Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Practical Network Simulation for Civil and Defense Resilience Communications

Spyridon K. Chronopoulos

spychro@gmail.com

University of Ioannina https://orcid.org/0000-0003-0132-2338

Konstantinos P. Peppas

University of Peloponnese https://orcid.org/0000-0002-8772-2502

Malamati Louta

University of Western Macedonia

Vasilis Christofilakis

University of Ioannina https://orcid.org/0000-0001-6751-4557

Research Article

Keywords: TeleReNT, Network Digital Twin, Dual-use, civil protection, defense use, LoRaWAN, FTTH, resilient communications, IoT, mountainous networks

Posted Date: June 5th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9923283/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

(Research Article)

A Practical Network Simulation for Civil and Defense Resilience Communications

Spyridon K. Chronopoulos [1*], Konstantinos P. Peppas [2], Malamati Louta [3] and Vasilis Christofilakis [1]

[1] Electronics-Telecommunications and Applications Laboratory, Physics Department, University of Ioannina, 45110 Ioannina, Greece; spychro@gmail.com (S.K.C.), vachrist@uoi.gr (V.C.)
[2] Department of Informatics and Communications, University of Peloponnese, 22100 Tripoli; peppas@uop.gr (K.P.P.)
[3] Department of Electrical and Computer Engineering, University of Western Macedonia, 50151 Kozani, Greece; louta@uowm.gr (M.L.)
* Correspondence: spychro@gmail.com (S.K.C.)

Highlights

- Proposition of a dual-use resilient Network Digital Twin (civil and defense applications).
- Combination of FTTH, wireless PtP/PtMP links, wireless PtP/PtMP technology, and GIS.
- Introduction of a network risk score and a model intended for emergency telemetry, while based on a compatible Octave code for near-future implementation.

Abstract

The TeleReNT (Telecommunications Resilience Network) platform proposal is based on a fast dual-use Network Digital Twin architecture for wireless infrastructure, Internet of Things (IoT) applications, and hybrid fibre to the home (FTTH). The deployment includes various environments such as mountainous and semi-rural areas of interest. The structured architecture implements telemetry originated from optical access networks, point-to-point (PtP) and point-to-multipoint (PtMP) wireless links (WL), long-range wide area network (LoRaWAN) gateways, various environmental sensors, and the appropriate field maintenance tasks. The above procedures with the corresponding hardware contribute to the computation of the link-health, the infrastructure-risk, and the prioritization of selected mission indicators.

As far as the system is concerned, it operates in two modes. The civil protection mode is applicable to various types of monitored assets and smart city environments, while the defense mode is intended for resilient communications and to mitigate drawbacks such as sensor discontinuity, disruption events, and limited bandwidth.

This study does not introduce a new sensor-placement optimization algorithm or even an innovative measurement-acquisition method. Instead, it proposes an interpretable Digital Twin workflow and protocol-oriented reference framework. This helps organize heterogeneous telecommunications, Internet of Things (IoT), environmental, and maintenance indicators into operational risk states and telemetry-priority decisions. The wildfire scenario is used as a representative case study to demonstrate the workflow, while the same structure can be specialized for other civil-protection cases, critical infrastructure, and defense applications after specific calibrations, specialized code infusion, and validation. Consequently, to describe the proposed platform, a compatible prototype based on Octave code was developed to estimate link risk scoring, detecting degradation while classifying priority telemetry. Specifically, the prototype includes weighted indicators without a deep learning technique (having hidden internal structure) to be suitable for an initial field pilot without needing adequate data.

Keywords: TeleReNT, Network Digital Twin, Dual-use, civil protection, defense use, LoRaWAN, FTTH, resilient communications, IoT, mountainous networks

1. Introduction

Regions and areas that can be correlated with signal degradation when it is transmitted through them could be mountainous and semi-rural. In turn, there is a need for communication infrastructures to exhibit not only high capacity and reliability in handling telecommunication service-load but also being maintainable under various factors and constraints such as power, weather, terrain, and accessibility performance.

Heterogeneous infrastructure means a diverse environment that includes different processor architectures and, more generally, dissimilar system components. These components may range from different hardware to various operating systems and vendors. Thus, for regional telecommunications integrators, the goal is to innovate by transforming heterogeneous infrastructure into a resilient platform with measurable and predictable conditions [1, 2, 3].

As many companies and organizations could be an important local anchor toward the direction of transforming heterogeneous systems, only a few can combine the aforementioned with optical-fiber planning, deployment, maintenance, and FTTH repairing while implementing based on their agenda, wireless projects of large scale and intensity, and IoT applications for fire protection, energy optimization, and smart cities' applications [4, 5].

The proposed platform is a network digital twin (NDT), characterized by low cost, easy field deployment, and it uses operational telemetry rather than employing full 5G carrier technology. This fact leads to a feasible and viable implementation always aligned with global telecommunications rules and trends [1, 2, 3]. Rather than delving into a sensor-placement optimization method, this study directs attention to a protocol-oriented Digital Twin workflow that transforms heterogeneous asset telemetry into interpretable risk states and telemetry-priority decisions. So, the main contribution of this work is the design and demonstration of an interpretable Digital Twin workflow for dual-use infrastructure resilience. The proposed system does not attempt to optimize or use specific algorithmic approaches toward the physical placement of sensors or to introduce a new measurement-acquisition algorithm. Instead, it defines how heterogeneous asset data can be structured, normalized, scored, classified, and prioritized in a transparent decision-support pipeline. Consequently, the wildfire-monitoring scenario is addressed as a representative case study. Thus, the same workflow can be adapted to other use cases by modifying the asset models, telemetry variables, risk weights, normalization bounds, thresholds, and validation datasets.

The structure of this paper consists of eight sections. In the second section, the related scientific work is mentioned in order for the reader to really understand the basics of this work. Then, in the third section, the proposed system architecture is given along with the necessity of both proposed architectures, and then the dual-use operational concept is explained. In the fourth section, the purpose is to explain the methodology and simulation concept. The primary information for randomization tactics and sample generation is presented for normal and wildfire scenarios. It provides information about the description, simulation strategy, and assets. Section five exhibits the experimental results, and especially the simulation data schema, followed by summary statistics, visual, and spatial results. In section 6, the proposed pilot deployment and

evaluation plan is presented. Finally, sections 7 and 8 present the restrictions and conclusions, respectively.

2. Related scientific work

2.1. Network Digital Twins

In general, a network digital twin (NDT) should be addressed as a representation of comprehensive and dynamic content describing a physical network infrastructure, which is a fully synchronized real-time system with its real-world counterpart. As this technology could serve as an advanced emulation platform, it could enable any authorized network operator to construct scenario design and "what-if" analysis [6] relevant to real-time conditions. The scenario could even include traffic loads of high peak while predicting service degradation, without all those computations endangering the stability of an existing system or services [7, 8, 9].

Apart from simple representation and visualization of results, the NDT framework could be a key changer for impact analysis and for researching new ways of project management. It could provide a new kind of environment without the danger of acting on crucial components, with the goal to validate new schemes, systems, and near-future deployments, such as those based on 5G, before the final green light for final production. An essential role in the complete operational status is support for automated self-correcting adjustments through data-driven closed-loop automation. It is accomplished by incorporating machine learning (ML) techniques and artificial intelligence (AI), giving them the capability of understanding and processing high-dimensional data streams with the goal of recognizing patterns. In turn, the fact of forecasting network failures becomes viable while it is correlated to the system's execution of various autonomous correcting actions in real-time [10, 11, 12].

As far as the transition from theoretical proposals to architectures based on standardized references has been significantly conducted by Standards Development Organizations (SDOs). Some important acts are relevant to the Internet Research Task Force (IRTF) / Network Management Research Group (NMRG) [13]. The IRTF has contributed to the development of publications (drafts) for components, interfaces, and reference architectures (e.g., RESTful [REpresentational State Transfer] northbound and NETCONF [Network Configuration] interfaces) for the purpose of accomplishing, as soon as possible the industrial adoption [14].

The aforementioned industrial adoption definitely includes a virtual framework for network administrators for conducting real-time analysis, along with the needed protocol testing and proper monitoring. Specifically, the NDT, by serving as a digital replica, consists of telecommunications and network services, providing a quick testing solution which plays a key role across multiple areas [1,2] such as:

- Telecommunications (e.g., 5G and 6G) with proactive resource management and automatic control under environments of high complexity.
- Network traffic optimization for strengthening the routing strategies and properly handling congestion issues, as in smart cities, this adoption acts as a tool for finding potential congestion for implementing optimization where applicable (e.g., smart traffic lights) [15, 16].

- Data centers and large networks use operational rules and specific topologies to troubleshoot and diagnose anomalies for accomplishing enhanced performance and route optimization.
- Smart cities where systems exchange data with real-time IoT and various sensors for optimizing public services, emergency readiness, and other urban applications [15, 16].

The TeleReNT twin project employs the NDT case for specified regional hybrid access networks and various sensor implementations. The application conforms especially to edge computing toward reducing latency and bandwidth requirements. The hybrid networking, governed by the inclusion of multiple networks at the same time, is important for achieving connectivity even in "off-the-grid" areas based on a seamless and resilient manner of applying the needed services. In this way, the proposed platform delivers real-time anomaly detection and autonomous action against cyber threats and emerging uncertainties [17, 18, 19].

2.2. NDT predictive maintenance

The predictive maintenance is an advanced mode of approach, which is not restricted to one of the following such as reactive, and periodic preventative maintenances. Reactive type refers to repairing after a failure and periodic to predetermined time intervals. None of these are sufficient, while they provoke disruptions in network operations with increased cost [20]. On the contrary, predictive maintenance acts from a more advantageous position because it foresees imminent equipment failures by scheduling interventions in a timely manner. In this way, the hardware cannot reach an undesirable state of non-functionality. The connection to this concept comes from the evolution of simple threshold rules toward data processing intelligence based on machine learning (ML) techniques. So, ML and, in turn, artificial intelligence (AI) combined with the Internet of Things (IoT) architecture have evolved the concept of predictive maintenance. The workflow depends on two important pylons, which are (1) the huge amount of data produced from IoT systems in real-time and (2) the ML / deep learning algorithms that analyze the data for finding and/or understanding patterns, predicting equipment failures while improving the schedule of various maintenance [3, 10, 21]. As far as the industrial IoT areas, networks such as industrial Wi-Fi and 5G exhibit low latencies with high data transfer for quick anomaly detection. Also, low-power wide-area networks (LPWANs), like long-range wide area network (LoRaWAN), are distinguished for their energy efficient communication capabilities, providing advanced monitoring of specific assets. Communication protocols, designed for industrial implementation such as message queuing telemetry transport (MQTT) and open platform communications unified architecture (OPC UA) , can sustain secure data transmission between devices and cloud platforms in a scalable and lightweight manner to provide predictive capabilities, advanced analytics, and autonomous maintenance [23].

Deep learning (DL) models show a capability of processing and predicting failures, whereas other models cannot, thus model performance based on DL is more effective, relevant to learning performance, and adaptability to equipment altered behavior with accuracy of over 93% (adaptive ensemble) in comparison to almost 86% of random forest models [24].

2.3. IoT for civil protection and wildfire monitoring

It is widely known that IoT is relevant to connecting various devices and objects over the internet. These devices can be equipped with sensors that acquire data originating from various

environmental conditions. The acquired data can also be transmitted to other systems, which can be analyzed and, in turn, feed a decision-making system. So, smart sensors and networks based on IoT technology can be placed in various areas around and inside cities and areas of interest for monitoring crucial parameters such as air quality, environmental variables, and even structural integrity. So, situational awareness in times of crisis is greatly enhanced with the use of IoT. As far as the relevant events and economics on this category of devices, only in 2023, natural disasters caused about 95000 deaths worldwide, with the resulting economic costs reaching around 380 billion dollars. Based on the UN Office for the Reduction of Risk Relevant to Various Disasters, warning and prevention systems can accomplish a turn from managing disasters to managing risk. In this way, the endless cycle of disasters with vast economic costs and human lives can be broken and lead to a more predictive economy and safety zone for all citizens around the world [25, 26, 27].

LPWANs can address the challenge of being a robust communication network that can be reliable for IoT during a crisis, where these devices should even operate over large distances, remotely, and often with a minimal requirement of energy. These requirements can be fulfilled by the LoRaWAN protocol as aforesaid and, in this matter, has gained popularity amongst IoT applications, and is especially relevant to environmental monitoring. In accordance with the previous, a generic IoT architecture for civilian purposes contains three layers: (1) the device layer including sensors and actuators, (2) the network layer for connecting the devices through a gateway, and (3) the application layer for analyzing the data and making decisions accordingly [25, 26, 28].

Unfortunately, forest fires pose a significant danger to the whole European landscape, and according to the Joint Research Centre (JRC) of the European Commission, the worst case is found in areas near the sea (Mediterranean) due to high summer temperatures and strong winds. Specifically, wildfires contribute to the destruction of millions of vegetation every year, apart from the resulting losses of fauna, flora, and numerous losses of human lives. Other cases correspond to humans' responsibility in a deliberate or negligent way of acting [29].

Regarding the IoT architecture relevant to wildfire, it comprises additional sensor modalities. There are two kinds of ground sensors. The vision and environmental monitoring sensors contribute to the collection of visual and meteorological data for local or centralized analysis. There are also other weather sensor types for acquiring temperature, relative humidity, and air pressure data that could be essential for detecting wildfires. However, these types of sensors cannot do so on their own to properly detect early stages of fires. On the other hand, experiments have shown that gas sensors, even at a distance of 30 meters, are more capable of detecting small fires, and this evidence makes them a necessary component of early-stage fire detection [30]. An example of deploying a critical environmental sensor that could indicate the occurrence of fire is a CO_2-based node, which can be implemented in regions similar to the one which is illustrated in Figure 1. The capabilities of the IoT range from storage and analysis to alert generation while providing crucial information to system operators [31, 32].

Nevertheless, a crucial parameter in operational deployments is the balance between sensitivity and false positive rates. So, data are collected for identifying false conditions (e.g. alerts), for cross correlation between sensors, and comparison of the acquired data with already stored ones from a different time period. In the case of fire ignition detection, alerts are sent to (predefined) authorities while showing the sensors' position on the map and a representation with various visualizations and graphs [29]. The implementation (LoRaWAN forest-fire monitoring) in [33] covers a specific area, and it includes a fire-alert calibration algorithm. When the monitored indicators exceed the predefined thresholds, then it can send alerts to the authorities for their immediate response.

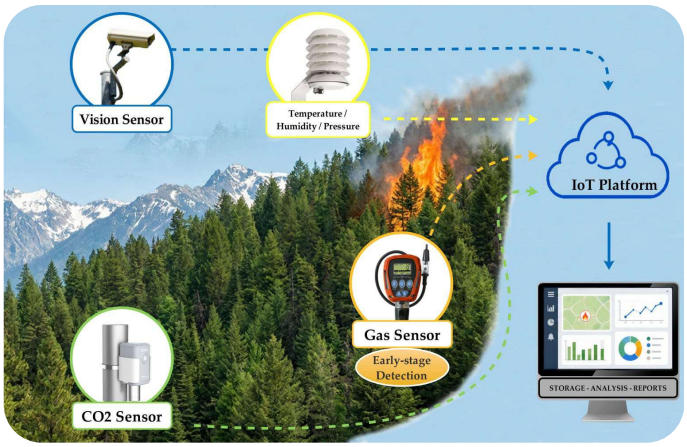


Figure 1. IoT Sensor architecture for Early-Stage Wildfire Detection

2.4. IoBT, military SDN and the tactical edge

Areas, marked as defense-type, exhibit communication drawbacks which can be considered as extreme versions of emergency civilian networks with low bandwidth, energy limitations, heterogeneous devices, while they should meet the most strict security requirements. These constraints are properly described by the concept of the Internet of Battle Things (IoBT). The latter architecture reshapes the modern battlefield (Figure 2) by interconnecting military assets such as autonomous vehicles, unmanned aerial vehicles (UAV), wearable and/or environmental sensors, surveillance cameras, and generally telecommunication apparatus, whereas their combination increase situational awareness and provide better decision-making. Some tactical edge networks are based on 5G and LTE architectures (high-speed, low-latency), while software-defined networking (SDN) provides enhanced network management across heterogeneous nodes [34].

The primary networking challenge increases enormously at an operational battlefield while cloud-centric architectures strive to work. So, the key factor of IoBT infrastructure is based on enhanced computing architecture, which can acquire data from various sensors (e.g., biometric, environmental, cameras, etc) on the battlefield and, in this way, help the military personnel be more efficient against dangerous conditions [35].

