ROBUST communication platform – A decentralized, distributed communication platform for the earthquake early warning system ROBUST

Michael Jendreck
Fraunhofer FOKUS
michael.jendreck@fokus.fraunhofer.de

Janine Hellriegel
Fraunhofer FOKUS
janine.hellriegel@fokus.fraunhofer.de

Jonas Allmann
Fraunhofer FOKUS
jonas.allmann@fokus.fraunhofer.de

Hannes Restel
Fraunhofer FOKUS
hannes.restel@fokus.fraunhofer.de

Stefan Pfennigschmidt
Fraunhofer FOKUS
stefan.pfennigschmidt@fokus.fraunhofer.de

Ulrich Meissen
Fraunhofer FOKUS
ulrich.meissen@fokus.fraunhofer.de

Frank Fuchs-Kittowski
Fraunhofer FOKUS
frank.fuchs-kittowski@fokus.fraunhofer.de

ABSTRACT

Strong earthquakes of great intensity pose a severe threat to human life and property. Earthquake early warning systems are designed to give people in endangered areas valuable seconds to save their lives and property. The basis of an efficient warning system is a communication infrastructure that provides high-speed and reliable communication between the components of the warning system. This paper presents the distributed, decentralized communication platform for the ROBUST project. It discusses the key challenges and requirements such as resilience, real-time capability and target group-specific information distribution that are placed on such a communication platform. In addition, it presents the conception of the communication platform, which is based on a subscriber procedure between autonomous, decentralized peers (nodes), in order to be able to realize the requirements. Finally, it details the technical implementation, practical realization, and evaluation of the communication platform.

Keywords

Earthquake, early warning system, communication platform.

INTRODUCTION

Earthquakes have by far been the deadliest natural disasters in recent years (UNDRR, 2020). In Germany and Europe, the magnitude and frequency of earthquakes do not reach the dimensions experienced in other parts of the world. Nevertheless, the (moderate to strong) seismic events (magnitude >= 6 in some regions) occurring in Germany and Europe can cause great damage, especially to buildings and critical infrastructures, due to the high population density and the concentration of values (Clinton et al., 2016). Earthquake monitoring and early warning systems are being developed and deployed to provide early response to earthquakes and reduce potential damage to people and infrastructures (Allen and Melgar, 2019). Earthquake early warning systems are capable of detecting earthquakes at an early stage, sending out reliable warnings in a timely manner, and initiating an appropriate emergency response (Allen et al., 2009). The ROBUST project is currently developing a novel earthquake early warning and response system based on the combination of interconnected, decentralized earthquake sensors and local monitoring systems of structures connected to digital building information models (BIM). The system is tailored to the special conditions in Germany, like short warning times and high population density. It enables earthquake detection, rapid damage prognosis, target group-specific real-time information transmission, triggering of automatic shutdown procedures and other immediate measures (CWE, 2023).

An important content-related focus and a central challenge of the ROBUST project is the development of a distributed, decentralized communication platform, via which the interaction of the individual distributed components of the ROBUST system is to be enabled. Earthquakes are to be registered at an early stage employing a network of distributed sensors. Seismic data from the connected sensors, intensity forecasts, and damage diagnoses relating to the earthquake are to be distributed and reported to operators of critical infrastructures (such as industrial plants or public buildings) in a targeted, decentralized manner via the communication platform. Specific messages can be used to trigger the detection of damage to structures and/or industrial plants as early as possible. A particular challenge here results from the short warning and associated short response times. In addition to this real-time capability, performance, reliability, and target group-specific information distribution are further challenges.

This paper presents a distributed, decentralized communication platform, proposed within the ROBUST project to overcome the aforementioned challenges. In a first step the requirements for such a communication infrastructure are discussed, which were collected and analyzed in several workshops with stakeholders and potential users of the communication infrastructure. The conception of the communication infrastructure is presented next. It is based on a subscriber procedure between autonomous, decentralized peers (called nodes), designed to address central challenges and requirements such as failure safety, real-time capability and target group-specific information distribution. Finally, the paper details the technical implementation, practical realization, and evaluation of the communication infrastructure.

This paper is structured as follows: First, the background and related work on the ROBUST communication platform form is presented. The intended functionality of the earthquake early warning and response system to be developed in the ROBUST project is outlined in the form of a reference scenario. Starting from an earthquake event, a typical action sequence (scenario) of the system and thus its supporting effect is described, and related work on the ROBUST system and the ROBUST communication platform is discussed. Based on this, the goals and the basic solution approach of the ROBUST communication platform are described. The next section identifies and describes the functional requirements of such a communication platform, followed by the concept of the ROBUST communication platform targeting these requirements. After that, the technical realization of the platform is presented in the form of a prototypical implementation. The following section presents the results of the evaluation of the concept and its technical realization in the context of a laboratory test using a permanently operated test setup to prove the feasibility and functionality of the communication infrastructure. The paper ends with a summary and an outlook.

