it addressed not only capabilities to handle threats as disturbances but also opportunities to learn and constantly adapt. Last, resilience management was discussed in the UAM ground context, providing means to plan for productive safety. It is essential to allow the ecosystem to learn from opportunities instead of only focusing on protecting assets against threats.

The UAF has accomplished the modeling purpose of defining UAM security viewpoints. The model was updated multiple times during the study. Discussions and validations with experts, iterations, and recursion among views resulted in the abovementioned diagrams. The success of the modeling

effort was measured by achieving views with coverage, coherence, and consistency. Moreover, the model has supported the process elaboration to support UAM's resilient performance. Besides, the personnel and operational viewpoints, the UAF provides a security viewpoint with elements ready to use or customized according to the modeling effort. The relationships offered by the metamodel can provide a link among viewpoints and be used for traceability and verification.

Physical and human resources are not the only ways to address security. To establish robust security measures, exploring other dimensions of the solution space, such as doctrine, organization, training, material, leadership and education, personnel, and facilities, is essential. The breadth and depth of the UAF can be explored according to the model effort strategy. The following steps on the coverage include other scenarios like during takeoff, cruise, and landing. In-flight operations can be explored with different configurations to focus on the loss of communication and navigation or other categories of risks.

Regarding the depth of the model, the next steps include defining measures of security performance, detailing security enclaves' structure and connectivity, and specifying resources concerning technologies and exchanges. The UAF features a viewpoint called actual resources that accurately represents tangible assets in real-world operations. Additionally, the model offers a user-friendly approach to managing complex and interconnected data. Users can employ various tools, such as tables, diagrams, hierarchical views, matrices, and relation maps, to analyze how various enterprise components are interconnected. Finally, the UAF provides a valuable modeling framework for exploring cross-cutting concerns like security, safety, and resilience.

REFERENCES

[1] Annex 17 of the Chicago Convention of the International Civil Aviation Organization (ICAO), 12th ed., Jul. 2022.

[2] Urban Air Mobility (UAM) Concept of Operations 1.0, Federal Aviation Admin., Washington, DC, USA, 2020.

[3] Urban Air Traffic Management Concept of Operations version 1.0, Air Service Australia and Embraer Business Innovation Center, 2020.

[4] L. Ribeiro, S. Giles, R. Katkin, T. Topiwala, and M. Minnix, "Challenges and opportunities to integrate UAS in the national airspace system," in *Proc. Integr. Commun., Navigation Surveill. Conf.*, 2017, pp. 6C3–6C1–6C3–13, doi: 10.1109/ICNSURV.2017.8011942.

[5] A. Jordan et al., "Systematic evaluation of cybersecurity risks in the urban air mobility operational environment," in *Proc. Integr. Commun., Navigation Surveill. Conf.*, 2022, pp. 1–15, doi: 10.1109/ICNS54818.2022.9771507.

[6] M. Cenk Ertürk et al., "Requirements and technologies towards UAM: Communication, navigation, and surveillance," in *Proc. Integr. Commun., Navigation Surveill. Conf.*, 2020, pp. 2C2–2C1–2C2–15, doi: 10.1109/ICNS50378.2020.9223003.

[7] J. A. Maxa, R. Blaize, and S. Longuy, "Security challenges of vehicle recovery for urban air mobility contexts," in *Proc. IEEE/AIAA 38th Digit. Avionics Syst. Conf.*, 2019, pp. 1–9, doi: 10.1109/DASC43569.2019.9081808.

[8] D. Kwon et al., "Design of secure handover authentication scheme for urban air mobility environments," *IEEE Access*, vol. 10, pp. 42529–42541, 2022, doi: 10.1109/ACCESS.2022.3168843.

[9] T. H. Stelkens-Kobsch and A.-V. Predescu, "Contribution to a secure urban air mobility," in *Proc. IEEE/AIAA 41st Digit. Avionics Syst. Conf.*, 2022, pp. 1–5, doi: 10.1109/DASC55683.2022.9925845.

[10] C. Nemeth and J. Holbrook, "Resilience engineering's potential for advanced air mobility (AAM)," in *Proc. 72nd Int. Symp. Aviation Psychol.*, 2021, pp. 128–133.