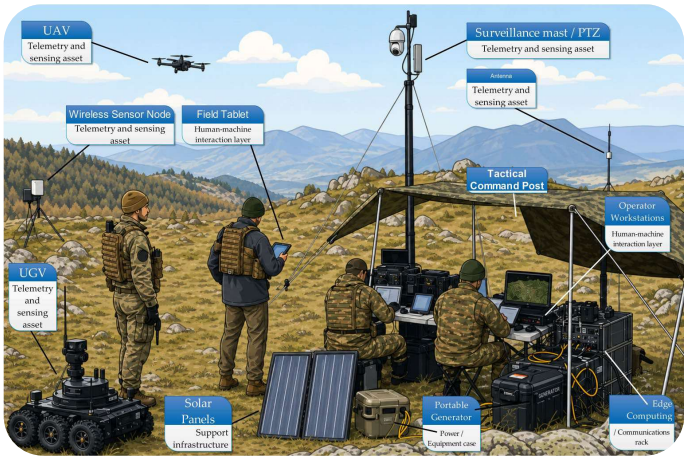


Figure 2. Internet of Battle Things (IoBT).

For coping with this heterogeneity in a dynamic manner, software-defined networking (SDN) has been employed as the most appropriate management architecture. The needed network strategy for command and control (C2) in such an environment of IoBT, combines the layers of applications and network in a multi-layer, while it uses a cybersecurity scheme with a specific strategy. The latter is related to defense in depth (DiD), which consists of various layers with supernumerary (in some cases) security measures for protecting various candidate targets, resulting in a multiplexing technique composed of sequential and complementary methods of protection. SDN, with the integration of information-centric networks (ICN), exhibits an overall upgrade in end-to-end delay and network load compared to common architectures [36, 37]. As far as the energy constraints, SDN optimizes the path selection for better energy preservation in IoBT environments, based on the energy-efficient path selection (EEPS) algorithm. This is accomplished by selecting the best possible network paths with minimal energy requirements while ensuring seamless communications. Specifically, the U.S. Army Research Laboratory (relevant to IoBT) aims toward lowering latencies (of decision cycles), enhancing the resilience of analytics, and advancing machine intelligence for the imminent future tactical network types [38]. In comparison to dual-use platforms (applicable to civil protection), direct relevance depends on the formal similarity of the restrictions. Consequently, various scientific methods and principles for coordinated communications are needed at the tactical level, along with appropriate sensing and processing for the purpose of obtaining context-aware analytics. These could utilize parameters such as location, time, and environmental conditions for providing information and/or actions. However, we should not overlook the fact that commercial IoT research needs to be elevated to higher levels using interdisciplinary contributions to reach a solution relevant to the drawbacks that can emerge in environments of poor infrastructure. Nevertheless, the same demands arise as soon as any serious civil protection or monitoring platform operates in severe (e.g., heavy noise) or serious remote (e.g., increased channel update rate) conditions [39]. The TeleReNT borrows all the aforesaid principles for telemetry and service resilience, while it is intended for defensive applications [40, 41].

3. Proposed system architecture

The proposed TeleReNT Twin architecture was designed on purpose, through the use of two discrete steps (versions V1 and V2 shown in Figure 3). The utilized strategy presents the system in a more realistic manner and at the same time in an incremental way. The first step is a lightweight prototype having compatibility with already deployed monitoring assets, while the second step is a more advanced version including a closed-loop NDT platform. So, in this context, V1 corresponds to the minimum but viable innovation, while V2 corresponds to an enhanced architecture on the research level.

The first version (V1) corresponds to the implementation of the proposed system and aims to highlight the analytical core of TeleReNT Twin. It shows the collection and simulation of telemetry from the network and various IoT resources. Latency, signal-to-noise ratio (SNR), battery levels, packet loss, temperature, and environmental parameters are presented, while a unified network risk score (taking into account all the previous values) is inserted as a performance indicator. Having implemented this score, each link or node is arranged in predetermined operational states named as normal, watch, degraded, or critical. Furthermore, TeleReNT V1 introduces a classification method where information is prioritized as low, medium, high, and

emergency. In conclusion, the principal innovation is that the proposed architecture combines IoT telemetry and heterogeneous telecommunications for converting the acquired results into a simple, and yet operational model to be easily interpreted. In comparison to other conventional systems, which can typically present several standalone alarms or various metrics, TeleReNT V1 aims to support any civil-protection and defense application on decision-making level. The architecture (Tables 1 and 2) can be easily implemented without significant changes to any typical infrastructure, while it fits for pilots, demonstrations on proof of concept (POC) level, and preliminary validations.

The second version (V2) extends the capabilities to a new level. It is no longer a risk-scoring prototype, but furthermore transforms to a modular system consisting of telemetry sources, an edge collector, the digital twin (DT) core, a prediction engine, a priority telemetry router, a dashboard, and finally the civil protection / defense layer. An important addition is an iterative function that includes feedback to the DT core from the dashboard, operator with incident updates, and field validation outcomes. The iterative function provides an adaptable mechanism to the V1 platform, which can now be updated, and perform not only one-way monitoring. Let's consider a team that has been deployed in a field. When its members validate a potential fault, a false alarm, or even inform about an update in a part of the system, then all information is acquired by the DT core. In turn, the received information can be used to affect / update future risk score, operational prioritization, to estimate the system parts' state of operation, and in this way to enhance the system's awareness. Consequently, the V2 solution (Tables 1 and 2) is a more demanding (to be implemented) but more realistic as it is correlated to the term of a "living twin" model [42]. This model is constantly updated with telemetry data and by human-in-the-loop (HITL) reporting [43].

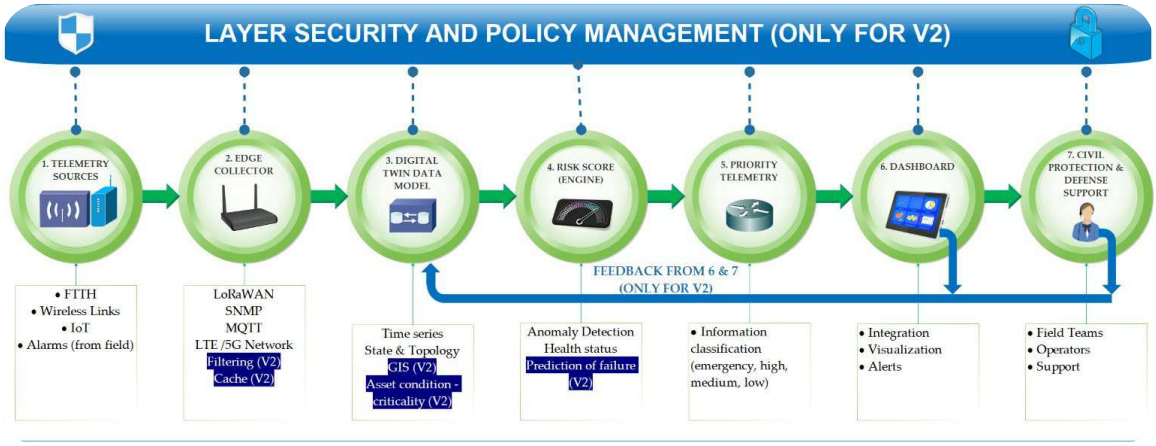


Figure 3. TeleReNT Twin V1 and V2 (version 2 add-ons are presented in blue color along with a proposed feedback function)

In Figure 3, the layer of security and policy management (cross-layer, only for V2) is shown in a stochastic and simplified manner, indicating a role-based access and control level with the capability of communicating with every layer. The goal was not to simulate a complete cybersecurity substructure (frame) but instead, to exhibit the way that various constraints, relevant to security and policy, might regulate data diffusion, telemetry issues, and user access across any layer of the recommended architecture.

For the purpose of explaining the whole procedure of the proposed architecture versions, we emphasize a hypothetical scenario where a risk of wildfire is discovered in a mountainous area. There, a network sustains both the telecommunications of a civilian community and provisional defense operations. The assumed infrastructure (stage 1) contains wireless links, various IoT sensors (environmentally oriented), field alarms, FTTH backhaul at some points, and the capability of sustaining mobile users. In the case of V1, the proposed system performs as a one-way pipeline. Raw data are collected from various sensors (including IoT), wireless links, and field alarms. Let's presume that near an area of interest, CO_2 detection rises, humidity drops, temperature increases, while there is a smoke probability, and wireless links deteriorate. The edge collector (stage 2) acquires all the aforementioned heterogeneous signals (inputs) using protocols such as SNMP, MQTT, LoRaWAN, or LTE/5G and converts them into a similar data format (normalization). Then, this kind of data leads to the digital twin data (DTD) model (stage 3). There, parts of the infrastructure (nodes, links, and sensors) are shown as a portion of the observable infrastructure. The engine of risk score (stage 4) assesses each collected measurement or indication while designating a higher score for the affected area of interest. In the case of severe events, the priority telemetry (router) arranges, at stage 5, the related data as high or emergency level. In the 6th stage, the dashboard / API (application programming interface) shows any alert to operators (of civil protection, and/or defense – stage 7), giving them the capability of inspecting the event which is correlated to the alarm, and accordingly to organize the appropriate response in the affected field. The first version includes the innovative perspective of integrating parts such as telecommunication telemetry, IoT sensors, various indicators, risk score, and priority classification into a lightweight workflow using an easy-to-understand single pipeline. Nevertheless, this version does not contain feedback (loop). This means that when the related information is acquired by the dashboard, by users, and/or operators, any validation or decision cannot be fed into the model for producing the necessary actions.

The second version includes the same functions (7 stages), but the updated system is more adaptive and further developed. As far as the stage add-ons, these include filtering and caching (stage 2), geographic information system (GIS), and asset condition (stage 3), with a final prediction of failure (stage 4). So, in this case, the edge collector (stage 2) not only sends all acquired telemetry to the central platform but also conducts filtering and caching. Filtering contributes to reducing not necessary or redundant data. It allows the system to concentrate on potential anomalies, changes, or even high-priority events. During an emergency (e.g., the hypothetical scenario), large volumes of telemetric data could overload the communication services. In addition to filtering, the cache function could greatly help when the backhaul connection is not stable or even not available due to power failures, various asset damages, or a special morphological surface. In the given case, the edge collector can store non-critical data (from telemetry) for a certain time and highly prioritize the transmission of elevated (high or emergency) risk information. It therefore ameliorates the operational status while preventing the loss of significant data (e.g., from the field). In this context, filtering reduces the inserted noise and bandwidth use, and at the same time, caching enhances resilience during fragmentary connectivity. Moving on to the third stage, the DT core is enhanced with GIS and information about the assets' condition. GIS provides information to the system about the location of every infrastructure part, wireless link, sensor, and node. It is important because the information on assets' locations, apart from various readings, plays a crucial role in understanding the severity of the event. In this example, if the wildfire has been validated as being present near a

village, then this could be of high importance, as many lives can be saved from immediate evacuation due to an on-time briefing. Also, the insertion of asset condition improves the updating of healthiness, battery condition, and status of repair (e.g., recent or not). Consequently, GIS, along with asset condition, could contribute to information retrieval based on "location of an anomaly" and the "importance and/or vulnerability" of a specific asset, respectively. As far as the risk score (stage 4), it is extended into a risk analysis and failure-prediction engine. As a result, the system not only conducts an evaluation of the current state of the network and/or sensors, but also evaluates the probability of a near-future failure occurrence. So, the prediction of a failure initiates a proactive effect instead of reactive procedures. In accordance with the example of wildfire, a wireless sensor that in the previous period exhibited an increase in packet loss, a decrease in SNR, or malfunctions in battery levels, then the V2 of the system can classify the above sensor's condition to be degraded before the occurrence of the final outage. In dual-use applications, these types of predictions benefit the operators as they can take measures before the total failure of the ecosystem.

One major addition of V2 is the layer security and policy management (Figure 3), which poses various rules and generally manages all the parts of the architecture. Furthermore, it is defined here the data access clearance and visibility of telemetry streams (and to whom). Another major addition is the feedback loop. For the specific wildfire scenario, as soon as the dashboard produces an emergency alert, then the team on the field may approve the event to be real, sensors are not working properly, or/and wireless links were degraded, not due to fire but due to other environmental reasons. The validation is led to the DT core for the purpose of updating the detected condition of the affected area. In turn, the risk score and priority telemetry become more accurate over time. So, the lightweight and one-way pipeline (V1) is transformed into a closed-loop NDT (V2). The enhanced system not only has the ability to observe and alert accordingly, but it is also updated internally, based on validation originating from operational feedback. In this way, the second version is more appropriate for dual-use applications where the users (from civil protection or defense support) have predetermined access, enhanced and adaptive situational awareness.

3.1. Necessity of both proposed architecture versions

For clarifying each version's use, the specific goal orientation of the two types is presented (Tables 1 and 2). TeleReNT V1 can be compared to existing systems, whose integration follows an easy path with already implemented technologies such as current network monitoring schemes, common IoT platforms, and various dashboard environments. So, fewer updates and add-ons are needed on the architectural level, and therefore, it can be used for rapid prototyping and validation with a reduced prospect of faulty adoption by a candidate integrator. On the contrary, TeleReNT V2 is the complete potential of the proposed innovational scheme, but it needs more large-scale changes, such as an edge collection mechanism, a feedback and update mechanism, interoperability interfaces, and consequently, this model acts as a structured DT data platform. It is definitely more powerful on the awareness level, but also is more complicated from the aspect of integration. Consequently, V1 refers to the present while V2 refers to future capabilities and innovative logic of NDT technology.

Table 1. Purpose of each stage for both system versions (stages with " * " beside them indicate system V2)

Architecture stage	Operational purpose	System Version
Stage 1: Telemetry Sources	Acquirement of heterogeneous telemetry from: • Telecommunication infrastructure • Wireless links and IoT • Environmental sensors, field alarms • Battery status • Operational logs This data is relevant to real-world measurements, which are needed for DT workflow.	V1 & V2
Stage 2: Edge Collector	The Edge Collector assembles the incoming telemetric data using various protocols such as SNMP, MQTT, LoRaWAN, and LTE/5G and converts them into a unified form intended for producing a risk score and the DT representation.	V1 & V2
Stage 2 *: Filtering and Cache	• The edge collector conducts the filtering and caching locally. • Filtering contributes to reducing not-so-important telemetric data (e.g., redundant), • While caching has the role of maintaining data during problematic connectivity (e.g., intermittent communications). • The usefulness is profound in mountainous areas and areas of dual use (emergency and defense support).	V2 only
Stage 3: DT Data Model (Core)	• The DT shows the infrastructure under surveillance in the form of a structured model containing: Links, sensors, states of operation, time series data, asset-relevant information, and relationships. • Raw telemetry is described as a part of a virtual representation of the monitored targets and physical network.	V1 & V2
Stage 3 *: GIS and Asset Condition	These add-ons lift the expectations from the DT core to perform at an enhanced level. The system now knows: • the site of the incidence, • the assets that are affected, • the condition of the assets (e.g., full operation, degraded, in critical state, battery suffering)	V2 only
Stage 4: Risk Score	Every node, link and sensor is assigned a normalized risk score based on the following: • Signal-to-noise ratio (SNR) • Received Signal Strength Indicator (RSSI) • Packet loss • Latency • Battery condition and temperature • Environmental measurements and asset condition (criticality) • Alarm frequency	V1 & V2
Stage 4 *: Predictive Analysis / Failure Prediction	In this version, the risk score includes prediction characteristics. There is not only a classification of the acquired asset's condition but also an estimation relevant to the degradation or failure in the near future of a communication link, sensor, node, or any part that is capable of communicating.	V2 only

Architecture stage	Operational purpose	System Version
Stage 5: Priority Telemetry (Router)	• There are classifications of degraded communications during emergent critical conditions: Low, medium, high or with emergency priority (urgent). • Various data messages from assets under crisis, along with critical alerts, are maintained and transmitted with the highest priority, i.e., before any typical telemetric data.	V1 & V2
Stage 6: Dashboard	The stage of Dashboard /API produces the visual result of information for various types of users (e.g., civil-protection and defense support) such as: • Alerts and nodes status • Risk scores • Other useful information (intended additionally for future implementation) • It can also expose selected information to users with a specific clearance through the application programming interface (API).	V1 & V2
Stage 7: Civil-Protection and Defense-Support	The platform sustains multiple types of users and multiple user groups. These include: • Network operators and field teams • Civil-protection authorities and defense support • Technical maintenance • Relevant to the operational role, each group has a different capacity for output clearances.	V1 & V2
Layer Security and Policy Management *	• There is a cross-layer (stage that communicates with all others) which supervises the data visibility, access control, role permissions, and operational policies across all other stages (1-7). • This layer stage is a group of rules and regulations (a unified mechanism) and is visualized as a common layer to all other stages.	V2 only
Closed-loop Feedback*	• The closed-loop helps the system to be properly updated and, in this way, to enhance its performance. • The updates include validated information from various users, dashboards, or teams in the field. • All the acquired information is led back to the DT core. So, the system becomes an adaptive closed-loop NDT architecture.	V2 only

Table 2. Comparing the two versions of the proposed architecture (TeleReNT)

Version	Advantages	Limitations
TeleReNT V1: Lightweight Prototype	• Easier integratiom • Compatible with current monitoring systems • Early pilot testing • Reduced infrastructure changes • Risk scoring	• Limited DT functionality • No full security/policy layer • Absence of closed-loop feedback

Version	Advantages	Limitations
TeleReNT V2: Closed-Loop NDT	• Fully supports DT Core, edge collection, and predictive analytics • Dashboard integration and feedback updates • Better suited for dual-use resilience scenarios.	• More complex (requires additional engineering effort) • Requires more data for governance, extensive cybersecurity, and operational validation.