BACKGROUND AND RELATED WORK ON THE ROBUST COMMUNICATION PLATFORM

The communication platform presented in this paper is part of an integrated earthquake warning and response system based on digital building models and advanced sensor technologies, which is currently being developed in the ROBUST research project. The background to developing the ROBUST integrated earthquake warning and response system is presented below, followed by related work on the designed communication platform.

The integrated earthquake warning and response system ROBUST

Within the ROBUST project, a user-oriented earthquake early warning and response system is to be developed based on the combination of interconnected decentralized sensor systems for earthquake early warning and local monitoring systems of structures connected to digital building information models (BIM) (cf. Figure 1). The system enables earthquake detection, triggering of fast automatic shutdown procedures and other immediate measures, rapid damage prognosis and target group-specific real-time information transmission based on a distributed, decentralized communication infrastructure.

Figure 1 shows how the various components interact and communicate with each other. The communication platform is responsible for the communication between the individual components, which are shown in Figure 1. Communication paths are represented by arrows.

The following section describes a typical scenario (reference scenario) in which the ROBUST system can play a supporting role in the event of an earthquake. This scenario illustrates the operation of the ROBUST system and forms the basis for defining objectives and evaluating solution approaches for the communication platform.

The starting event of such a scenario is an earthquake. This earthquake is first detected by the nearby seismic sensors (Najdahmadi et al., 2023) and reported to the communication platform. The first messages emitted by the sensors do not represent a confirmed earthquake, but only seismic events that may indicate one.

Participants of the ROBUST communication platform who have subscribed to this type of (event) message receive the messages immediately, ideally even before the actual quake has reached them. Typical recipients are monitoring systems of critical infrastructures, like industrial plants or road bridges. These initial event messages can be used, for example, to activate such monitoring systems and/or to increase the sampling rates of the sensors of these systems.

Messages from the seismic sensors are also forwarded to a cloud service, which determines the occurrence of an actual earthquake and its approximate intensity based on the included data. If the occurrence of an earthquake is confirmed, this cloud service reports it to the communication platform, which distributes this information according to participants' subscriptions.

Based on the earthquake confirmation message, the monitoring systems can calculate damage forecasts for the respective infrastructures and distribute these in turn via the communication platform, ideally even before the earthquake has reached the infrastructures.

In the course of an earthquake, all messages can be constantly updated. With regard to the infrastructures, the measurement results of the sensors (monitoring systems) can lead to the adjustment of damage forecasts and the creation of structural damage diagnoses.

Damage forecasts and diagnostic messages are processed by further participants of the system. Among others, these are warning and information systems responsible for alerting affected groups of people. A typical example is a warning to employees of an industrial plant asking them to get to safety or to inform safety personnel in control centers about possible damage.

Participants of the ROBUST communication platform can control technical systems based on the forecast and diagnostic messages. This includes control systems such as traffic lights, dynamic escape route marking, sirens, and loudspeaker announcements. Direct interventions in the actual production processes are also conceivable.