[11] D. Wing, E. Chancey, M. Politowicz, and M. Ballin, "Achieving resilient in-flight performance for advanced air mobility through simplified vehicle operations," in *Proc. AIAA Aviation Forum*, Jun. 2020, doi: 10.2514/6.2020-2915.

[12] Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, National Institute of Standards and Technology (NIST) NIST SP 800-160 volume 2, 2021.

[13] R. Hoffmann, H. Nishimura, and R. Latini, "Urban air mobility situation awareness from enterprise architecture perspectives," *IEEE Open J. Syst. Eng.*, vol. 1, pp. 12–25, Mar. 3, 2023, doi: 10.1109/OJSE.2023.3252012.

[14] C. Null et al., "Human performance contributions to safety in commercial aviation," National Aeronautics and Space Administration Technical Memorandum NASA/TM-2019-220417, 2019.

[15] J. Holbrook et al., "Enabling urban air mobility: Human-autonomy teaming research challenges and recommendations," in *Proc. AIAA Aviation Forum Conf.*, Jun. 2020, doi: 10.2514/6.2020-3250.

[16] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), Version 1.1, 2018.

[17] Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology (NIST), NITS SP 800-53 r5, 2020.

[18] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility," in *Proc. AIAA Scitech Forum*, Jan. 2021, doi: 10.2514/6.2021-0773.

[19] C. Torens et al., "HorizonUAM: Safety and security considerations for urban air mobility," in *Proc. AIAA Aviation Forum*, Aug. 2021, doi: 10.2514/6.2021-3199.

[20] A. Zaid, B. E. Y. Belmekki, and M. Alouini, "Technological trends and key communication enablers for eVTOLs," *IEEE Commun. Mag.*, vol. 61, pp. 154–160, 2023, doi: 10.1109/MCOM.004.2300061.

[21] M. Hause, "Integrating security into enterprise architecture with UAF and PLE," *INSIGHT*, vol. 23, no. 3, pp. 44–50, 2020, doi: 10.1002/inst.12310.

[22] M. Hause and L.-O. Kihlström, "Using the security views in UAF," in *Proc. INCOSE Int. Symp.*, 2021, pp. 64–79, doi: 10.1002/j.2334-5837.2021.00826.x.

[23] F. Dandashi, "Modeling security views with unified architecture framework, risk assessment and analysis modeling language, and systems modeling language," MITRE Tech. Rep. MTR220019, 2022. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1173412

[24] M. Pillay, "Resilience engineering: An integrative review of fundamental concepts and directions for future research in safety management," *Open J. Saf. Sci. Technol.*, vol. 7, pp. 129–160, 2017, doi: 10.4236/ojsst.2017.74012.

[25] D. Woods, "Creating foresight: Lessons for enhancing resilience from columbia," in *Organization at the Limit: Lessons From the Columbia Disaster*, M. Farjoun and W. H. Starbuck, Eds. Oxford, U.K.: Blackwell, 2005, pp. 289–308.

[26] E. Hollnagel, C. P. Nemeth, and S. Dekker, *Resilience Engineering Perspectives: Remaining Sensitive to the Possibility of Failure*, vol. 1. Aldershot, U.K.: Ashgate Publishing, 2008.

[27] M. Pillay, "Resilience engineering: A state-of-the-art survey of an emerging paradigm for organisational health and safety management," in *Advances in Safety Management and Human Factors*, vol. 491, P. Arezes Ed. Berlin, Germany: Springer, 2016, pp. 211–222, doi: 10.1007/978-3-319-41929-9_20.

[28] D. Mendonça, "Measures of resilient performance," in *Resilience Engineering Perspectives: Remaining Sensitive to the Possibility of Failure*, vol. 1. Aldershot, U.K.: Ashgate Publishing Ltd., 2008, pp. 29–48.

[29] S. M. Amin, "Smart grid security, privacy, and resilient architectures: Opportunities and challenges," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2012, pp. 1–2, doi: 10.1109/PESGM.2012.6345767.

[30] T. Maksymyuk, M. Beshley, M. Klymash, O. Petrenko, and Y. Matsevityi, "Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface," in *Proc. 14th Int. Conf. Adv. Trends Radioelectron., Telecommun. Comput. Eng.*, 2018, pp. 1127–1130, doi: 10.1109/TCSET.2018.8336392.