3.2 Dual-use operational concept

The platform can serve dual-use applications, and it is based on already available technology of telecommunications, IoT, and high-performance monitoring. Relevant to civil-protection capabilities, these include coordination of various field teams, wildfire sensing, infrastructure monitoring, and any customized sensor as long as it has any kind of connectivity interface (I/O, input output) [4, 32, 33]. In parallel, defense applicability is based on the same technology on the condition that it will be used to improve operational consistency by supervising and monitoring the selected communication links, sensor status and availability, and health of all interconnected assets in various kind of environments such as remote or degraded ones (DDIL - Disconnected, Denied, Intermittent, and Limited or DIL - Disconnected, Intermittent, and Limited). So, the most significant point of view in this case is that through the proposed technology, the value of its implementation is enormous because it offers resilience that it can compensate against not needed inclusion of weapon-based tactics. It is due to the existence of situational awareness, the immediate classification, dispatching of telemetry levels (e.g., low or high), and the support of various technical or military teams, when the connectivity is degraded [40, 41, 44, 45]. The first version supports, as aforesaid, a realistic deployment, and the second version corresponds to a platform that includes security and policy management, while the inserted feedback provides real-time updates from various sources (e.g., sensors and operators) for making the final system more adaptive and proactive [1, 3, 44].

4. Methodology and Simulation Concept

4.1 Description, simulation strategy and assets

For conducting a representative experiment of the proposed work and for proving the validity of the proposed platform, an octave-compatible code was constructed for implementing an enhanced lightweight prototype of the TeleReNT twin based on the introduced 7-stage pipeline. The simulation is based on V1 of the proposed architecture, as it already includes the core logic (from telemetry to decision), which is needed for evaluating the feasibility of the proposed NDT. Despite the fact that V1 is presented as the basic version of the architecture, the final implementation at the simulation level is not limited only to the simplicity of proof of concept. It furthermore contains an inventory of wireless links, FTTH, IoT sensors, an edge node, and various heterogeneous telemetric variables. The simulated scenarios include two operating modes, such as normal conditions and a wildfire case, normalized risk indicators, classification of asset states, priority telemetry assignment, dashboard, and outputs of CSV datasets. These CSVs are relevant to a final level of asset reporting. Also, the code is rule-based for supporting an early field pilot before replacing the code-generated data with real-world measurements.

The V2 architecture was not considered for simulation (in full) because its additionally proposed mechanisms, consisting of the layer security and policy management, the closed loop

validation from the field, and the adaptive DT updating process, need feedback, role definitions of users, real records, and validated data from the real action field. The previous mechanisms would fit perfectly for a near-future study relevant to a real-world deployment of the system. So, V2 is considered to be the subsequent evolution of V1 under validation. In parallel, the presented simulation provides all the technical facts and the basic elements on which the evolved version can be supported.

A transparent case study of a wildfire scenario is used for the proposed Digital Twin workflow. The selected properties (e.g., asset types, geographic coordinates) are engineering assumptions used for testing the behavior of the proposed decision pipeline. They should not be treated as an optimized deployment plan, a sensor-placement methodology, or field-validated recommendations for positioning IoT devices. Instead, the purpose of the case study is to demonstrate the transformation of heterogeneous telemetry and assets' condition into normalized risk indicators, operational states, and telemetry-priority decisions. The same workflow can be adapted to other civil protection or defense-support scenarios after specialized calibration and validation. All the values that are used on the simulation level are generated and/or included in the constructed code, and various rules apply that will be discussed later in this section. Consequently, the used data are not considered operational, but instead they are constructed based on a logical way for accomplishing an adequate portion of real-world conditions. One important purpose is to show the mechanism of the V1 workflow from telemetry to decision, just before the calibration with measurements under real conditions. Also, the GIS coordinates and any asset metadata are used only for spatial labeling of each asset, and they are not yet used for advanced spatial study or for providing adaptation through a closed-loop. Therefore, the full potential of this data is intended for the V2 architecture.

Both scenarios utilize the same type and number of assets: 16 wireless links, 3 FTTH zones, 60 IoT sensor nodes, and 1 edge node, resulting in a total of 80 monitored assets (Table 3). This assures that the normal and wildfire scenarios are based on the same system blocks, and indeed, the experimental differences in various variables are caused by telemetry alteration rather than by changing the system size.

Table 3. Type and name of simulated assets

Asset type	Normal scenario	Wildfire scenario	Name of assets and range
Wireless links (PtP/PtMP)	16	16	from WL-001 to WL-016
FTTH zones / cabinets	3	3	from FZ-001 to FZ-003
IoT sensors	60	60	from IS-001 to IS-060
Edge node	1	1	EN-001
Total assets	80	80	Common for both scenarios

4.2 Randomization and sample generation for the scenario of "normal conditions"

The constructed code uses deterministic randomization so that the results are repeatable by employing the "seed" function. Essentially, the "rand" function is used, i.e., uniform randomness. The following equation (1) is used for producing the needed values for the experiment, and it is a uniform random variable with a probability density function (PDF) of $f(u) = 1$ for $0<u<1$, otherwise

equal to 0. So, the values can be produced with a range of values [a, a+b] by employing equation (a + bU)

$$U \sim \text{Uniform}(0,1) \quad (1)$$

For alarm/ticket counts, the simple Poisson logic is used inside the code. So, relevant to these counts, there are no fixed values, because under real conditions, alarms/tickets could appear as random events. Instead of reporting that each sensor always exhibits 1 alarm, it would be proper to report that each sensor has a small probability of displaying an alarm at each time sample. In this way, the Poisson logic works. When λ is small, e.g., 0,05, most values correspond to 0 alarms, sometimes 1 alarm, and rarely 2 or more. An important fact in the current code is that the seed function is set once at the beginning. So, the normal and wildfire scenarios are reproducible. Obviously, alarm and ticket counts are generated by using a simple Poisson process (equation 2), because these variables correspond to discrete operational events that could occur irregularly over time. Specifically, during this simulation, the two scenarios (normal and wildfire) are generated from a similar type of random stream. Consequently, both of these scenarios could be reproduced, but they do not use the same scheme of generating data. In the case of the wildfire scenario, a similar type of baseline is produced randomly (compared to the normal scenario), but it includes injections of controlled network and environmental disturbances into selected system assets. The two produced baselines are shown qualitatively in equation (3).

$$P(X = k) = \frac{e^{-\lambda} \cdot \lambda^{k}}{k!}, \text{ όπου } k = 0, 1, 2, 3, \ldots \quad (2)$$

$$\begin{aligned} \text{normal values} &= \text{baseline A} \\ \text{wildfire values} &= \text{baseline B} + \text{wildfire injections} \end{aligned} \quad (3)$$

The following relationships, which are shown in Table 4, apply to the normal scenario (A) and constitute the initial baseline for the wildfire scenario (B) before the disturbances are introduced. The same statistical baseline is used in both scenarios, but not the same numerical baseline (please see equation 1, i.e., $U_A \neq U_B$). Notably, from the full telemetry table, focus can be given on some of the meaningful parameters for the V1 simulation: packet loss (%), received signal strength indicator (RSSI – dBm), throughput (Mbps), uptime (%), battery level (%), alarm count (count/sample), fault tickets (count/sample), and restoration time (hours). The aforementioned variables give the potential of network reliability under test, the condition of wireless links, device autonomy, and various impacts. The variables of packet loss, throughput, and uptime are relevant to the viability of the communication service. Specifically, RSSI calculates the quality of the wireless signal, and the battery level indicates the autonomy of the corresponding field sensors and other devices. Also, alarms, fault tickets, and restoration time are connected with the fact of operational degradation and the imminent maintenance procedures. All the variables are shown in brief, along with their mode of operation, in Table 5.

Table 4. Generation of Baseline values for the normal scenario (in some cases, the values are intentionally degraded to take into account the worst-case scenario, even under normal conditions)

Variable	Wireless links (→ value range)	FTTH zones (→ value range)	IoT sensors (→ value range)	Edge node (→ value range)
Latency (ms)	25 + 20U → 25–45	5 + 12U → 5–17	70 + 90U → 70–160	10 + 10U → 10–20
Packet loss ratio, PLR, (×100 = %)	0,005 + 0,020U → 0,005–0,025	0,001 + 0,008U → 0,001–0,009	0,010 + 0,030U → 0,010–0,040	0,001 + 0,005U → 0,001–0,006
SNR (dB)	22 + 8U → 22–30	30 + 5U → 30–35	12 + 13U → 12–25	30 + 5U → 30–35
RSSI (dBm)	-78 + 15U → -78 to -63	-60 + 5U → -60 to -55	-96 + 25U → -96 to -71	-60 + 5U → -60 to -55
Throughtput (Mbps)	50 + 70U → 50–120	200 + 300U → 200–500	0.05 + 0.20U → 0.05–0.25	100 + 200U → 100–300
Uptime (%)	98 + 2U → 98–100	99 + U → 99–100	96 + 4U → 96–100	99 + U → 99–100
Battery (%)	90 + 10U → 90–100	100 fixed	55 + 40U → 55–95	80 + 15U → 80–95
Temperature (°C)	28 + 12U → 28–40	22 + 12U → 22–34	18 + 14U → 18–32	30 + 10U → 30–40
Humidity (% RH)	35 + 35U → 35–70	35 + 35U → 35–70	35 + 45U → 35–80	35 + 35U → 35–70
CO_2 sensor (ppm)	410 + 30U → 410–440	410 + 25U → 410–435	405 + 45U → 405–450	410 + 30U → 410–440
Alarm (count/sample)	P(λ=0,08) *	P(λ=0,04) *	P(λ=0,05) *	P(λ=0,03) *
Fault tickets (count/sample)	P(λ=0,02) *	P(λ=0,03) *	P(λ=0,01) *	P(λ=0,01) *
Restoration time (hours)	0,2 + 2U → 0,2–2.2	1 + 4U → 1–5	0,5 + 3U → 0,5–3.5	0,2 + U → 0,2–1,2
Optical loss (dB)	0	0,20 + 0,80U → 0,20–1,00	0	0

* where P(λ) refers to Poisson (λ = value), and λ means that λ alarms are expected on average per sample.

Table 5. Variables and their mode of operation.

Variable	Unit	Explanation
Latency	ms	Network Delay / Transfer Delay: It is used as a basic QoS variable.
Packet loss	ratio ή %	Packet loss ratio: In the code is referred to as a ratio, e.g. 0,055 = 5,5%.
SNR	dB	Signal-to-noise ratio: This is relevant to radio signal quality.
RSSI	dBm	Received signal strength indicator: It is a negative value and its value, and the closer of being to 0, the stronger the signal is.
Throughtput	Mbps	Available data rate: Refers to the capacity of the communication link.
Uptime	%	Availability - continuity of operation.
Battery	%	The remaining battery levels of field devices and/or sensors.
Temperature	°C	Environmental or device temperature.
Humidity	% RH	Relative humidity refers to the amount of water vapor in the air compared to the maximum amount that the air can hold at a specific temperature.
CO_2 sensor	ppm	The CO_2 concentration.

Variable	Unit	Explanation
Alarm	count/sample	Number of alarms in a one-time sample. It is generated by Poisson.
Fault tickets	count/sample	Number of maintenance/fault tickets in one time sample. It is generated by Poisson.
Restoration time	hours	The estimated restoration or repair time.
Optical loss	dB	Optical attenuation / insertion loss in fiber infrastructure.

4.3 Randomization and sample generation for the scenario of "wildfire conditions"

The wildfire scenario does not alter the number of assets. Instead, it varies specific values of predetermined assets at specific time points (Table 6). The affected sensors are IS-012, IS-015, IS-018, IS-021 and IS-024. The start point of altering sensor conditions is at sample 55. Based on the fact that each sample is produced every 5 minutes, sample 55 corresponds to about (55-1) x 5 min. = 270 min = 4,5 hours from the simulation beginning. Specifically, the simulation uses a five-minute sampling interval because each sample is fixed at the operational state of the monitored assets during a five-minute time step. This hypothesis is introduced to reduce unnecessary data volume and computational burden. In the proposed model, most network, IoT, and environmental variables do not need to exhibit new data, as we consider that the wildfire scenario reveals updated conditions every 5 minutes (meaning that between two samples, the conditions are changing slightly toward the next sample's virtual measurements). It must be noted that every sample contains new values relevant to Table 5. Therefore, the five-minute interval allows the prototype to show meaningful changes while avoiding producing large volumes of unneeded telemetry.

Table 6. Variables affected from wildfire injection.

Variable	Range (Normal)	Wildfire injection	Resulting raw sensor range before smoothing
Temperature (°C) *	18–32	+24 + 8U → +24 to +32	42–64
Humidity (% RH) *	35–80	-25 - 8U → -25 to -33	2–55 → clamped to 5–55
CO_2 sensor (ppm) *	405–450	+250 + 100U → +250 to +350	655–800
Alarm (count/sample) *	P(λ=0,05)	+ P(λ=2,0)	≃ P(λ=2,05)
Battery (%) *	55–95	-10 - 5U → -10 to -15	40–85 (bounds of 1, 100)
Latency (ms) +	25–45	+80 + 30U → +80 to +110	105–155
Packet loss (%) +	0,5–2,5	+10 + 6U → +10 to +16	10,5–18,5
SNR (dB) +	22–30	-12 - 4U → -12 to -16	6–18
RSSI (dBm) +	(-78) – (-63)	-15 - 5U → -15 to -20	-98 to -78
Throughtput (Mbps) +	50–120	× 0.35	17.5–42 (min bound of 0)
Uptime (%) +	98–100	-6 - 2U → -6 to -8	90–94 (bounds of 0, 100)
Alarm (count/sample) +	P(λ=0,08)	+ P(λ=1,5)	≃ P(λ=1,58)
Fault tickets (count/sample) +	P(λ=0,02)	+ P(λ=0,5)	≃ P(λ=0,52)
Fault tickets (count/sample) ◆	P(λ=0,03)	+ P(λ=0,4)	≃ P(λ=0,43)
Alarm (count/sample) ◆	P(λ=0,04)	+ P(λ=0,6)	≃ P(λ=0,64)
Restoration time (hrs) ◆	1–5	+3 + 2U → +3 to +5	4–10

* The wildfire-affected sensors become hotter, drier, with higher levels of detected CO_2, exhibiting greater alarm activity, and battery stressing; + The wildfire scenario affects selected wireless links by altering various relevant variables; ◆ The FTTH zone is stressed and this is obvious through additional tickets, alarms, and altered restoration time.

Relevant to Table 6, the fact that must be underlined is the wildfire injection volume and its mechanism for producing a sensor behavior similar to detected wildfire conditions. The raw sensor range (*) comes from the addition of normal scenario's values with those of the wildfire injection, e.g. temperature (°C) (raw) = range (normal) + range (wildfire) = [18+24, 32+32] = [42, 64], so temperature in the specific wildfire scenario ranges from 42°C to 64°C. Therefore, the simulated wildfire temperature range corresponds to nearby environmental heating and early-warning sensing, and not in any case the direct exposure of the corresponding sensor node to flames.