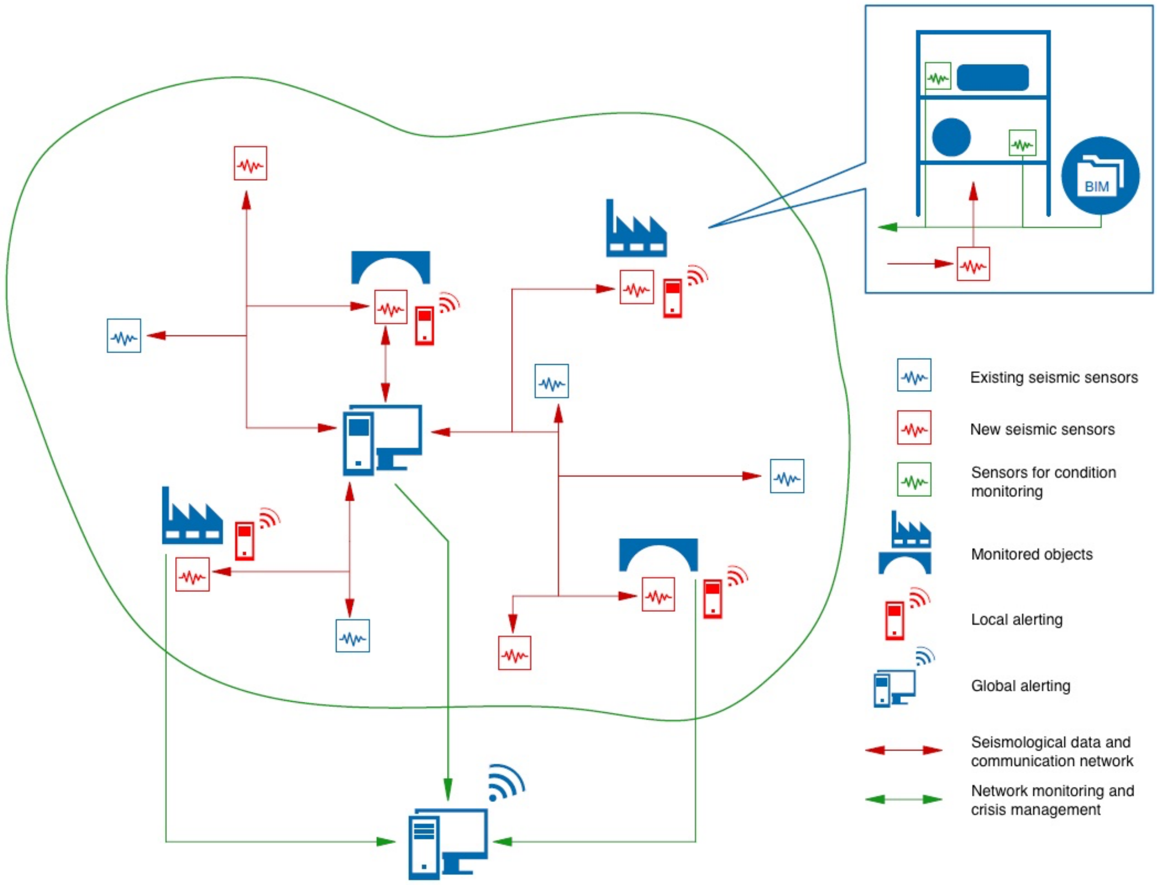

BIM
Existing seismic sensors
New seismic sensors
Sensors for condition monitoring
Monitored objects
Local alerting
Global alerting
Seismological data and communication network
Network monitoring and crisis management

Figure 1. Overview of the ROBUST system (CWE, 2023)

Related work to the ROBUST system

Earthquake early warning systems capable of detecting strong earthquakes at an early stage, sending reliable warnings in a timely manner, and initiating appropriate emergency response measures have been successfully deployed in Japan and Mexico (Allen & Melgar, 2019; Allen et al. 2009), and in the United States for the West Coast (ShakeAlert, 2023) and California (CEEWP, 2023). In addition, early warning systems can provide information for forecasting potential damage to critical structures in real time (Megalooikonomou et al., 2018; Pittore et al., 2014). Complementing earthquake early warning systems, powerful methods and sensors are now available for structural health monitoring (SHM) to record the condition of structures (Ostachowicz and Güemes, 2013).

The analysis of existing literature (topics: Earthquake early warning systems, structure monitoring and sensor technology coupled with digital building models) revealed, however, that a cross-disciplinary earthquake early warning and response system - such as the ROBUST system - based on the technical capabilities of decentralized networks of seismic stations, intelligent sensor technology for recording the condition of structures and processes with evaluation by digital building models (BIM) has not yet been developed. In addition, the ROBUST system is being developed specifically for the seismological processes prevailing in Europe and Germany with short warning times and with seismic fault zones close to densely populated areas.

Related work to the ROBUST communication platform

There are numerous studies on the characterization and design of network and communication frameworks for disaster management (for a review, see (Yan, 2011; Khaled and Mcheick, 2019)). Different technologies are used and system architectures are developed depending on the use case.

For real-time information transmission and alerting, a decentralized sensor network is used in ROBUST instead of a classical information infrastructure with a central network node for data evaluation and generation of warnings and alerts (SARMEX, 2019; Suárez, 2022). The triggering of warnings and alerts in such a dedicated network is based on the continuous exchange of information between the participating sensors in real time, with calculations and evaluations performed locally on the individual sensors. The real-time communication and robustness required for this during the information exchange requires the use of the latest communication protocols and technologies.

In terms of communication protocols, the main candidates are ISO/OSI concepts and protocols from the field of the "Internet of Things", which are intended for wireless "ad-hoc" sensor networks, e.g. WiFi according to IEEE 802.11 (IEEE, 2023), 5G mobile architectures for dedicated network layers with secured resources (Zhang, 2017), and low-power wide area networks (LoPWAN) for secure data transmission in distributed sensor networks (Gündogan et al., 2019).

