An Interoperable Framework for Network-Enabled Cross-Border Multi-Agency First-Aid Vehicles in Multiple Casualty Incidents

Marco Manso
PARTICLE Summary
Lisbon, Portugal
e-mail: marco@particle-summary.pt

Alberto Montarelo
TASSICA
Madrid, Spain
e-mail: alberto.montarelo@tassica.com

Jorge Maestre Vidal
INDRA
Madrid, Spain
e-mail: jmaestre@indra.es

Pedro Petiz
PARTICLE Summary
Lisbon, Portugal
e-mail: pedro@particle-summary.pt

Navid Behzadi Koochani
Servicio de Urgencias Medicas de Madrid, Madrid, Spain
e-mail: navid.behzadi@salud.madrid.org

Meritxell Bassols Tayeda
INDRA
Madrid, Spain
e-mail: mbassols@indra.es

Bárbara Guerra
PARTICLE Summary
Lisbon, Portugal
e-mail: barbara@particle-summary.pt

Ioannis Chatzichristos
ARATOS
Athens, Greece
e-mail: ichatzichristos@aratos.gr

Sergio López Bernal
Universidad de Murcia
Murcia, Spain
e-mail: slopez@um.es

***Abstract*- A cross-border Multiple Casualty Incident (MCI) affects a large number of persons requiring urgent medical assistance by authorities and warrants significant international coordination. This work addresses the technical challenge of building a cross-border multi-agency coalition as a federated system supporting international coordination, while delivering the required assistance to the victims. Using as basis a reference MCI cross-border scenario, an overarching architecture is defined, the VALKYRIES architecture, including the rules, protocols and data models that enable integration of heterogeneous entities, being those services, applications or sensors. By implementing the VALKYRIES architecture, organisations become ready to participate in a federated collaborative environment, exchange MCI-related information and achieve high-levels of shared situational awareness, thus contributing towards a better employment of resources and improving the mission's effectiveness and efficiency.**

Keywords- Multiple casualty incident; Emergency Services; Interoperability; Federated System; Technical Architecture.

I. INTRODUCTION

A MCI affects a large number of persons requiring urgent medical assistance by authorities. It may demand more resources and capabilities than those available in a single organisation, thus collaborating with other agencies is fundamental to deliver an efficient response. This is even more so for incidents crossing borders, where international coordination is mandatory. Implementing a cross-border multi-agency coalition offers significant technology-related challenges, since different technological solutions, applications, communication networks, data models, and protocols – including legacy solutions – are used by the different involved partners, resulting in a heterogeneous landscape of artifacts and tools. Standards for interoperability, contributing towards the harmonisation between heterogeneous organisations, have to be defined, implemented and adopted.

This paper presents the work performed in the VALKYRIES Action towards defining rules and protocols enabling the integration of the different capabilities, technologies, data gathering sensors and artifacts at play in a cross-border MCI, in a coordinated and in-field deployable way. The paper is structured as follows: Section II describes an operating cross-border MCI scenario, including involved actors, artifacts and information flows; Section III presents the technical architecture defined for VALKYRIES, including relevant standards and defined services; Section IV introduces the data models used in VALKYRIES; and Section V concludes this paper.

II. OPERATING IN A MULTIPLE CASUALTY INCIDENT SCENARIO

The VALKYRIES Innovation Action analyses and defines harmonised mechanisms for the effective management and deployment of resources during the run-up to a major crisis related to any kind of cross-border disaster (natural or intentional) that demands the fast actuation and coordination of first-aid emergency services and associated response teams, with Civil-Military Cooperation (CIMIC) and volunteering. Its primary objective is to develop, implement, validate, and apply innovative theoretical foundations, methods, prototypes, and their demonstration on a reference integration framework to support the ongoing/planned European actions for pre-standardisation