The wildfire injection mechanism, relevant to humidity (% RH), can produce a range of [2%, 55%]. It is obvious from Table 6 that there is a clamping at 5%, indicating that this is the lower bound. It is a constraint based on practicality rather than literature derivation. The purpose is to prevent the produced value of humidity from taking unrealistic values (e.g., low, negative) in the wildfire scenario. Values below the level of 5% would not be meaningful for contributing to the risk score (will be analyzed later), while a false value would lead to a faulty interpretation of the dataset. Consequently, the clamp leads to numerical stability and, in turn, to a reasonable potential for real-world implementation without assuming that the value of 5% RH is an environmental bound.

In general, after the wildfire injection technique, selected data (telemetric variables) are bounded or smoothed to be closer to naturally detected conditions. Edge-level smoothing (edge collector) is accomplished with a moving average of five samples (equations 4 and 5). The general mathematical expression corresponds to equation 4, while equation 5 is the implemented one for including the first samples (<4). Since every sample corresponds to a telemetry snapshot of five minutes, the corresponding moving average being conducted at the edge collector provides a 25-minute smoothing window. Each processed value is therefore computed from the current sample and the previous four samples. Its aim is to minimize as much as possible the telemetry noise and to avoid exaggerating relevant to some isolated sample fluctuations without nevertheless affecting the emergency alerts. The scenario takes into account that the wildfire conditions extend over consecutive samples, permitting the moving average to sustain a degradation strain. In real-world implementation, the emergency thresholds should not be smoothed to provide the necessary escalations in the presence of critically detected conditions.

In more detail, the wildfire scenario has a discrete disturbance mechanism. Environmental anomalies are introduced first, at sample 55, extending almost 4,5 hours after the beginning of the simulated period. This corresponds to an early-warning phase in which selected IoT sensors detect nearby wildfire before the occurrence of communication degradation. Also, wireless links and FTTH disturbances are introduced later, at sample 75, corresponding to 6 hours and 15 minutes. This tactic of escalating at different time points contributes to an environmental stress being detected first, and then communication links and fixed infrastructure are affected later due to propagation degradation, instability, and stress to the rest of the infrastructure. Unaffected assets exhibit normal operation while providing behavior for reference and comparison purposes (Table 7).

$$\bar{x} = \frac{1}{5}\sum_{k=0}^{4} x_i(t-k) \tag{4}$$

$$\bar{x_t} = \frac{1}{n_t}\sum_{\tau=\max(1,\ t-M+1)}^{4} x_i(\tau), \quad M = 5 \tag{5}$$

$$\text{where} \quad n_t = t - \max(1, t - M + 1) + 1$$

From Table 6, it is also obvious that the wireless-link (+) degradation occurred near the wildfire event, with affected links of WL-004, WL-008, and WL-013. The wildfire scenario affects selected wireless links by increasing their delay and loss, decreasing radio quality, reducing throughput and uptime, while increasing alarms and tickets. Also, the start point of the degradation is at the 75th sample (time = [75-1] x 5 = 370 minutes = 6 hours and 10 minutes). The FTTH (◆) operational impact is relevant to zone FZ-002 with a start point at the 75th sample. It must be noted that the FTTH zone is not intended to be destroyed at the simulation level, but instead, it receives an increased operational burden through an increased number of tickets, alarms, and longer estimated restoration time.

In the current simulation, the edge node is not correlated to the wildfire injection. It is simulated by its baseline telemetry generation rules in both the normal and wildfire scenarios. Alarm counts and fault tickets can be considered as low-rate baseline Poisson events. This assumption keeps the local edge-processing layer up and running, allowing the scenario to be simulated relevant to environmental sensing, wireless-link degradation, and FTTH operational impact.

Table 7. Asset behavior under baseline and wildfire conditions

Asset type	Asset IDs	Wildfire injection	Baseline behavior	Wildfire behavior
Affected IoT sensors (start at ~ 4.5 h) - 1st sample of disturbance → 55	IS-012, IS-015, IS-018, IS-021, IS-024	Yes	Normal IoT-sensor rules for temperature, humidity, CO_2, battery, and alarms.	Environmental stress is injected: temperature and CO_2 increase, humidity and battery decrease, alarm counts increase.
Wireless links (start at ~6.2 h) - 1st sample of disturbance → 75	WL-004, WL-008, WL-013	Yes	Normal wireless-link rules for latency, packet loss, SNR/RSSI, throughput, uptime, alarms, and tickets.	Communication degradation is injected: latency and packet loss increase, SNR/RSSI decrease, throughput and uptime decrease, and alarms/tickets increase.
FTTH zone (start at ~6.2 h) - 1st sample of disturbance → 75	FZ-002	Yes	Normal FTTH rules for alarms, tickets, restoration time, and optical loss.	Operational degradation is injected: alarms, fault tickets, and restoration time increase.
Unaffected wireless links (medium-criticality)	WL-002, WL-006, WL-011, WL-016	No	Normal wireless-link rules.	No wildfire disturbance. Communication links as reference

Asset type	Asset IDs	Wildfire injection	Baseline behavior	Wildfire behavior
Other unaffected wireless links	Remaining WL assets	No	Normal wireless-link rules.	No wildfire disturbance.
Unaffected FTTH zones	FZ-001, FZ-003	No	Normal FTTH rules.	No wildfire disturbance. They remain critical reference zones.
High-criticality but unaffected IoT sensors	IS-001, IS-006, IS-017, IS-031, IS-046	No	Normal IoT-sensor rules.	No wildfire disturbance. They remain important supporting sensors as a reference.
Medium-criticality but unaffected IoT sensors	IS-002, IS-008, IS-013, IS-022, IS-036, IS-051	No	Normal IoT-sensor rules.	No wildfire disturbance. They serve as comparison showing that the wildfire impact is localized.
Other unaffected IoT sensors	Remaining IS assets	No	Normal IoT-sensor rules.	No wildfire disturbance.
Edge node	EN-001	No	Follows edge-node rules.	No wildfire disturbance. It remains operational to support edge processing and dashboard service.

4.4 Geographic distribution and operational importance of assets

Spatial metadata are produced and assigned to all assets in the simulation. Each wireless link, FTTH zone, IoT sensor, and edge node is determined by a pair of geographic coordinates, named as latitude and longitude values, which are found in a preset bounded area. Specifically, the simulated asset coordinates are produced through a uniform distribution, not a normal distribution. For each asset, latitude and longitude values are designated within a preset geographic window using equation 1. Therefore, assets are randomly distributed across the bounded area with the same probability (Table 8), without producing a swarm around a central point. The coordinates are used as reference points for traceability and visualization, and rather than as active inputs whose location can affect the risk-scoring model. In simple words, the current simulation produces the location of each, but the computed risk score, state, and priority are affected by telemetry variables, which were already mentioned previously. The criticality field and operation strategy govern each asset by using predefined rules.

The produced geographic coordinates have a point of reference around the wider region of Ioannina in Epirus, Greece. Notably, the values of geographic coordinates (latitude, longitude), which are equal to (39,60 , 20,75), define a point of interest at the Zitsa area (being at the lower-left corner of the simulated latitude–longitude window, while the added random uniform component distributes the assets within a bounded area). The selected point of reference corresponds to a semi-rural and mountainous setting for assessing wildfire sensing, telecommunications resilience, and edge-based monitoring.

Table 8. Geographic distribution

Metadata variable	Assignment rule	Simulated range	Interpretation
Latitude	(39,60 + 0,15U)	From 39,60 to 39,75 degrees	Code generated latitude assigned to asset.
Longitude	(20,75 + 0,15U)	From 20,75 to 20,90 degrees	Code generated longitude assigned to asset.

Relevant to the simulated area, it is assumed that there are 80 monitored assets that are supported by intermediate communication infrastructure, including some wireless relay points, LoRaWAN gateways, and backhaul links. These elements are not included as separate assets with a risk score, but instead, they are considered as communication infrastructure supporting the monitored wireless links, FTTH zones, IoT sensors, and edge node for operating over a wider mountainous area. Nevertheless, a real pilot would require, prior to deployment, a coverage study along with specific site radio planning. The aforesaid are mentioned because the simulated area (equations 6 to 8) has an approximate size of almost 215 km² [46, 47, 48]. With a lower degree spread, the simulated area could be reduced to almost 15 km² or 9 km² (Table 9). Still, the larger area of 215 km² (Appendix A) was retained for representing an early-warning scenario rather than a small local fire-detection deployment. At this selected area scale, a volume of 80 assets is justified as a distributed monitoring and communications resilient network for covering forests, rural areas, infrastructure, and access-link zones before a wildfire directly impacts the entire area.

$$\text{Latitude span} \simeq 111{,}32 \times \text{d km} \tag{6}$$

$$\text{Longitude span} \simeq 111{,}32 \times \cos(\text{latitude}) \times \text{d km} \tag{7}$$

$$\text{Area} \simeq \text{Latitude span} \times \text{Longitude span} \tag{8}$$

Table 9. Area size for different degree spreads

Degree spread	Latitude span	Longitude span at 39.60°	Estimated area
0.15°	≃ 16.7 km	≃ 12.9 km	≃ 215 km²
0.04°	≃ 4.45 km	≃ 3.43 km	≃ 15.3 km²
0.03°	≃ 3.34 km	≃ 2.57 km	≃ 8.6 km²

4.5 Risk score

The introduced risk score is designed as an important decision metric that converts heterogeneous telemetric data into a single normalized value between 0 and 1 [49]. The purpose is to rate various assets according to their operational condition while sustaining state classification and telemetry prioritization. In the proposed architecture, this scoring technique helps to identify which wireless links, FTTH zones, IoT sensors, or edge assets need monitoring, inspection, or priority data transmission. The risk components (Table 10) are related to wireless-link quality, communication performance, field/environmental stress, and device autonomy [50]. The risk score is computed based on equation 9.

$$\begin{aligned}\text{Risk} = {} & 0.22 \times \text{LatencyRisk} + 0.25 \times \text{LossRisk} + 0.20 \times \text{QualityRisk} + 0.15 \times \text{BatteryRisk} + \\ & 0.08 \times \text{TemperatureRisk} + 0.10 \times \text{AlarmRisk}\end{aligned} \tag{9}$$

Before this weighted sum is applied, the raw telemetry values are transformed into normalized risk indicators in the interval of [0,1] (please see Appendix B). When the variables have higher values, which are worse, such as latency, packet loss, temperature, and alarm count, the

normalization increases with the increase of the raw value. Otherwise, for variables with lower values being worse, such as battery level, then the normalization increases with the decrease of the raw value (Appendix B). Packet loss has been set to the highest weight because faulty telemetry directly affects service continuity. Specifically, in applications of emergency or defense monitoring, a lost message is usually more severe than a delayed message. Latency is the second severe condition in the hierarchy because delayed telemetry reduces operational value, with a possibility of remaining usable. Wireless quality related to SNR and RSSI is strongly weighted because poor radio performance is often present prior to packet loss or link degradation. Also, battery risk is included for including sensor autonomy, while the variables of alarms and temperature are related to field conditions and environmental factors.

This weighting method implies that communication-failure indicators (their sum) dominate the risk score by 67% (0,25 + 0,22 + 0,20 = 0,67) while field/device-condition indicators contribute by 33% (0,15 + 0,10 + 0,08 = 0,33). This is appropriate for the proposed prototype because it is fixed as a telecommunications/IoT resilient system rather than as a standalone wildfire-detection model.

Table 10. Risk components

Risk component	Weight	Interpretation
LossRisk	0,25	The highest weight because packet loss corresponds to the telemetry that may not be delivered.
LatencyRisk	0,22	High weight because delayed telemetry reduces operational condition.
QualityRisk	0,20	Related to SNR/RSSI degradation as an early indication of wireless-link weakness.
BatteryRisk	0,15	Field-device autonomy related to possible sensor outage.
AlarmRisk	0,10	Indicates event's presence or operational load, while possibly including false positives and repeated alerts.
TemperatureRisk	0,08	Indicates abnormal temperature increase. It is assigned the lowest weight because the simulation is designed primarily to assess telecommunication resilience, and not to operate as a dedicated wildfire detection model.

After the calculation of the risk score, the system maps each asset to an operational state governed by Table 11. The state is also combined with asset criticality for determining priority in telemetry services. In simple words, the score is used to change the raw telemetry into asset state and telemetry priority. The priority order is given by equation 10. This order presents the following objective: preserving communication reliability first, while still incorporating device and environmental conditions as supporting indicators. The weights should therefore be considered as the initial engineering assumptions for a prototype under development. They are not claimed to be universal constants and should be recalibrated using various real pilots.

$$\text{Packet loss} > \text{Latency} > \text{Wireless quality} > \text{Battery} > \text{Alarms} > \text{Temperature} \quad (10)$$

Table 10. Risk Classification and Telemetry Priority

Risk range	Assigned state	Additional condition	Assigned priority
Risk < 0.35	Normal	Criticality = 1	Low
Risk < 0.35	Normal	Criticality ≥ 2	Medium
0,35 ≤ Risk < 0.55	Watch	Any criticality	Medium

0,55 ≤ Risk < 0.75	Degraded	Criticality = 1	Medium
0,55 ≤ Risk < 0,75	Degraded	Criticality ≥ 2	High
Risk ≥ 0,75	Critical	Criticality = 1	Medium
Risk ≥ 0,75	Critical	Criticality = 2	High
Risk ≥ 0,75	Critical	Criticality = 3	Emergency

If the asset is degraded or critical, but has a criticality of 1, then the high/emergency priority is not initiated. The final priority depends on the introduced rule of equation 11. This means that priority is not only determined by risk/state, but also by the operational importance of the asset. Therefore, the assigned state shows the current compromised status of the asset: Normal, Watch, Degraded, and Critical. Criticality shows the importance of the asset: 1 = low, 2 = medium, 3 = high, while priority presents the way that the asset's telemetry should be forwarded (quickly / importance). It should be noted, though, that the priority rules are evaluated sequentially from top to bottom, so that emergency priority overrides High, Medium, and Low priority conditions. For example, when S=3 and C=3, the second condition of S≥2 and C≥2 also applies, but it should give assigned priority = 4 (corresponds to Emergency), and not value of 3 (corresponds to High).

$$\text{Priority} = f(\text{State, Criticality})$$

$$\text{Priority}(S, C) = \begin{cases} 4, & S = 3 \text{ and } C = 3 \\ 3, & S \geq 2 \text{ and } C \geq 2 \\ 2, & S \geq 1 \text{ or } C \geq 2 \\ 1, & \text{otherwise} \end{cases} \quad (11)$$

where, S=State, C=Criticality, P ∈ [1,2,3,4], where 1 = Low, 2 = Medium, 3 = High, and 4 = Emergency.

4.6 Analysis of the developed algorithm

The proposed architecture depends on two complementary algorithms. The main algorithm is directly related to the TeleReNT simulation, where telemetric data are generated and transformed (e.g., normalization) into risk scores that are relevant to asset states and mapped into telemetry properties. The auxiliary algorithm, which depends on exactly the same principles and properties, is a procedure used for supplementary post-processing and visualization issues, for generating spatial interpretations of various assets along with their distribution maps and time properties. As for the first six produced figures (main and supplementary algorithm), these are the same for both and are derived strictly from the same simulated outputs, ensuring that the results remain comparable between normal and wildfire scenarios. Specifically, the supplementary algorithm contributes to the geographic distribution of various assets and the spatial impact of the wildfire injection mechanism into the simulated design. In every case, the original telemetry, risk score, various states, conditions, and priority calculations remain exactly the same.

The following Tables 11 and 12 describe the algorithmic implementation used to generate and post-process the simulation outputs. The experimental results produced by these algorithms are presented separately in the next section. Table 11 shows a functional summary of the main simulation code. The table summarizes the purpose, inputs, processing stages, and outputs of compatible Octave code, which is used to simulate the normal and wildfire scenarios. Table 12 summarizes the post-processing procedure for producing spatial maps of various assets, area

diagnostics, final risk maps, and other significant summaries. Finally, the unified algorithmic workflow of the simulation is shown in Figure 4.

In the specific study, the term algorithm refers to the implemented prototype workflow (at the simulation level) in contrast to a newly proposed optimization or machine-learning algorithm. The objective here is not to determine the optimal physical placement of IoT sensors or to improve the accuracy of the sensing hardware. Instead, the developed workflow presents a proposed protocol for available or simulated telemetry streams being transformed into normalized indicators, risk scores, operational states, and telemetry-priority levels in a clear and repeatable procedure.