[31] A. A. Alsulami and S. Zein-Sabatto, "Resilient cyber-security approach for aviation cyber-physical systems protection against sensor spoofing attacks," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf.*, 2021, pp. 0565–0571, doi: 10.1109/CCWC51732.2021.9376158.

[32] D. J. Bodeau, R. Graubert, R. McQuaid, and J. Woodill, "Cyber resiliency metrics, measures of effectiveness, and scoring," MITRE Technical Report MTR180314, 2018.
[33] R. Patriarca, J. Bergström, G. Di Gravio, and F. Costantino, "Resilience engineering: Current status of the research and future challenges," *Saf. Sci.*, vol. 102, pp. 79–100, 2018.
[34] K. Rajashekara, Q. Wang, and K. Matsuse, "Flying cars: Challenges and propulsion strategies," *IEEE Electrific. Mag.*, vol. 4, no. 1, pp. 46–57, Mar. 2016, doi: 10.1109/MELE.2015.2509901.
[35] A. P. Cohen, S. A. Shaheen, and E. M. Farrar, "Urban air mobility: History, ecosystem, market potential, and challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 6074–6087, Sep. 2021, doi: 10.1109/TITS.2021.3082767.
[36] Unmanned Aircraft System (UAS) Urban Traffic Management (UTM) Concept of Operations 2.0, Federal Aviation Admin., Washington, DC, USA, 2020.
[37] Incose Systems Engineering Handbook a Guide for System Life Cycle Processes and Activities, 2015, Version 4. Ed. New York, NY, USA: John Wiley & Sons, ISBN 9781118999417.
[38] Software, systems and enterprise—Architecture processes, ISO/IEC/IEEE 42020, 2019.
[39] Enterprise Architecture Guide for UAF—Object Management Group Unified Architecture Framework (OMG UAF)—Appendix C Version 1.2, 2022.
[40] Unified Architecture Framework Modeling Language (UAFML) Version 1.2.—Object Management Group Unified Architecture Framework (OMG UAF), 2022.
[41] Information technology—Object Management Group Unified Architecture Framework (OMG UAF)—Part 1: Domain Metamodel (DMM), ISO/IEC 19540-1:2022, 2022.
[42] E. Hollnagel, J. Pariés, D. Woods, and J. Wreathall, *Resilience Engineering Perspectives: Resilience Engineering in Practice*, vol. 3. Farnham, U.K.: Ashgate Publishing Ltd., 2011.

RAQUEL HOFFMANN received the bachelor's degree in electrical engineering from the National Institute of Telecommunications, Minas Gerais, Brazil, in 2007, and the master's degree in aeronautical engineering from the Aeronautical Institute of Technology, Sao Jose dos Campos, Brazil, in 2010. She is currently working toward the Ph.D. degree in systems engineering with the Graduate School of System Design and Management, Keio University, Yokohama, Japan.

She worked with the Aviation Industry as an Avionics Systems Engineer, from 2009 to 2020. Her research interests include urban air mobility, safety, security, human systems integration, enterprise architecture modeling, and the unified architecture framework.

DANIEL PATRICK PEREIRA received the bachelor's degree in computer engineering from Santa Cecilia University, Santos, Brazil, in 2003, the master's degree in computer engineering from the Federal University of Amazonas, Manaus, Brazil, in 2008, and the doctoral degree in electronic engineering and computing from the Aeronautical Institute of Technology, Sao Jose dos Campos, Brazil, in 2020.

He is currently a Cybersecurity Architect with the Airbus Defence and Space applying model-based systems security engineering approaches in civil, space, and military programs.

HIDEKAZU NISHIMURA (Member, IEEE) received the Ph.D. degree in mechanical engineering from Keio University, Kanagawa, Japan, in 1990.

He was an Associated Professor with the Chiba University, Chiba, Japan, from 1995 to 2007, a Visiting Researcher with the Delft University of Technology, Delft, The Netherlands, in 2006, and a Visiting Associate Professor with the University of Virginia, Charlottesville, VA, USA, in 2007. He is currently a Professor with the Graduate School of System Design and Management, Keio University. His research interests include applying model-based systems engineering approach for various highly complex systems as well as designing an automated driving system.