 ISBN: 978-1-68558-083-4

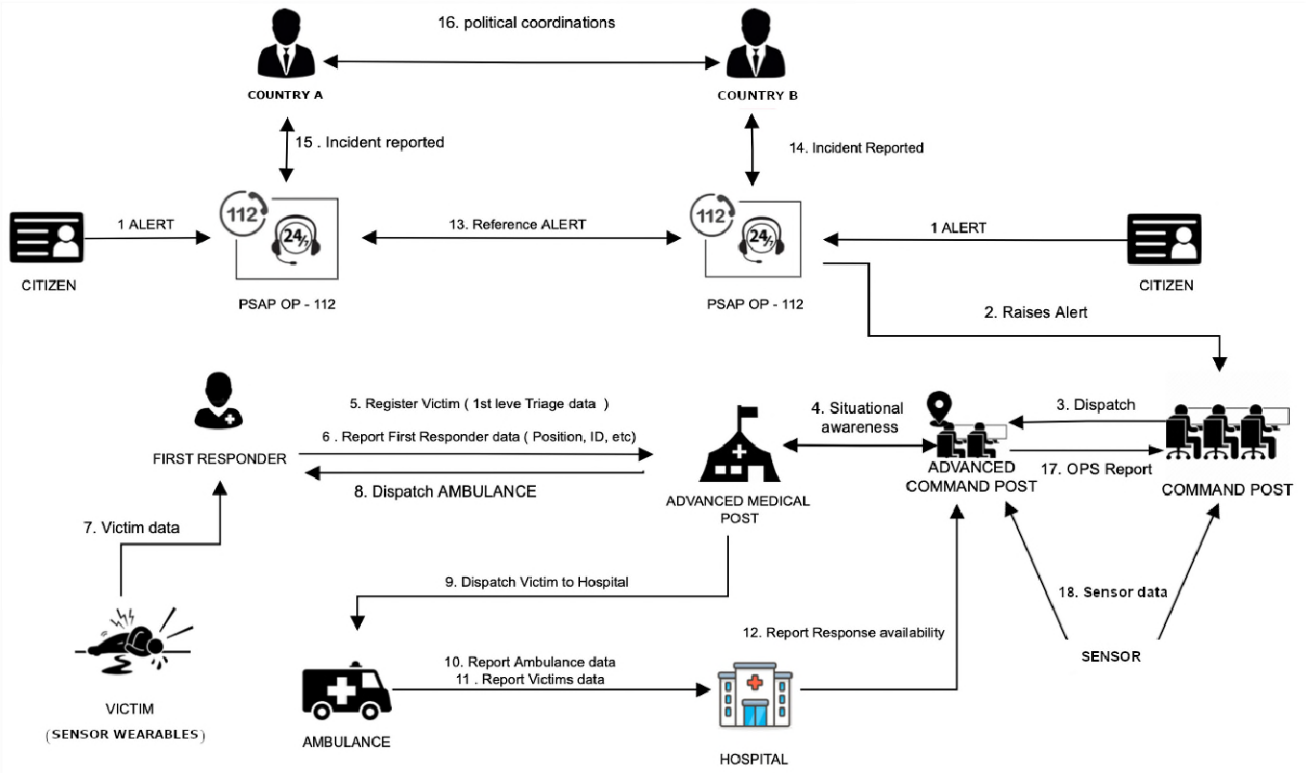

Figure 1. General Operating Scenario: Interaction Diagram

and harmonisation technologies, procedures, preparedness, and cross-border/sector cooperation for first aid response at disaster management by first aid emergency services, with the focus on health services and vehicular deployments. VALKYRIES also aims to generate synergies between different parties, regardless of their language and action protocols, to optimize the management of the incident without trying to modify its structure and normal operation. By improving interoperability in cross-border and cross-sector emergency situations, particularly when involving a MCI, the reference integration framework will empower improved coordination and employment of resources and increased mission efficiency and effectiveness.