Table 11. Brief Description of the main simulation algorithm

Code step	Type and brief description of operations
1	Initialize the asset set, including wireless links, FTTH zones, IoT sensors, and the edge node.
2	Select the operating scenario: normal conditions or wildfire conditions.
3	Acquire or simulate telemetry for each asset, including latency, packet loss, SNR/RSSI, battery level, temperature, humidity, CO_2, alarms, tickets, throughput, and uptime.
4	Smooth the raw telemetry (Edge Collector) using a five-sample moving average.
5	Normalize every telemetry variable into a risk value between 0 and 1.
6	Build the digital-twin data model by linking each asset with its ID, type, criticality, GIS location, and associated infrastructure element.
7	Compute the risk score for every asset using the weighted risk model.
8	Classify asset into one operational states: Normal, Watch, Degraded, or Critical.
9	Assign the telemetry priority to Low, Medium, High, or Emergency, based on the criticality state and asset.
10	Generate dashboard outputs, including top risk assets, state maps, priority maps, and other comparisons.
11	Export the final datasets and figures for evaluation and reporting purposes.

Table 12. Brief Description of the supplementary spatial analysis algorithm

Code step	Type and brief description of operations
1	Load the existing simulation output object generated by the main algorithm.
2	Extract the asset inventory, including asset ID, asset type, criticality, latitude, longitude, and affected/unaffected status.
3	Define the wildfire-affected assets according to the scenario, including affected IoT sensors, wireless links, and the affected FTTH zone.

4	Calculate the total simulated area from the selected latitude and longitude limits.
5	Calculate the actual area occupied by the assets using their outermost generated coordinates.
6	Check the spatial distribution of the assets using approximate area, latitude/longitude span, nearest-neighbor distance, and grid-cell occupancy.
7	Generate a spatial asset distribution map by presenting wireless links, FTTH zones, IoT sensors, the edge node, and directly affected wildfire-scenario assets.
8	Generate spatial final risk maps (end of the scenario, i.e., T=120 samples / 10 hours) for the normal and wildfire scenarios.
9	Summarize every asset over time by calculating its average risk, maximum risk, step risk (final time), and the time percentage spent in each state and priority class.
10	Generate a wildfire priority frequency map showing how often each asset enters High or Emergency priority.
11	Export supplementary data and figures for spatial interpretation and reporting.

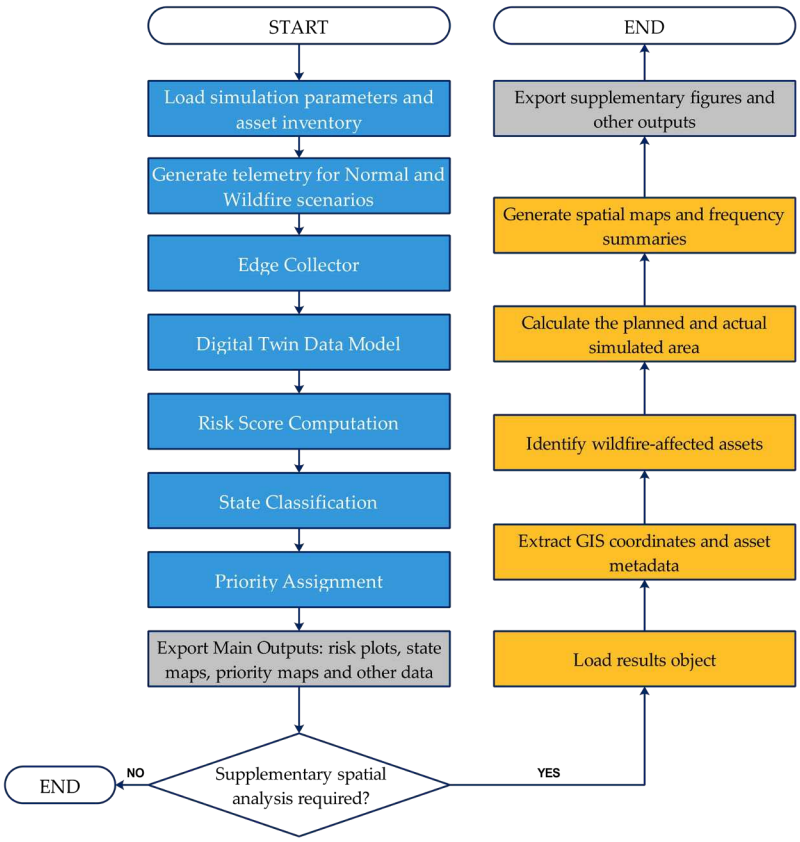


Figure 4. Algorithmic workflow and supplementary asset spatial analysis. The blue branch represents the main telemetry-to-decision pipeline, whereas the orange branch represents the supplementary post-processing procedure. The orange branch uses the original simulation code and results to generate spatial maps, asset-distribution outputs, and risk/priority frequency summaries.

5. Experiment and results

In this section, the simulation results are presented and generated by Octave-compatible code. The simulation generates virtual measurements relevant to telemetry for both types of scenarios. Then, it converts them into operational states, telemetry priority data, and risk scores. The main code produces six figures (windows), which include risk-score plots, state, and priority maps. Also, the simulation can export data to files, including simulation data schema, summary statistics, and various scenario outputs. The dashboard summaries (Table 13) report the final time-step condition of the 80 monitored assets for both scenarios. Comparing the normal scenario with the wildfire scenario, it leads to an increased number of watches and degraded assets, while no asset reaches the critical state or emergency priority level. This indicates a controlled early-warning degradation pattern. Specifically, under normal conditions, 73 assets remain in the normal state, and 7 assets enter the watch state, while no assets are found as degraded or critical. The corresponding priority distribution includes 54 of low priority and 26 of medium priority assets, without high or emergency telemetry priority. In the wildfire scenario, the final time step comparison shows a clear degradation pattern where 63 assets remain normal, 14 are classified as watch, and 3 enter the degraded state. No asset reaches a critical state or emergency priority level in the current configuration. These results indicate that the wildfire injection increases the operational stress and asset risk, but the scenario remains within a controlled early warning and resilient monitoring condition rather than representing full infrastructure collapse.

Table 13. Final time step for dashboard summary related to normal and wildfire scenarios

Scenario	Normal assets	Watch assets	Degraded assets	Critical assets	Low priority	Medium priority	High priority	Emergency priority
Normal	73	7	0	0	54	26	0	0
Wildfire	63	14	3	0	49	28	3	0

5.1 Simulation data schema and summary statistics

Before analyzing the graphical simulation outputs, the structure of the generated data should be analyzed first. The simulation data schema (Table 14) acts as a data dictionary for the proposed prototype, defining the meaning, type, example format, and operational purpose of each exported variable. It should be interpreted as predefined typical values. The actual telemetry values are produced dynamically (and not in a preset manner) by the simulation code through randomization rules, Poisson processes, and wildfire injection equations. Consequently, the schema is followed by summary statistics tables for producing a meaningful quantitative description of the generated data. Under normal conditions, telemetry statistics are classified by asset type, while under wildfire conditions, the statistics are classified employing directly affected assets and unaffected reference assets. This structure allows the reader to understand the expected numerical behavior of the simulation before moving to the interpretation of generated figures, risk scores, states, priorities, and spatial outputs.

Table 14. Simulation data schema

Field	Type / Unit	Illustrative example	Purpose
Timestamp	datetime	25/4/2026 19:55	Final time-step alignment
Asset ID	string	WL-004	Asset identifier

Field	Type / Unit	Illustrative example	Purpose
Asset type	Enumerated categorical variable	Wireless link / FTTH zone / sensor / edge node	Asset class used by the model
Zone name	String	Mountain backhaul	Operational zone or infrastructure group
Parent asset	String	EN-001	Related infrastructure element
GIS x / latitude	Floating point	39,675	Produced latitude coordinate
GIS y / longitude	Floating point	20,825	Produced longitude coordinate
Latency	Floating-point, ms	42,5	Network delay / QoS indicator
Packet loss	floating-point ratio	0.015	Packet-loss ratio (x 100 to obtain percentage)
SNR	Floating point, dB	22,8	Signal-to-noise ratio (wireless quality indicator)
RSSI	Floating point, dBm	-71	Received signal strength indicator
Throughput	Floating point, Mbps	85,4	Available communication capacity
Uptime	Floating point, %	98,7	Service availability indicator
Battery level	Floating point, %	83	Device autonomy indicator
Temperature	Floating point, °C	38,1	Device or environmental temperature
relative humidity	Floating point, % RH	45,2	Environmental humidity condition
CO_2 concentration	Floating point, PPM	720	CO_2 concentration / fire-warning indicator
Alarm count	integer or smoothed floating-point number	2	Recent alarm activity
fault tickets	integer or smoothed floating point	1	Maintenance / fault activity
Restoration time	Floating-point, hours	2,5	Estimated restoration or repair effort
Optical loss	Floating point, dB	0,62	Fiber / FTTH optical-loss indicator
Criticality	Integer, 1–3	3	Operational importance
Risk score	Floating point, 0–1	0,72	Computed risk score
State	Enumerated categorical variable	Normal / Watch / Degraded / Critical	Operational state classification
Priority	Enumerated categorical variable	Low / Medium / High / Emergency	Telemetry transmission class
Note	String	Final time-step record	Optional operator or reporting note

Note: Categorical / enumerated fields take one value from a predefined set of allowed labels. For instance, the *Asset type* is restricted to *wireless link*, *FTTH zone*, *sensor*, or *edge node*, while *state* and *priority* are restricted to the decision classes produced by the constructed model.

The normal scenario (Table 15) exhibits a consistent behavior across various asset types. FTTH zones and the edge node present the best communication performance, with low latency, low packet loss, high SNR/RSSI, high throughput, and uptime close to 99,5%. Nevertheless, wireless links show moderate latency and packet loss, but remain within the expected normal operating range. IoT sensors show higher latency, weaker RSSI/SNR, and very low throughput, which is consistent with a field detecting operation (of low-power) rather than with high-capacity communication. Also, their lower average levels of battery reflect the autonomous nature of these

field devices. Alarm and fault-ticket activity remains at low levels across all asset types, confirming (by definition) that the normal scenario does not refer to a degraded or emergency condition. Optical loss is related only to FTTH zones, with a mean value below 1 dB, while it is zero for asset types where fiber attenuation is not applicable. Overall, the normal scenario provides the needed stable reference against which the wildfire scenario can be compared.

In this context, Table 15 summarizes the telemetry values generated under normal conditions, which are grouped by asset type. The values are reported as *mean ± sample standard deviation* over the 120-sample range of the simulation period. This format shows both the average operating behavior and the fluctuation bounds of each asset group before the introduction of wildfire-related disturbance.

Table 15. Normal telemetry summarized statistics by asset type

Variable	All WL (NC), n=16	All FTTH (NC), n=3	All IoT (NC), n=60	EN (NC), n=1
Latency (ms)	34,93 ± 2,81	11,10 ± 1,63	114,58 ± 11,97	14,75 ± 1,54
Packet loss (%)	1,51 ± 0,27	0,51 ± 0,11	2,52 ± 0,39	0,35 ± 0,06
SNR (dB)	25,97 ± 1,05	32,33 ± 0,63	18,53 ± 1,72	32,63 ± 0,68
RSSI (dBm)	-70,54 ± 1,94	-57,55 ± 0,67	-83,44 ± 3,44	-57,65 ± 0,73
Throughput (Mbps)	85,02 ± 9,29	353,86 ± 41,12	0,149 ± 0,026	198,19 ± 26,06
Uptime (%)	98,99 ± 0,27	99,50 ± 0,14	97,97 ± 0,53	99,49 ± 0,11
Battery level (%)	94,96 ± 1,29	100,00 ± 0,00	74,98 ± 5,20	86,88 ± 1,89
Temperature (°C)	33,87 ± 1,55	27,91 ± 1,57	25,01 ± 1,84	35,08 ± 1,47
Relative humidity (% RH)	52,12 ± 4,62	52,56 ± 5,29	57,31 ± 5,93	52,92 ± 4,56
CO_2 concentration (PPM)	424,91 ± 4,02	422,96 ± 3,11	427,30 ± 6,01	425,25 ± 3,58
Alarm count (count/sample)	0,079 ± 0,139	0,028 ± 0,069	0,050 ± 0,104	0,025 ± 0,066
Fault tickets (count/sample)	0,019 ± 0,065	0,019 ± 0,059	0,011 ± 0,046	0,017 ± 0,056
Restoration time (h)	1,22 ± 0,26	2,90 ± 0,48	2,02 ± 0,39	0,67 ± 0,12
Optical loss (dB)	0,00 ± 0,00	0,59 ± 0,10	0,00 ± 0,00	0,00 ± 0,00
All WL (NC) →	All wireless-link assets under normal conditions			
All FTTH (NC) →	All FTTH zone/cabinet assets under normal conditions			
All IoT (NC) →	All IoT sensor assets under normal conditions			
EN (NC) →	Edge node under normal conditions			

Note: Packet loss is stored as a ratio in the simulation and is reported here as a percentage. Alarm count and fault-ticket values may appear as non-integer averages because the table summarizes smoothed values over multiple samples and assets.

Table 16 summarizes the wildfire telemetry generated over the simulation period of 120 samples. The results are grouped according to whether assets are directly injected with wildfire deviations or remain as reference assets. This grouping gives the capability to distinguish environmental stress in affected IoT sensors, communication degradation in affected wireless links, operational impact in the affected FTTH zone, and baseline behavior in unaffected reference assets. Values are reported as *mean ± sample standard deviation* over 120 samples. Packet loss is reported as a percentage.

In more detail, the affected IoT sensors capture the early environmental stress of the wildfire scenario, with increased temperature and CO_2, reduced humidity, and substantially higher alarm activity. The affected wireless links show a different type of impact, such as communication degradation, obvious in increased latency and packet loss, weaker RSSI/SNR, reduced throughput, and lower uptime. The affected FTTH zone mainly reflects operational and

maintenance impact, especially through increased restoration time, alarms, and fault tickets. Instead, the (unaffected) reference assets exhibit behavior closer to baseline values, supporting the fact that the wildfire scenario is localized rather than related to a full area failure (of assets).

Table 16. Wildfire telemetry summarized Statistics by affected and reference asset groups

Variable	IoT-DAW, n=5	WL-DAW, n=3	FTTH-DAW, n=1	REF-UW, n=71
Latency (ms)	116,66 ± 12,26	69,55 ± 45,61	11,56 ± 1,88	96,07 ± 37,01
Packet loss (%)	2,47 ± 0,45	6,36 ± 6,26	0,48 ± 0,10	2,23 ± 0,65
SNR (dB)	18,57 ± 1,65	20,88 ± 6,81	32,45 ± 0,59	20,46 ± 4,16
RSSI (dBm)	-83,77 ± 3,13	-76,89 ± 8,41	-57,34 ± 0,63	-80,11 ± 7,58
Throughput (Mbps)	0,153 ± 0,027	64,86 ± 27,14	347,73 ± 40,14	28,14 ± 67,18
Uptime (%)	97,95 ± 0,49	96,41 ± 3,37	99,55 ± 0,15	98,24 ± 0,67
Battery level (%)	67,73 ± 8,22	94,98 ± 1,34	100,00 ± 0,00	79,51 ± 9,65
Temperature (°C)	39,95 ± 14,11	34,22 ± 1,61	28,00 ± 1,69	26,95 ± 3,97
Relative humidity (% RH)	41,08 ± 15,27	53,40 ± 5,10	52,60 ± 4,34	56,54 ± 6,10
CO_2 concentration (PPM)	586,12 ± 147,93	425,15 ± 4,24	422,57 ± 3,02	426,96 ± 5,76
Alarm count (count/sample)	1,074 ± 1,051	0,626 ± 0,766	0,248 ± 0,374	0,054 ± 0,106
Fault tickets (count/sample)	0,005 ± 0,031	0,163 ± 0,276	0,195 ± 0,283	0,012 ± 0,049
Restoration time (h)	2,00 ± 0,41	1,24 ± 0,26	4,42 ± 1,94	1,88 ± 0,55
Optical loss (dB)	0,00 ± 0,00	0,00 ± 0,00	0,57 ± 0,10	0,017 ± 0,103
IoT-DAW →	IoT sensors directly affected by wildfire injection			
WL-DAW →	Wireless links directly affected by wildfire injection			
FTTH-DAW →	FTTH zone directly affected by wildfire injection			
REF-UW →	Unaffected reference assets under wildfire scenario			

Note: Packet loss is stored as a ratio in the simulation and is reported here as a percentage. Alarm count and fault-ticket values may appear as non-integer averages because the table summarizes smoothed values over multiple samples and assets.

Table 17 presents summary statistics of the decision level. Unlike the telemetry summary tables, which describe the generated sensor and network variables, the certain table summarizes the outputs of the decision support layer: risk score, operational state, and telemetry priority. The values are computed over the complete simulation time (of 120 samples) for each asset group. Therefore, the table shows not only the final state of the system, but also how frequently each group remains in various conditions (such as normal, watch, degraded, critical, low, medium, high, or emergency priority) during the complete simulated period.

In the wildfire scenario, the affected IoT sensors present the most obvious early-warning behavior. Their mean risk increases to 0,380, and they spend almost 63% of the simulated period in the watch state. Nevertheless, they are not found in the degraded or critical state, showing that the environmental disturbance is detected as an elevated risk but does not represent sensor collapse or destruction. As far as the affected wireless links are concerned, they show the strongest operational degradation. Although their mean risk is 0,331, their standard deviation is high, while their maximum risk reaches 0,658. They are found 35% of the simulation time in a degraded state and 35% in high priority, revealing that the wildfire degradation injection has a direct impact on the network resilience. The affected FTTH zone is in the normal state throughout the simulation, despite higher restoration time and ticket indications. This is expected because the risk score is primarily weighted toward communication continuity indicators such as packet loss, latency,

wireless quality, battery, alarms, and temperature. So, FTTH impact (at the operational level) is visible in the telemetry statistics but does not dominate the risk score.

Finally, none of the groups reaches the critical or emergency priority state. This defines the wildfire scenario as a controlled early warning and monitoring case using resilience rather than a situation involving full infrastructure collapse.

Table 17. Summary statistics (decision level) for normal and wildfire scenarios

Scen.	Group	Assets n	Samples n	Risk mean ± SD	Risk min–max	Norm. (%)	Watch (%)	Degr. (%)	Crit. (%)	Low (%)	Med. (%)	High (%)	Emerg. (%)
Norm	WL (NC)	16	120	0,159 ± 0,010	0,120–0,195	100,000	0,000	0,000	0,000	56,250	43,750	0,000	0,000
Norm	FTTH (NC)	3	120	0,056 ± 0,006	0,031–0,073	100,000	0,000	0,000	0,000	0,000	100,000	0,000	0,000
Norm	IoT (NC)	60	120	0,328 ± 0,022	0,237–0,450	84,306	15,694	0,000	0,000	74,097	25,903	0,000	0,000
Norm	EN (NC)	1	120	0,091 ± 0,006	0,076–0,104	100,000	0,000	0,000	0,000	0,000	100,000	0,000	0,000
Wild	IoT-DAW	5	120	0,380 ± 0,051	0,287–0,508	37,500	62,500	0,000	0,000	37,500	62,500	0,000	0,000
Wild	WL-DAW	3	120	0,331 ± 0,209	0,147–0,658	63,333	1,667	35,000	0,000	0,000	65,000	35,000	0,000
Wild	FTTH-DAW	1	120	0,060 ± 0,011	0,042–0,095	100,000	0,000	0,000	0,000	0,000	100,000	0,000	0,000
Wild	REF-UW	71	120	0,286 ± 0,083	0,039–0,425	87,512	12,488	0,000	0,000	69,190	30,810	0,000	0,000

Norm. = Normal ; Degr. = Degraded ; Med. = Medium ; Crit. = Critical ; Emerg. = Emergency

REF-UW = unaffected reference assets under wildfire conditions

EN (NC) = edge node under normal conditions

WL (NC/ DAW) = wireless links under normal conditions / directly affected by wildfire

FTTH (NC/DAW) = FTTH zones under normal conditions / directly affected by wildfire

IoT (NC/DAW) = IoT sensors under normal conditions / directly affected by wildfire

The simulated scenarios (normal and wildfire) can also be examined from a dual-use perspective. In civil-protection mode, the monitored variables reveal infrastructure resilience, wildfire early warning, sensor autonomy, and service continuity. In defense applications, the same variables correspond to edge tactical, where the crucial point is maintaining communications, monitoring infrastructure health, prioritizing telemetry, and supporting local decision-making under degraded conditions. This interpretation is aligned with the Internet of Battle Things concept related to distributed sensing, communication, collaboration, and autonomous decision processes, which are expected to be sustained under rapidly changing mission conditions. In the IoBT literature, there is increased attention on communication flexibility, energy constraints, security, interoperability, and network resilience, which are considered the basic challenges in battlefield IoT environments. Therefore, the simulated raises in packet loss, latency, reduced RSSI/SNR, lower

uptime, alarm activity, and battery stress are expected to be the civil emergency correlation to the tactical-edge degradation. Similarly, the edge-based processing and priority routing support the fact that decision-relevant information should remain available locally when connectivity is constrained. The proposed architecture, therefore, remains defensive and resilience-oriented. It does not consist of model targeting, weapons integration, lethal autonomy, and generally offensive functions but demonstrates how telecommunication infrastructure monitoring can be in service of both civil protection and defense support [8, 45, 51].

With the aforementioned dual-use interpretation in mind, the figures of the next section (which refer to simulated scenarios) are analyzed as visual evidence of the way that telemetry degradation is injected into risk scores, operational states, and priority classes under normal and wildfire conditions.

5.2 Visual results of the simulated scenarios

This subsection presents the six graphical outputs that are generated by the main simulation code. These figures are used to visually understand the way that the generated telemetry is injected into risk scores, operational states, and telemetry priority classes under the conditions of the two scenarios. Therefore, the plots compare the temporal evolution of the highest risk assets, the state classification maps, and the priority assignment maps for both scenarios. Their main purpose is to show how the injected disturbance (wildfire) causes alterations at various points of the workflow while leading to increased watch, degraded, and high-priority behavior without reaching critical state or emergency priority.

The configuration of coordinates, as aforesaid, defines the maximum simulated regional coverage, with latitude ∈ [39,60 , 39,75] and longitude ∈ [20,75 , 20,90], corresponding to an approximate area of 214.60 km². However, the actual generated asset locations occupy a slightly smaller bounding area of 198,67 km². This difference was expected because the assets are randomly generated within the configured coordinate window using a fixed seed for reproducibility, but they are not forced to be placed on the four extreme boundary corners. Consequently, the realized occupied area (for all figures in this subsection) represents the spatial footprint of the generated assets' layout, while the configured area represents the intended (theoretical) simulation window.

As a simple theoretical confirmation check, the realized occupied area contains 80 assets over approximately 198.67 km², corresponding to an average density of about 0,40 assets/km² (80 / 198,67). Under a random spatial point-pattern approximation, the expected mean nearest-neighbor distance can be estimated as $r_E = 1/2\sqrt{\rho}$, where ϱ is the point density. This gives $r_E \simeq 0{,}79$ km, while the observed mean nearest neighbor distance produced by the simulated layout is $r_O \simeq 0{,}83$ km. The ratio $r_O/r_E \simeq 1{,}05$ indicates that the generated distribution is close to the expected spacing of a random layout with the same density, without strong clustering. In addition, all 16 cells of the 4×4 diagnostic grid contain at least one asset, supporting the interpretation that the simulated deployment provides reasonable regional coverage [52].

Figure 5 presents the temporal evolution of the risk score for the five highest risk assets under the normal scenario. The x-axis represents the simulation time samples, from 1 to 120, where each sample corresponds to a five-minute telemetry interval. The y-axis represents the normalized risk score, ranging approximately from 0,26 to 0,42 in this figure. The selected top risk assets are the IoT sensors named as IS-017, IS-036, IS-041, IS-001, and IS-032. Their risk scores fluctuate over time because the simulation continuously generates telemetry variations, such as battery level,

temperature, alarms, packet loss, SNR/RSSI, and other indicators. However, these fluctuations remain at a relatively moderate level. Most values stay around the normal to watch boundary, and none of the curves approach the degraded or critical thresholds. The most important observation from Figure 5 is that, under normal conditions, even the highest risk assets remain within a controlled risk range. The system identifies some IoT sensors of needing observation, but no asset shows sustained degradation or an emergency behavior.

Figures 6a and 6b present the normal scenario's state and priority maps generated at the simulation level. Both figures use the same axes: the x-axis represents the 120 simulation samples, while the y-axis represents the 80 monitored assets. Figure 6a shows the operational state assigned to each asset over time, whereas Figure 6b presents the corresponding telemetry priority class. The two maps, together, illustrate the way that the proposed architecture converts telemetry-derived risk scores into operational states and then into priority levels under normal operating conditions.

Figure 6a shows that the normal scenario remains stable throughout the simulation. Most assets remain in the normal state, while some assets intermittently enter the watch state. No asset enters the degraded or critical state. This confirms that the normal scenario shows a baseline operation with limited telemetry variability. The most important finding from Figure 6a is that normal operation produces only normal and watch states, with no degraded or critical behavior.

Figure 6b presents the telemetry priority assigned to each asset under normal conditions. Only low and medium priority levels are present, while high and emergency priorities are absent. The persistent medium priority horizontal bands are mainly caused by asset criticality rules, where some assets are kept at medium priority because they are operationally important, even when their state is normal. Therefore, the medium priority does not necessarily indicate degradation. Instead, it may also indicate that the asset is so important that it should remain visible to the operator. The most important finding from Figure 6b is that the system sustains visibility for important assets by utilizing the medium priority state, while avoiding unnecessary escalation to high or emergency priority (under normal conditions). Overall, Figures 6a and 6b confirm that the proposed architecture behaves conservatively under normal conditions. It supports the fact that the normal scenario is a stable baseline against which the wildfire scenario can be compared.

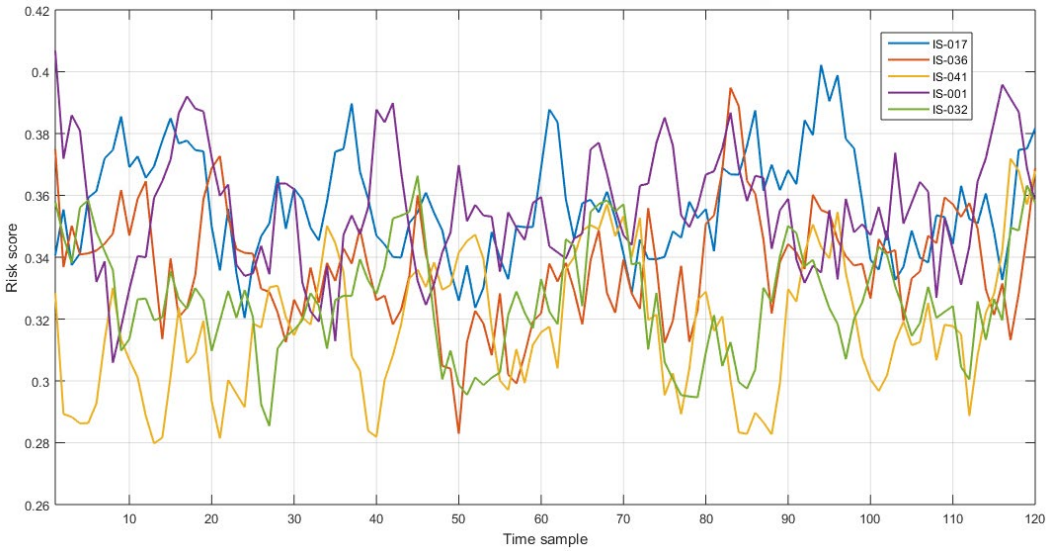
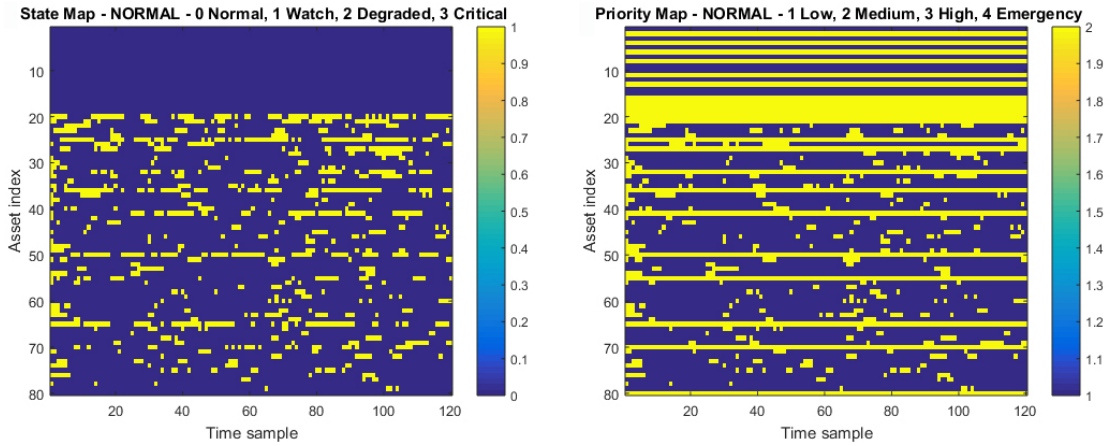


Figure 4. Top-risk assets under normal conditions.



(a) (b)

Figure 6. Maps under normal conditions: (a) the state map shows that assets remain mainly in the normal state, with intermittent watch states, while (b) the priority map shows only low and medium telemetry priority levels. Medium level means asset criticality and monitoring importance, not necessarily degradation.

Figure 7 presents the temporal evolution of the risk score for the five highest risk assets under the wildfire scenario. This figure shows two different degradation patterns where the affected IoT sensors exhibit a gradual risk increase (after the beginning of the environmental disturbance), while affected wireless links show a sharper risk increase when communication degradation is injected later in the simulation. In simple words, the most important finding is that the wildfire scenario generates a clear and controlled escalation of risk. Specifically, the affected wireless links, WL-004, WL-013, and WL-008, show the strongest increase, reaching the degraded range after the communication disturbance. The affected IoT sensors, IS-018 and IS-012, remain mainly in the watch range, reflecting the inserted environmental stress without sensor collapse.

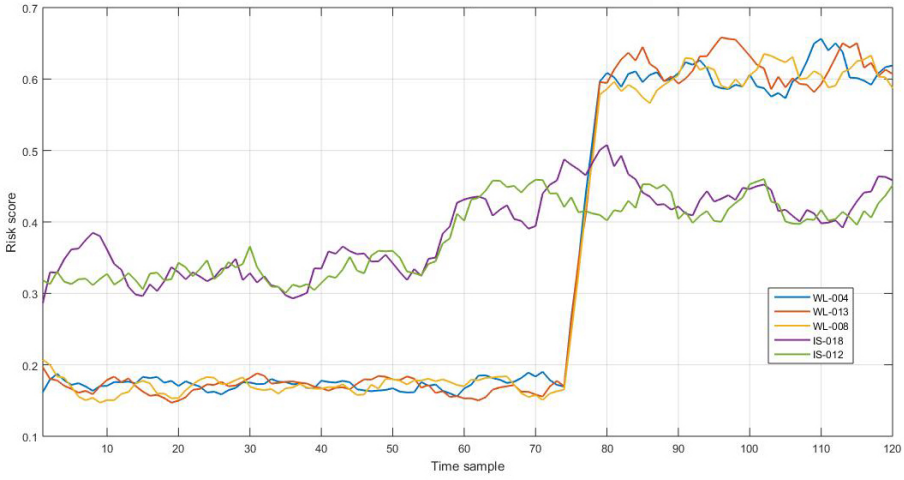
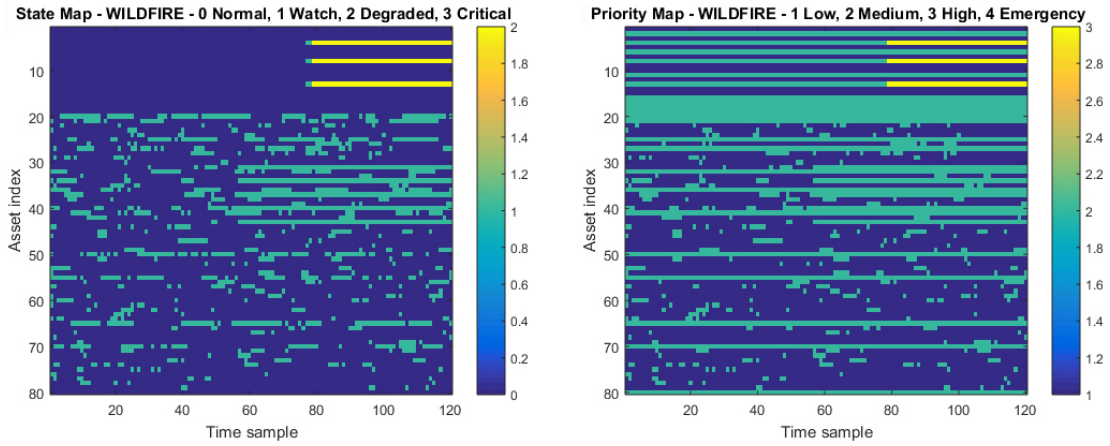


Figure 7. Top-risk assets under wildfire conditions

Figure 8a shows the state classification map for all 80 assets during the wildfire scenario. The x-axis represents 120 simulation samples, while the y-axis represents the monitored asset

index. Compared with the normal scenario, the wildfire case produces a visible increase in watch states and introduces degraded states for selected assets (mainly after the wildfire-related disturbance time period). No critical state appears, confirming that the scenario remains inside a controlled degradation state. In Figure 8b, the priority map (related to telemetry) is assigned to each asset during the wildfire scenario. The map shows clearly that several assets are upgraded from low or medium priority to high priority, especially during the later disturbance period. Nevertheless, no emergency priority is found, since the code rules require both a critical state and high asset criticality. So, the key point in Figure 8b is that it demonstrates the priority routing layer reacting to wildfire injection (which leads to degradation) by elevating selected assets to high priority, while avoiding unnecessary emergency escalation.