The project implements an Observe-Orient-Decide-Act (OODA) approach for solving the identified harmonisation challenges [1], where:

- Observe: Resembles the acquisition of preliminarily factual knowledge.
- Orient: Reasons on the best hypothetical approach for addressing identified gaps and materialise opportunities.
- Decide: Selects the most suitable harmonisation options and applies them on a reference integration framework.
- Act: Coincides with deploying, evaluating and contrasting the assumed hypothesis based on the achieved analytical and empirical results.

Next, a reference scenario is presented that will guide the definition of the VALKYRIES architecture.

A. Reference Operating Scenario

A MCI scenario involves multiple actors operating at different levels that need to interact with each other to develop shared situational awareness and ensure adequate coordination of resources.

A general overview of an operating scenario, showing the main involved actors and their interrelations, is depicted in Figure 1. The fictional scenario involves a large forest fire starting in the region of Badajoz, close to the border between Spain and Portugal. The fire rapidly spreads to the Natural Park of *Serra de S. Mamede* in Portugal, evolving into a cross-border incident. The intensity of the fire, together with the large extension of burned ground and weather conditions, cause the authorities to activate the regional emergency plan at both sides of the border. Authorities understand that, to minimise human and material damage, an effective collaboration is crucial. Cooperation is established at different levels, including political (e.g., ministries collaboration and protocols), tactical (civil protection authorities and command posts) and operational (e.g., firefighters, medical teams and their vehicles).

This fictional incident involves the deployment of several technological artifacts (presented in Table I) and information flows (presented in Table II).

 ISBN: 978-1-68558-083-4

TABLE I. ACTORS AND TECHNOLOGICAL ARTIFACTS

Actors	Technological Artifact
Citizens	User Terminal (e.g., Mobile phone and App), Web-client
Firefighters FR (*) Advanced Medical Post	Wearables (e.g., activity tracker with satellite positioning) User Terminal (e.g., Professional Mobile Phone with App) TETRA Terminal
PSAP (*) Operator 112 Coordination Centre	112 Terminal Emergency Management System
Coordination Centre Command Post	Emergency Management System Command and Control System
Political Liaison	User Terminal (e.g., Phone / E-mail)
First Aid Vehicles & Ambulances	Vehicle Terminal (with network connection and satellite positioning) Medical devices and wearables
Hospital	Hospital Information System
Victims	Medical devices and wearables

(*) PSAP: Public Safety Answering Point. FR: First Responder

TABLE II. INFORMATION FLOW

1. Alert	Communication of a medical emergency by a citizen via an emergency call
2. Raises Alert	Report of the emergency case to the Command Centre
3. Dispatch	Forward the emergency case to the Advanced Command Post in response to a confirmed incident
4. Situational Awareness	Report incident victims and medical status and data received, including victims, FR and assets' location status and priority
5. Register victim	Victim information including triage data
6. Report first response data	First responder information, including location and status
7. Victim data	Victim data update: symptoms, pathology, medical information; status (triage). Emergency case file updated
8. Dispatch Ambulance	Dispatch information: assign victim to an ambulance, victim information
9. Dispatch Victim to Hospital	Ambulance task, Destination hospital, victim information, Emergency case file updated; victim pathology
10. Report ambulance data	Ambulance position and time-of-arrival, victim information (on-transport)
11. Report victim data	Victim information; victim vitals data (ambulance or wearable devices); Victim triage update
12. Report response availability	Hospital medical emergency's availability
13. Reference Alert	Cross-border incident data alert
14. Incident Report (Spain)	Data on cross-border confirmed incidents generated from Spanish authorities
15. Incident Report (Portugal)	Data on cross-border confirmed incidents generated from Portuguese authorities
16. Political Coordination	National authorisations and political agreements
17. Operations Report	Operations' progress and status: incident updates; assets' updates; victims' updates; situational awareness of high risks elements
18. Sensor data	Deployed sensor data: weather, fire detection, air quality indicator, video, chemical/biological agents detection, beacon (location)

III. VALKYRIES ARCHITECTURE AND APPROACH

Considering the large variety of involved actors and sovereignty over their own systems, VALKYRIES adopts a federated approach to connect the different systems together, a system of systems approach aiming to provide distributed operational response, coordination capability and supporting services. VALKYRIES overarching architecture is presented next.