Together, Figures 8a and 8b show the way that the wildfire scenario affects the decision layers of the prototype. The system detects increased stress through watch and degraded states and translates this data into higher telemetry priority for selected assets. However, the absence of critical and emergency levels supports the interpretation of the scenario as early-warning and resilient in monitoring rather than leading to a full infrastructure collapse.



(a) (b)

Figure 8. Maps under wildfire conditions: (a) the state map shows increased watch behavior and selected degraded states, but no critical classifications while, (b) the priority map shows increased medium and high telemetry priority under wildfire stress, with no emergency priority activation.

5.3 Spatial results and their interpretation

This subsection presents the supplementary spatial outputs that are generated from the simulation code. The spatial figures do not modify the risk-score calculation, the state classification, or the priority assignment scheme. Instead, they use the generated GIS coordinates of the 80 monitored assets to provide a geographic interpretation of the simulated scenarios. The purpose is to show the way that wireless links, FTTH zones, IoT sensors, and the edge node are distributed inside the simulated area. Also, the spatial analysis provides how the wildfire-affected assets are positioned, and how the final risk or priority behavior appears when projected onto the simulated latitude–longitude field.

Figure 9 shows the simulated spatial distribution of the 80 monitored assets within the configured latitude–longitude window. Different marker types represent various wireless links, FTTH zones, IoT sensors, and the edge node, while circled markers indicate the assets directly

affected by the wildfire injection scheme. The figure contributes to the interpretation of the simulation by proving that the wildfire disturbance is applied to a defined subset of assets rather than to the entire monitored region. It also confirms that unaffected assets remain available as spatial reference points for comparison purposes. So, the contribution is to clarify the spatial form of the simulated deployment and to identify the predefined wildfire-affected assets that are used in the scenario design.

Figures 10a and 10b compare the spatial distribution of the risk score (at the final time step) under normal and wildfire conditions. Figure 10a presents the final risk map for the normal scenario, where risk values are generally moderate and spatially dispersed without a strong localized degradation pattern. However, Figure 10b shows the corresponding wildfire scenario, where higher final risk values appear around the directly affected wireless links and selected IoT sensors. The comparison demonstrates the way that the wildfire disturbance increases risk locally while the rest of the monitored area remains closer to baseline behavior (normal states). Together, Figures 10a and 10b show that the wildfire scenario produces localized risk escalation rather than uniform degradation across the entire simulated area.

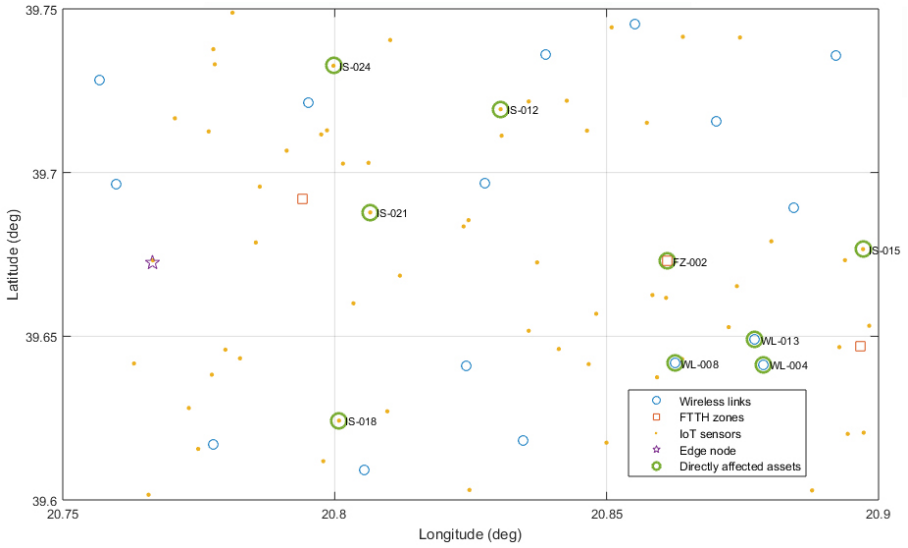
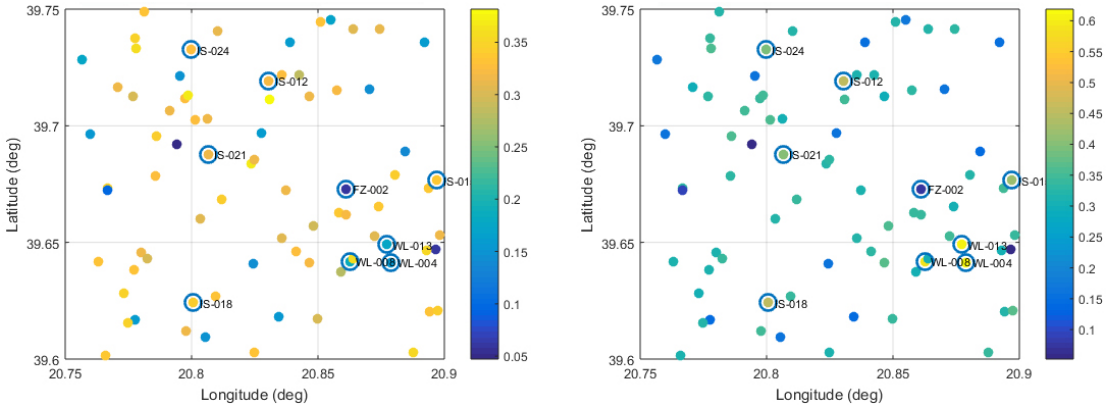


Figure 9. Simulated spatial distribution of monitored assets. Different marker types indicate asset classes, while circled assets identify the predefined assets directly affected by the wildfire scenario.



(a) (b)

Figure 10. Spatial final risk map: (a) under normal conditions and (b) under wildfire conditions.

Figure 11 shows the simulation time percentage for each asset assigned to high or emergency priority under the wildfire scenario. This is not just a final time step snapshot, but instead it is a spatial-frequency representation over the full simulation period (of 120 samples). The figure highlights assets that repeatedly require increased telemetry priority, especially the affected wireless links. The absence of emergency priority behavior confirms that the scenario remains an early warning and resilience monitoring case. Therefore, Figure 11 adds a different aspect to the spatial analysis by showing not only the high-priority behavior occurrence, but also how often it occurs (frequency) during the wildfire scenario. Specifically, the color bar indicates the percentage of the simulation period (120 samples) during which each asset is assigned to either high or emergency priority. The frequency factor is reported as a percentage of the total simulation period, and it is described by equation 12.

$$Frequency_i = \frac{\mathrm{N_i}^{\text{High or Emergency}}}{120} \times 100 \tag{12}$$

where, for each asset i, the frequency of increased priority is computed as the number of simulation samples $N_i^{\,High\ or\ Emergency}$ in which the asset is assigned to high or emergency priority, divided by the total number of simulation samples. Since the simulation contains 120 samples, the result is multiplied by 100 and reported as a percentage.

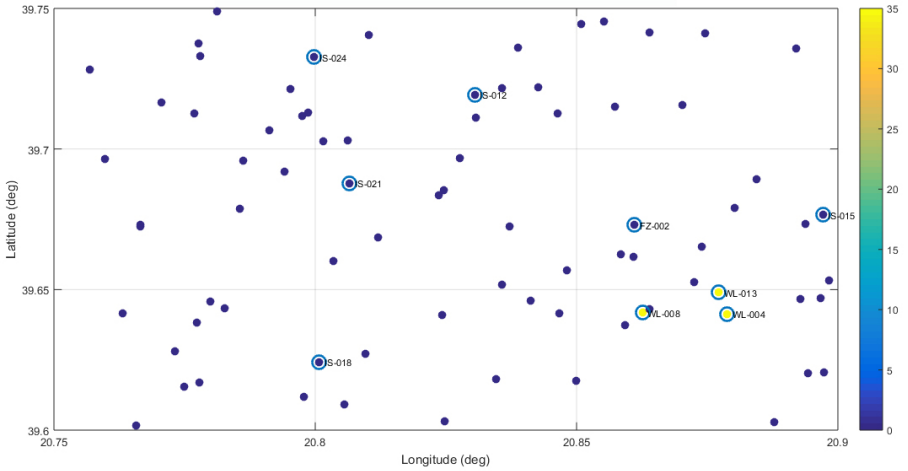


Figure 11. Spatial distribution of increased priority behavior under wildfire conditions. The map shows how often each asset enters high or emergency priority during the wildfire simulation (of 120 samples).

Overall, the spatial analysis acts as a complement to the temporal risk, state, and priority plots by showing where the simulated effects occur. They confirm that the wildfire scenario is localized, controlled, and interpretable. It is obvious that selected assets are in a state of increased risk and priority, while the wider monitored area remains available for reference comparison.

6. Pilot Deployment, Evaluation Plan, and Expected Contribution

The conducted simulation provides a controlled proof of concept (POC). Nevertheless, a real pilot deployment is needed to validate the model under operational conditions. A practical pilot could include a fixed number of wireless links, FTTH zones, IoT sensors, and one edge node, deployed

across a regional semi-rural area with the aim of civil protection. The evaluation should focus on measurable indicators such as latency, packet loss, RSSI/SNR, throughput, uptime, battery level, environmental telemetry, alarms, fault tickets, restoration time, and operator feedback. Therefore, the simulated risk thresholds and priority rules can be compared with real field behavior, allowing the proposed scoring model to be calibrated even better with a full set of extensive measurements, with the goal of progressing while keeping its interpretability intact.

The expected contribution of the work is the demonstration of a telecommunication resilience layer based on IoT that connects infrastructure monitoring, early warning, and priority telemetry in a single operational workflow. From a commercialization perspective, the concept can be positioned as a dual-use resilience service for municipalities, civil-protection authorities, telecommunication operators, critical-infrastructure owners, and defense operating environments. Its value depends on using existing or low-cost infrastructure to improve situational awareness, maintenance prioritization, and continuity of service even under heavy degraded conditions. The current prototype remains intentionally defensive and monitoring-oriented, while future versions could integrate field validation, adaptive thresholds, risk modeling based partially on GIS, and enlarged interoperability with operational dashboards.

7. Restrictions

The proposed architecture is subject to limitations and assumptions. First, the results are based on code-generated telemetry rather than measurements from a real field deployment. The normal and wildfire scenarios are conducted through predefined randomization ranges, Poisson processes, and controlled disturbance injections. Therefore, the reported risk scores, state transitions, and priority assignments should be interpreted as POC simulation outputs rather than validated operational thresholds. Although the randomization ranges and normalization bounds were partially regulated by technical field feedback, engineering experience, and realistic operating assumptions, they should not be interpreted as fully validated operational thresholds. A real pilot deployment would be required to calibrate the normalization bounds, risk weights, state thresholds, and priority rules against measured incidents, operator feedback, maintenance records, and environmental observations.

The current implementation is intentionally interpretable and linear. It uses transparent weighted scoring rather than trained machine learning models, predictive anomaly detection, or GIS-driven propagation modeling. Spatial coordinates are used for visualization and interpretation, but they do not directly influence the risk score. In a similar manner, the wildfire scenario represents localized early-warning degradation and does not model fire spread, wind direction, terrain effects, radio-propagation physics, or very heavy infrastructure failures. The system is also restricted to defensive monitoring, resilience support, and priority telemetry. It does not include targeting functions, weapons integration, offensive cyber capabilities, and lethal autonomous decision-making.

The proposed simulated framework does not include an optimized sensor-placement methodology, nor does it validate the physical accuracy of specific sensing devices. The formulation of sensor locations, telemetry ranges, and affected assets is a specific design assumption for simulation purposes. In a real deployment, the sensor placement, calibration, measurement reliability, communication coverage, and operational thresholds would probably need to be validated through field measurements and operator feedback.

8. Conclusions and future scopes

This work presented the TeleReNT (Telecommunications Resilience Network) prototype as an interpretable telecommunication resilience framework for monitoring distributed infrastructure under normal and wildfire conditions. The proposed workflow connects code-generated telemetry, edge-level smoothing, digital-twin asset representation, normalized risk scoring, state classification, and telemetry priority assignment into a single controllable simulation pipeline.

The simulation results show that the normal scenario remains stable, with assets mainly classified as normal or watch and without exhibiting any of these behaviors: Degraded, critical, high-priority, or emergency. Under wildfire conditions, the system produces a controlled degradation pattern. Affected IoT sensors exhibit environmental stress, affected wireless links present communication degradation, and selected assets are elevated to a degraded state and high priority. However, no asset reaches a critical state or emergency priority. This supports the interpretation of the scenario as an early warning and resilience-monitoring case rather than a scenario with asset-collapsing characteristics.

The supplementary spatial analysis further demonstrates that the generated asset distribution provides a plausible monitoring layout. The configured simulation window covers approximately 214.6 km², while the realized generated asset footprint covers approximately 198.67 km². The spatial risk and priority maps also show that the wildfire impact remains localized and interpretable.

Overall, the contribution of this work is the demonstration of a defensive, resilience-oriented digital-twin approach that can transform heterogeneous telecommunications, IoT, environmental, and maintenance indicators into operational states and telemetry priorities. The proposed model's value lies in showing how existing or low-cost infrastructure can be organized into an interpretable early warning and priority routing mechanism.

Future work should focus on field validation through a real pilot deployment, using measured telemetry, maintenance records, operator feedback, and environmental observations to calibrate the normalization bounds, risk weights, state thresholds, and priority rules. Additional extensions may include GIS-aware risk modeling, adaptive thresholds, anomaly detection, real operational dashboard integration, and multi-site validation. A further communication-layer extension could investigate reconfigurable OFDM/DSP platforms (even included in unmanned vehicles) as software updatable modules for supporting adaptive connectivity under degraded conditions, while keeping the system strictly focused on resilience, monitoring, and continuity of service [53, 54].

In summary, the main outcome of this work is not a universal sensor-placement solution, but a reusable and interpretable Digital Twin protocol that can be specialized for different operational environments. Its practical use depends on future field deployment, calibration, and validation, where the generic workflow can be adapted to the sensing requirements, various infrastructure constraints, and decision rules of specialized civil-protection or defense-support scenarios.

References

1. "Y.3090 : Digital twin network - Requirements and architecture," *Itu.int*. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3090-202202-I [Accessed: 26-Apr-2026].