A. VALKYRIES Overarching Architecture

The VALKYRIES overarching architecture follows a federated approach capable of interconnecting heterogeneous applications, data sources and systems. It establishes a common integrated framework (e.g., principles, business processes, core functions, data models, protocols, communications and security requirements), herein named as VALKYRIES Interoperability Framework (VIF). VIF encompasses: **federation-level data services** enabling data sharing among the different applications; **communications services** that establish the connectivity among the different users; and the **core services** that establishes common functions required for the orchestration and deployment of resources. Applications and services provided by each agency interoperate with each other via SIGRUN, a conceptual connector complying with VIF. A high-level diagram illustrating the VIF integration concept is presented in Figure 2.

Within the VIF concept, applications and services are able to either natively implement VIF or, in case of legacy systems, a specifically connector may be applied. This ensures that the VALKYRIES concept can be universally applied to any application, data source and component, as illustrated in Figure 3.

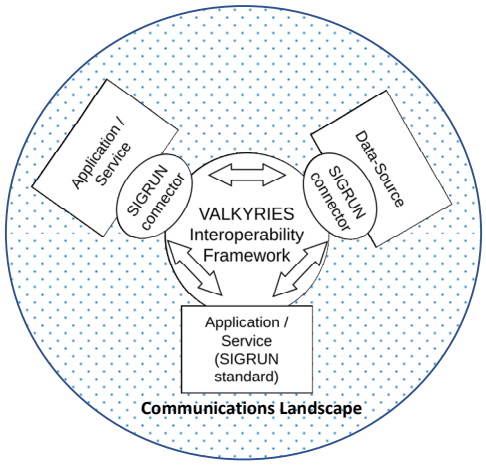

Figure 2. VIF Integration Concept Overview

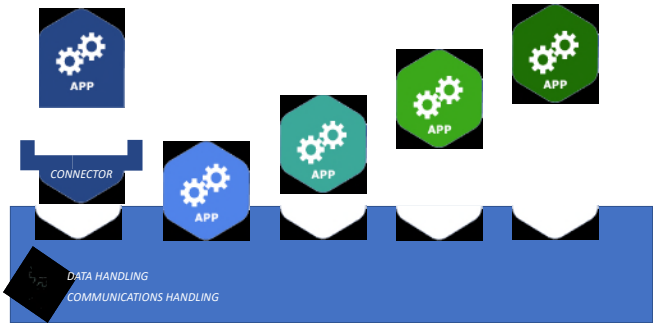

Figure 3. SIGRUN Integrations: native and connector-based

B. *Standards and Technologies for Interoperability*

VIF rules and principles were defined considering and benefiting from existing widely-used standards and technologies, presented next.