2. R. Poorzare, D. N. Kanellopoulos, V. K. Sharma, P. Dalapati, and O. P. Waldhorst, "Network digital twin toward networking, telecommunications, and traffic engineering: A survey," *IEEE Access*, vol. 13, pp. 16489–16538, 2025. DOI: 10.1109/ACCESS.2025.3531947
3. L. Ismail, A. Abdelmoti, A. Basu, A. D. E. Berini, and M. Naouss, "A systematic review of digital twin-driven predictive maintenance in industrial engineering: Taxonomy, architectural elements, and future research directions," *arXiv [cs.AI]*, 2025. DOI: 10.48550/arXiv.2509.24443
4. "Deployment & Operations committee," *Ftthcouncil.eu*. [Online]. Available: https://www.ftthcouncil.eu/about-us/committees/deployment-operations-committee. [Accessed: 27-May-2026].
5. A. Hassebo and M. Tealab, "Global models of smart cities and potential IoT applications: A review," *IoT*, vol. 4, no. 3, pp. 366–411, 2023. DOI: 10.3390/iot4030017
6. M. Golfarelli, S. Rizzi, and A. Proli, "Designing what-if analysis: Towards a methodology," in *Proceedings of the 9th ACM international workshop on Data warehousing and OLAP*, 2006.
7. C. Zhou *et al.*, "Network Digital Twin: Concepts and reference architecture," *IETF Datatracker*. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/10/ [Accessed: 26-Apr-2026].
8. N. Gallagher and M. M. Armstrong, "What is a digital twin?," *Ibm.com*, 03-Feb-2026.
9. B. Huff, K. Uregdthsa, K. Muhammad, and C. Searcy, "Network digital twins: Framework, applications, and challenges," *Techrxiv*, 2024.
10. Y. Sanjalawe, S. Fraihat, S. Al-E'mari, and S. N. Makhadmeh, "Bridging the gap: A comprehensive survey on AI-driven digital twin networks for future wireless systems," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 38, no. 3, 2026. DOI: 10.1007/s44443-026-00522-y
11. J. Wieme, M. Baert, and J. Hoebeke, "Architectural design for Digital Twin Networks," *Network*, vol. 5, no. 3, p. 24, 2025. DOI: 10.3390/network5030024
12. N. R. Burramukku, "AI-Enabled Closed-Loop Network Automation Using Digital Twin-Driven Validation Models," *Journal of Emerging Trends and Novel Research*, vol. 1, no. 11, pp. a28–a39.
13. "NMRG RG - network management research group," *IETF Community Wiki*. [Online]. Available: https://wiki.ietf.org/group/nmrg. [Accessed: 26-Apr-2026].
14. P. Almasan *et al.*, "Network digital twin: Context, enabling technologies, and opportunities," *IEEE Commun. Mag.*, vol. 60, no. 11, pp. 22–27, 2022. DOI: 10.1109/MCOM.001.2200012
15. M. Lis and M. Mądziel, "Green transportation planning for Smart Cities: Digital Twins and real-time traffic optimization in urban mobility networks," *Appl. Sci. (Basel)*, vol. 16, no. 2, p. 678, 2026. DOI: 10.3390/app16020678
16. R. F. El-Agamy, H. A. Sayed, A. M. AL Akhatatneh, M. Aljohani, and M. Elhosseini, "Comprehensive analysis of digital twins in smart cities: a 4200-paper bibliometric study," *Artif. Intell. Rev.*, vol. 57, no. 6, 2024. DOI: 10.1007/s10462-024-10781-8
17. V. Cheimaras *et al.*, "Emergency communication system based on wireless LPWAN and SD-WAN technologies: A hybrid approach," *Signals*, vol. 4, no. 2, pp. 315–336, 2023. DOI: 10.3390/signals4020017
18. "Resilient edge systems for critical infrastructure and urban environments," *CORDIS | European Commission*, 19-Jan-2026. [Online]. Available: https://cordis.europa.eu/project/id/101225910. [Accessed: 26-Apr-2026]. DOI: 10.3030/101225910
19. Hybrid Connectivity, "The future is," *Livewire.co.uk*. [Online]. Available: https://www.livewire.co.uk/wp-content/uploads/2023/12/The-future-is-Hybrid-Connectivity.pdf. [Accessed: 26-Apr-2026].
20. R. A. Abdulrazzq, N. M. Sajid, and M. S. Hasan, "Artificial intelligence-driven predictive maintenance in IoT systems," *S. F. J. of Dev.*, vol. 5, no. 12, p. e4781, 2024. DOI: 10.46932/sfjdv5n12-030
21. S. Sethi, "Predictive Maintenance in IoT Environments Using Machine Learning: Opportunities, Challenges, and Innovations," *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*, vol. 11, no. 4.

22. S. Chen, E. Turanoglu Bekar, J. Bokrantz, and A. Skoogh, "AI-enhanced digital twins in maintenance: Systematic review, industrial challenges, and bridging research–practice gaps," *J. Manuf. Syst.*, vol. 82, pp. 678–699, 2025. DOI: 10.1016/j.jmsy.2025.07.006
23. T. Bitam, A. Yahiaoui, D. E. Boubiche, R. Martínez-Peláez, H. Toral-Cruz, and P. Velarde-Alvarado, "Artificial Intelligence of Things for next-generation predictive maintenance," *Sensors (Basel)*, vol. 25, no. 24, p. 7636, 2025. DOI: 10.3390/s25247636
24. S. Subashree, M. Rajakumaran, G. Pushpa, and R. Manivannan, "Adaptive machine learning models for predictive maintenance in industrial internet of things (IIoT) systems," *Sci. Rep.*, vol. 16, no. 1, 2026.
25. R. Damaševičius, N. Bacanin, and S. Misra, "From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management," *J. Sens. Actuator Netw.*, vol. 12, no. 3, p. 41, 2023. DOI: 10.3390/jsan12030041
26. W. Leong, "Internet of things for enhancing public safety, disaster response, and emergency management," in *2024 IEEE 6th Eurasia Conference on IoT, Communication and Engineering*, 2025, p. 61. DOI: 10.3390/engproc2025092061
27. "How IoT is revolutionizing disaster prevention and response," *IoT For All*. [Online]. Available: https://www.iotforall.com/how-iot-is-revolutionizing-disaster-prevention-and-response. [Accessed: 26-Apr-2026].
28. V. Bonilla, B. Campoverde, and S. G. Yoo, "A systematic literature review of LoRaWAN: Sensors and applications," *Sensors (Basel)*, vol. 23, no. 20, p. 8440, 2023. DOI: 10.3390/s23208440
29. T. Brito *et al.*, "Data acquisition filtering focused on optimizing transmission in a LoRaWAN network applied to the WSN forest monitoring system," *Sensors (Basel)*, vol. 23, no. 3, p. 1282, 2023. DOI: 10.3390/s23031282
30. C. C. Chan, S. A. Alvi, X. Zhou, S. Durrani, N. Wilson, and M. Yebra, "A survey on IoT ground sensing systems for early wildfire detection: Technologies, challenges and opportunities," *IEEE Access*, pp. 1–1, 2024. DOI: 10.1109/ACCESS.2024.3501336
31. R. Vega-Rodriguez, S. Sendra, J. Lloret, P. Romero-Diaz, and J. L. Garcia-Navas, "Low cost LoRa based network for forest fire detection," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019. DOI: 10.1109/IOTSMS48152.2019.8939193
32. N. C. Gaitan and P. Hojbota, "Forest Fire Detection System using LoRa Technology," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, 2020.
33. A. De Rango, L. Furnari, F. Cortale, A. Senatore, and G. Mendicino, "Wildfire early warning system based on a smart CO2 sensors network," *Sensors (Basel)*, vol. 25, no. 7, p. 2012, 2025. DOI: 10.3390/s25072012
34. H. Safi, A. I. Jehangiri, Z. Ahmad, M. A. Ala'anzy, O. I. Alramli, and A. Algarni, "Design and evaluation of a low-power wide-area network (LPWAN)-based emergency response system for individuals with special needs in smart buildings," *Sensors (Basel)*, vol. 24, no. 11, p. 3433, 2024. DOI: 10.3390/s24113433
35. I. Zacarias, L. P. Gaspary, A. Kohl, R. Q. A. Fernandes, J. M. Stocchero, and E. P. de Freitas, "Combining software-defined and delay-tolerant approaches in last-mile tactical edge networking," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 22–29, 2017. DOI: 10.1109/MCOM.2017.1700239
36. "What is Defense in Depth? Defined and Explained," *Fortinet*. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/defense-in-depth. [Accessed: 30-Apr-2026].
37. D. S. Gaito, D. V. N. G. Soares, and V. Karyotis, "Special Issue: Delay-Tolerant Networking," *Future Internet (Mdpi.com)*. [Online]. Available: https://www.mdpi.com/journal/futureinternet/special_issues/delay-tolerant_networking. [Accessed: 30-Apr-2026].
38. "Internet of battlefield things (IoBT) REIGN," Illinois.edu. [Online]. Available: https://iobt.illinois.edu/. [Accessed: 30-Apr-2026].
39. J. E. C. Gomes et al., "Surveying emerging network approaches for military Command and Control systems," ACM Comput. Surv., vol. 56, no. 6, pp. 1–38, 2024. DOI: 10.1145/3626090

40. K. Poularakis, G. Iosifidis, and L. Tassiulas, "SDN-enabled tactical ad hoc networks: Extending programmable control to the edge," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 132–138, 2018. DOI: 10.1109/MCOM.2018.1700387
41. V. Gkioulos, H. Gunleifsen, and G. Weldehawaryat, "A systematic literature review on military software defined networks," *Future Internet*, vol. 10, no. 9, p. 88, 2018. DOI: 3390/fi10090088
42. S. Rokka Chhetri and M. A. Al Faruque, "IoT-enabled living digital twin modeling," in *Data-Driven Modeling of Cyber-Physical Systems using Side-Channel Analysis*, Cham: Springer International Publishing, 2020, pp. 155–182. DOI: 10.1007/978-3-030-37962-9_8
43. C. Stryker, "Human In The Loop," *Ibm.com*, 17-Nov-2025. [Online]. Available: https://www.ibm.com/think/topics/human-in-the-loop. [Accessed: 02-May-2026].
44. R. Kufakunesu, H. Myburgh, and A. De Freitas, "The internet of battle things: a survey on communication challenges and recent solutions," *Discov. Internet Things*, vol. 5, no. 1, 2025. DOI: 10.1007/s43926-025-00093-w
45. P. Fraga-Lamas and T. M. Fernandez-Carames, "Tactical Edge IoT in Defense and National Security," *arXiv [cs.CR]*, 2024. DOI: 10.48550/arXiv.2411.00511
46. "What is the approximate average distance, in kilometers, between two consecutive lines of latitude (separated by 1∘ of arc) on Earth?," *Prepp.in*. [Online]. Available: https://prepp.in/question/the-distance-between-two-latitudes-is-approximatel-64371fe9c5c73c24c6c94f70. [Accessed: 02-May-2026].
47. *Britannica.com*. [Online]. Available: https://www.britannica.com/science/latitude. [Accessed: 02-May-2026].
48. M. Kompf, "Distance calculation," *Martin Kompf*, 06-Jan-2023. [Online]. Available: https://en.kompf.de/gps/distcalc.html. [Accessed: 02-May-2026].
49. S. G. K. Patro and K. K. Sahu, "Normalization: A Preprocessing Stage," *Int. Adv. Res. J. Sci. Eng. Technol.*, pp. 20–22, 2015. DOI: 10.17148/iarjset.2015.2305
50. "Y.1540 : Internet protocol data communication service - IP packet transfer and availability performance parameters," *Itu.int*. [Online]. Available: https://www.itu.int/rec/T-REC-Y.1540/en. [Accessed: 02-May-2026].
51. A. Kott, A. Swami, and B. J. West, "The internet of battle things," *Computer (Long Beach Calif.)*, vol. 49, no. 12, pp. 70–75, 2016. DOI: 10.1109/MC.2016.355
52. P. J. Clark and F. C. Evans, "Distance to nearest neighbor as a measure of spatial relationships in populations," *Ecology*, vol. 35, no. 4, pp. 445–453, 1954.
53. M. Zamkotsian *et al.*, "Wireless SPIHT-encoded image transmission employing hierarchical modulation: A DSP implementation," in *IEEE International Symposium on Signal Processing and Information Technology*, 2013. DOI: 10.1109/ISSPIT.2013.6781929
54. S. K. Chronopoulos, "Flexible and reconfigurable OFDM implementation in DSP platform for various purposes and applications," *Sensors (Basel)*, vol. 24, no. 9, p. 2732, 2024. DOI: 10.3390/s24092732

Appendix A

Appendix A.1: Calculating an area size for specific degree spreads

In the case of Table 8 where latitude equals to 39,60 + 0,15U and taken into consideration that U ~ Uniform(0,1) then we could calculate the mean latitude and furthermore proceed on finding the estimated area for a specific case (≃ 214,7 km²) in Table 9. Please see below the method of calculation procedure (A1.1 to A1.6).

First we define the latitude from equation (A1.1). Then, taking into account that [U]=0,5, the later corresponds to the expected value of U without being a unit of measurement. U is a random number without units: U~Uniform(0,1). So, it can acquire values from 0 to 1 with equal probability. For this reason, the average is: E[U] = (0+1) / 2 = 0,5. Consequently, the latitude from previous equation can take values from 39,60 to 39,75 (= 39,60+0,15). Its mean value is the middle of the interval: E[latitude] = ϕ = 39,60 + (0,15 × 0,5) = 39,675.

A natural question would be weather we make all these calculations for finding the area. At this point, the aim is to find mean latitude, because longitude span depends on latitude via cos(latitude). The code doesn't distribute the assets within a circular area. Instead, it distributes them within a rectangular (latitude–longitude) window with the following restrictions:

$$\text{Latitude} = 39{,}60 + 0{,}15U \tag{A1.1}$$

$$\text{Latitude} \in [39{,}60\ ,\ 39{,}75] \tag{A1.2}$$

$$\text{Longitude} \in [20{,}75\ ,\ 20{,}90] \tag{A1.3}$$

The approximate area is calculated from degree spread (d=0.15°) and the mean latitude (39,675°):

$$\text{Latitude span} \simeq 111{,}32 \times d \rightarrow \text{Latitude span} \simeq 111{,}32 \times 0{,}15\ \text{km} = 16.698\ \text{km} \tag{A1.4}$$

$$\begin{gathered}\text{Longitude span} \simeq 111{,}32 \times \cos(\phi) \times d\ \rightarrow \\ \text{Longitude span} \simeq 111{,}32 \times \cos(39{,}675\circ) \times 0{,}15\ \text{km} \rightarrow \\ \text{Longitude span} \simeq 111{,}32 \times 0{,}770 \times 0{,}15\ \text{km}\ \rightarrow \text{Longitude span} \simeq 12{,}86\ \text{km}\end{gathered} \tag{A1.5}$$

$$\begin{gathered}\text{Area} = \text{Longitude span} \times \text{Latitude span}\ \rightarrow \text{Area} = 12{,}86\ \text{km} \times 16{,}698\ \text{km} \rightarrow \\ \text{Area} \simeq 214{,}7\ \text{km}^2\end{gathered} \tag{A1.6}$$

Appendix B

Appendix B.1: Definition of introduced normalized risk indicators

The included normalization bounds (used to convert different units of measurement to a common 0–1 scale) are based on engineering reference field limits for simulation and quality calculation purposes. Regarding each variable (Table B1.1), the lower bound corresponds to a low risk or nominal condition, while the upper bound corresponds to a severe degradation condition. Variables like packet loss and alarm count have a zero value as the lower risk reference, because zero packet loss or zero alarms indicate no observed degradation for the corresponding metric. These bounds are not universal thresholds. They are selected for providing an interpretable normalization scale for the prototype.

Table B1.1. Geographic distribution

Risk indicator	Formula	Why these bounds are used
LatencyRisk	$\frac{latency - 5}{220 - 5}$	5 ms refers to the low bound reference latency, while 220 ms is used as a high-delay bound. Zero latency is unusable because it is unrealistic under real communication conditions.
LossRisk	$\frac{packet\ loss - 0}{0{,}18 - 0}$	0 means no packet loss. 0,18 means 18% packet loss, treated as a very severe degradation in the simulation.
BatteryRisk	$\frac{100 - battery}{100 - 10}$	100% battery means no battery risk, while 10% is treated as a critical low-battery reference.
TemperatureRisk	$\frac{temperature - 15}{70 - 15}$	The value of 15 °C is used as a low environmental reference. 70 °C is used as a severe high-temperature stress (reference).
AlarmRisk	$\frac{alarm\ count - 0}{5 - 0}$	0 alarms means no alarm activity. 5 alarms per sample is considered as a high alarm-load (reference).
SNRRisk	$\frac{35 - SNR_{dB}}{35 - 5}$	The 35 dB is considered as excellent signal quality, while 5 dB refers to poor signal quality.
RSSIRisk	$\frac{-55 - RSSI_{dBm}}{-55 - (-105)}$	Inverse normalization. -55 dBm is strong received signal, while -105 dBm is weak received signal.