- **All-over-IP**: the Internet Protocol (IP) (RFC6864), is the current dominant network protocol, connecting billions of systems on the Internet. VIF uses IP to interconnect applications and services.
- **Emergency Data Exchange Language** (EDXL): the Organisation for the Advancement of Structured Information Standards (OASIS) sets the main goal of the EDXL as an enabler to facilitate emergency information sharing and data exchange among key stakeholders namely local, state actors, national agencies or non-governmental organisations supporting emergency response and management services [2].
- **EDXL Hospital Availability Exchange** (EDXL-HAVE) specifies an Extensible Markup Language (XML) document format that allows the communication of the status of a hospital, its services and resources, including bed capacity and availability, emergency department status, available service coverage, and the status of the hospital's facilities and operations [2].
- **NENA Emergency Incident Data Object** (EIDO): the United States' National Emergency Number Association (NENA) created EIDO, a standardised, industry-neutral format for exchanging emergency incident information between disparate manufacturer systems located within one or more public safety agencies, and with other incident stakeholders [3]. Recognising the existence of many functional elements involved in emergency management and response, which in turn involve multi-agencies and actors, EIDO provides a common representation of emergency incidents across the lifecycle of an emergency.
- **FHIR for medical data**: Fast Healthcare Interoperability Resources (FHIR) is a standard for healthcare data exchange, published by Health Level 7 (HL7) [4]. FHIR was created to cope with the fast digitisation of health records, aiming to provide a harmonised way to ensure that electronic health records and medical data are available, discoverable, and understandable across different medical agencies and healthcare systems.
- **Smart Applications REFerence ontology** (SAREF): under the aegis of the European Telecommunications Standards Institute (ETSI), SAFER is intended to enable interoperability between solutions from different providers and among various activity sectors in the Internet of Things (IoT) [5]. SAREF identified about 50 different semantic assets later translated into Web Ontology Language (OWL). SAREF is being extended to address specific sectors like agriculture, automotive, energy and environment.
- **VALKYRIES web-based requests**: components in VALKYRIES may need to issue requests to other federated components, such as retrieving a list of emergency incidents, retrieving information about the health status of a specific victim or even request the assignment of an ambulance to a victim. Federated components can issue web-based requests to other components using the widely adopted Representational State Transfer (REST) architectural style. REST emphasises scalability of component interactions, generality of interfaces, independent deployment of components, and intermediary components to reduce interaction latency, enforce security, and encapsulate legacy systems [6]. The application of REST principles with the Hypertext Transfer Protocol (Secure) (HTTP(S)) protocol (Request for Comments or RFC 7231) and JavaScript Object Notation (JSON)-formatted payload in web-based server-client architectures is widely used over the Internet. Servers expose their interfaces by what is called as "RESTful Application Programming Interfaces (APIs)".
- **Data exchange and communication protocols:** complementing transactional requests (i.e., RESTful API), VALKYRIES supports a message broker service following the publish-subscribe paradigm via the open standard Message Queuing Telemetry Transport (MQTT) version 5.0 [7]; data streaming via *Websockets* (Internet Engineering Task Force or IETF RFC 6455); video streaming via the Web Real-Time Communication (WebRTC) protocol suite [8]; and

 ISBN: 978-1-68558-083-4

multimedia communication via the Extensible Messaging and Presence Protocol (XMPP) standard (RFC 6120).

- **Security**: access to VALKYRIES is restricted to authorised users with valid credentials. Exchanged information is end-to-end encrypted, using Transport Layer Security (TLS). TLS is designed to prevent eavesdropping, tampering, and message forgery (RFC 8446).

C. *VIF Services*

VIF Services provide underlying functions that support the integration in the SIGRUN connector, enabling applications and services to become a part of the VALKYRIES federation. VIF Services are presented in Figure 4 and described next.

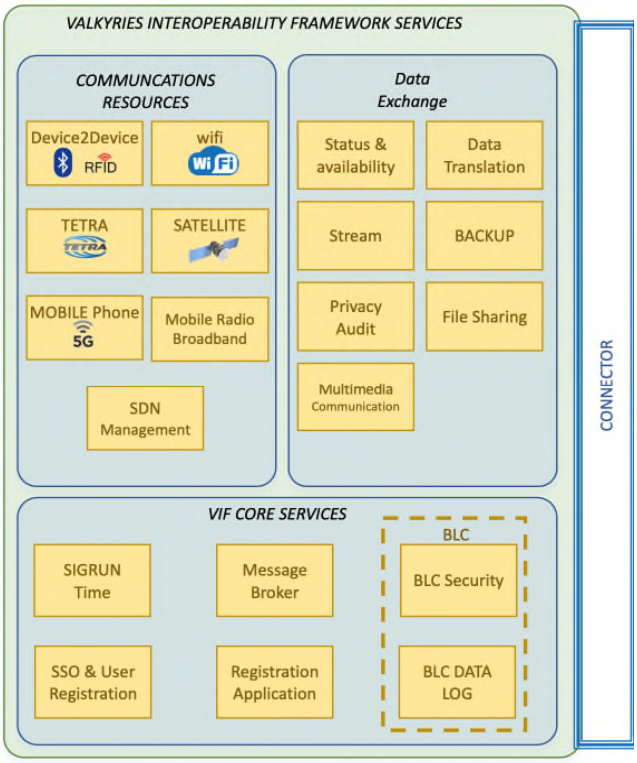

Figure 4. VIF Services.

VIF Services are organised in three categories:

Communication Resources: These services are responsible for delivering communication capabilities to federated entities, enabling them to access and interact with VALKYRIES resources. It also deals with management and coordination of different networks and technologies to deliver robust and resilient communications. It uses a Software Defined Network (SDN) approach to address traditional network architecture limitations, as pointed out by Priyadarsini *et al.* [9].

Data Exchange: These services provide data exchange protocols, enabling operational services to exchange data within SIGRUN (e.g., subscribe messages to the message broker).

VIF Core Services: These services provide the necessary functions to set-up, deploy and orchestrate the VALKYRIES federation. They enable a highly dynamic environment, where deployed services, at any time, can operate in a secure environment, enter or leave the federation, discover services and exchange data without the need to know the topology of the services in use. The VIF core services encompass the following services:

- The **Single Sign-On service & User registration** (SSO) provides authentication in the VALKYRIES system, functioning across the federation's different applications and services. It also supports registration of users and definition of roles within the federation. The SSO is a centralised service in VALKYRIES.
- The **Registration service** provides the mechanisms to register applications and components in the VALKYRIES system, thus becoming known in the federation. This service is a centralised service in VALKYRIES.
- The **SIGRUN time service** provides the reference time to the VALKYRIES system and thus consequently to VALKYRIES's applications and services. This service is a centralised service in VALKYRIES.
- The **Message broker service**, which can be realised by a single server or a cluster of servers, allows applications to exchange data following the publish-subscribe mechanism. The mechanism supports event-based processing by notifying subscribers when new messages are published.
- **Blockchain (BLC) based services** tracks exchanged data in VALKYRIES and stores the metadata and the transactional data in the BLC network. The BLC services function as a secure trace and auditing mechanism in VALKYRIES.

IV. VALKYRIES DATA MODEL AND METADATA

VALKYRIES defines data models representing MCI and emergency response information. The data models are designed to be agnostic of data producers' characteristics, being well adapted to support different types of producers, which can be sensors, algorithms and human inputs. The data model defines MCI specific data, represented by a MDS and associated metadata, as introduced next.

A. *Minimum Data Set*

A MDS is a structured collection of data associated with a unique body of work. It is designed to represent MCI-related information in SIGRUN, including the necessary information to support a coordinated action of the federated organisation. The MDS is structured into six main categories, as presented in Table III.

 ISBN: 978-1-68558-083-4

TABLE III. MINIMUM DATA SET CATEGORIES

Category	Description
Incident Data	Data related with an MCI. It observes EDXL and EIDO specifications.
Vehicle Data	Data concerning vehicles used in an MCI, like ambulances. It observes FHIR and EIDO specifications.
Smart Devices and IoT Data	Data related with connected devices and IoT, such as victims' vitals, fire detection and air quality. It observes FHIR and SAREF specifications.
First Responders Data	Data related to first responders. It observes EIDO and FHIR specifications.
Victim Data	Information collected about a victim during an MCI. This includes triage information, location and injuries. It observes FHIR standards.
Hospital Incident Data	Information about a hospital capabilities and capacity in receiving and treating victims. It observes EDXL, EDXL-HAVE and FHIR standards.

B. *Metadata*

Every generated message in VALKYRIES contains associated metadata, providing mechanisms to trace, control and restrict how it is handled and shared. The metadata includes:

- Timestamp: date and time the message was generated.
- ProducerID: identifier of the artifact (e.g., sensor or application) that generated the data.
- DataTimeValidity: time validity of the information.
- OwnerID: identifier of the owner of the data, used for traceability purposes and assure compliance with the General Data Protection Regulation (GDPR) [10].
- PriorityLevel: priority of the message.
- UserID: identification of the user that generated the data;
- Shared: flag indicating if the data is authorised to be shared cross-border.

VALKYRIES functions as a cooperative environment allowing entities to exchange data. Since the environment involves sensitive data, VALKYRIES implements mechanisms to trace and audit messages, as well as information flows. VALKYRIES stores all metadata in a Blockchain service, ensuring immutability and security. Blockchain auditing tools can be used, for example, in case a post-event assessment is needed.

V. CONCLUSION

This paper presents the work performed in the VALKYRIES project towards defining a technical architecture capable of enabling collaboration among multiple agencies operating in a cross-border MCI. The definition of the VALKYRIES architecture considers actors, artifacts and information flows involved in a cross-border MCI, from which an interoperability framework, named VIF, was defined. Organisations complying with VIF are empowered to easily participate in a federated collaborative environment, exchange MCI-related information and achieve high-levels of shared situational awareness, thus contributing towards a better employment of resources and improving the mission's effectiveness and efficiency. Next steps of VALKYRIES will involve to further detail the technical architecture and to validate its operational performance in several realistic demonstration scenarios planned for 2023 in Portugal, Spain, Bulgaria, Slovakia, Italy, Greece and Norway, as part of the VALKYRIES Action. A key objective will be to develop technical specifications serving as the basis for a standard, thus benefitting all organisations involved in MCI and cross-border emergency situations.

ACKNOWLEDGMENT

Funding: "This research has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement: Nº 101020676". The authors would like to thank all the partners of the VALKYRIES Action that supported and contributed to the concepts developed.

The authors declare no conflict of interest.

REFERENCES

[1] VALKYRIES website. https://www.valkyries-h2020.eu. [Retrieved: February, 2023].

[2] OASIS. 2013. *Emergency Data Exchange Language (EDXL)* Distribution Element Version 2.0. Available at: https://docs.oasis-open.org/emergency/edxl-de/v2.0/cs02/edxl-de-v2.0-cs02.html. Dated: September, 2013. [Retrieved: February, 2023].

[3] NENA. 2022. *NENA Standard for Emergency Incident Data Object (EIDO)*. NENA-STA-021.1-2021. Dated: October 19, 2021. Approved: April 4, 2022. [Retrieved: February, 2023].

[4] FHIR Website. https://www.hl7.org/fhir/. Accessed version 4.3.0 generated at 2022-May-28. [Retrieved: February, 2023].

[5] ETSI. 2020. *SmartM2M; Smart Applications; Reference Ontology and oneM2M Mapping*. ETSI TS 103 264 V3.1.1 (2020-02). [Retrieved: February, 2023].

[6] Fielding, R., *Architectural Styles and the Design of Network-based Software Architectures*". Doctoral Dissertation, University of California, Irvine, Sep-tember 2000. Available at: http://roy.gbiv.com/pubs/dissertation/top.htm. [Retrieved: February, 2023].

[7] OASIS. 2019. *MQTT Version 5.0. OASIS Standard*. Available at: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html. [Retrieved: February, 2023].

[8] W3C. 2021. *WebRTC 1.0: Real-Time Communication Between Browsers*. W3C Recommendation. Dated: 26 January 2021. Available at: https://www.w3.org/TR/webrtc/. [Retrieved: February, 2023].

[9] Priyadarsini, M., and Bera, P., *Software defined networking architecture, traffic management, security, and placement: A survey*. Computer Networks, 192, 2021.

[10] Regulation (EU) 2016/679 of The European Parliament and of The Council. Of 27 April 2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504