For a simple extension of the decentralized sensor network architecture, the real-time sensors must be integrated into the existing infrastructure by means of a simple configuration. For this purpose, many concepts and solutions are available today which fulfill this requirement when combined accordingly. For the communication between individual components IP-based "mesh networks" can be used, which represent a flat hierarchy of network participants. So-called "Named Data Networking" (NDN) offers solutions for the interconnection of sensor nodes, which originate from the field of information-centric networks (NDN, 2010; Shang et al., 2016; Nolan et al., 2016). NDN networks eliminate the need for IP configuration when integrating new nodes, as all nodes in the network can communicate with each other using names, regardless of IP address (Shang et al., 2018). To ensure real-time capability and timeliness of larger data streams, responsive "publish/subscribe" transmission concepts are used (Shang et al., 2018). Technologies that have proven themselves in this topic area include the Message Queue Telemetry Transport MQTT (MQTT, 2023) and Redis Streams (Redis Streams, 2023). Here, through topic subscriptions, messages and updated information are transmitted to selected participants (nodes).

GOALS AND SOLUTION APPROACH OF THE COMMUNICATION PLATFORM

In the previous section, the functionality of the planned, user-oriented earthquake early warning and response system ROBUST with intelligent sensor systems and digital building models was outlined on the basis of a typical scenario. In an earthquake event, earthquakes are to be registered at an early stage through a network of distributed sensors. The seismic data of the connected sensors as well as damage forecasts and diagnoses are to be distributed and reported in a targeted, decentralized manner to operators of critical infrastructures such as industrial plants or public buildings. Damage to buildings and/or industrial plants is to be diagnosed as early as possible to inform relevant audiences about it. Subsequent warnings can be relayed in a variety of ways. This ranges from audio and visual signals to direct coupling with facilities and equipment.

There are several challenges to overcome in this regard:

- The key challenge is the shortness of the warning time and the associated short response time (*real-time communication*).
- In addition to this required real-time communication, it must be taken into account that in the event of an earthquake, parts of the communication infrastructure may also fail, but (some) communication channels must still remain functional (*fail-safe*).
- In addition, large amounts of information may have to be distributed through the platform in the event of an earthquake. This must not result in any significant restrictions in terms of performance. Therefore, in the interests of efficient and secure communication, it must be ensured that information can only be fed into or retrieved from the platform in a targeted and needs-based manner (*needs-based and targeted communication*). This means, for example, that participants only receive information relevant to them and that only authorized participants can receive and feed in information (*security*).

The goal of the communication platform in the ROBUST project is to create a communication infrastructure that enables participants to exchange information in a demand-oriented, targeted, efficient, secure and real-time manner. The aim is to enable target group-specific, fail-safe and high-performance real-time communication between autonomous, decentralized participants.

For this reason, a communications infrastructure is being designed that:

- is based on a distributed, decentralized architecture,
- provides visibility and subscription-based communication filters, and
- ensures autonomy of sub-areas of the platform.

The decentralized, distributed architecture aims to,

- continue to guarantee functionality over as large an area as possible in the event of failure of certain components of the infrastructure, e.g. in the event of a partial failure of the platform, the functionalities of the unaffected areas continue to be guaranteed (robust and fail-safe communication),
- allow/support the operation of individual subnets encapsulated from other subnets,
- reduce the amount of information to be forwarded and counteract possible latency times by processing events or messages locally,
- enable, through a modular design, individually functioning systems for each site, which forward information to the overall system.

Communication filters limit the amount of information to be passed on and thus increase the *effectiveness* of communication on the part of both the *sender* and the *recipient*:

- *Restriction by sender (visibility/accessibility):* Messages that are transferred to the communication platform by participants (senders) should be configurable in relation to their recipients. Thus, each participant should be able to determine whether the message is only accessible to one participant, to a local participant network, or to all participants.
- *Restriction by recipients (subscriptions):* In order to ensure the effectiveness in the distribution of information also on the part of recipients of messages, participants must set up subscriptions in order to receive the desired messages. Participants without subscription(s) will not receive any messages. Subscriptions should be dynamically customizable and highly flexible. It should be possible to subscribe to specific message types, messages from specific participants, messages based on geographic region, and messages based on specific content.
- *Restriction of the circle of participants:* Open access to the platform should not be possible. That is, any circle of participants should be restricted to enable effective communication and limit potential disruptions. The information exchange should therefore occur in a closed and controllable circle of participants. To this end, the registration and deregistration of participants should be regarded as a fundamental prerequisite.

REQUIREMENTS FOR THE COMMUNICATION PLATFORM

Based on the objectives and solution approach of the communication platform described in the previous section, this section describes the functional requirements for the communication infrastructure. To this end, the requirements gathering method (Section: Requirements gathering method), the identified use cases of the communication infrastructure (Section: Use cases) and the functional requirements derived from them (Section: Functional requirements) are presented.

Requirements gathering method

Based on the reference scenario for the ROBUST earthquake early warning system, as well as the elaborated solution approach for the realization of the scenario (see above), functional requirements for the communication platform were developed systematically and together with potential users and stakeholders (chemical plant operator, bridge operator, hospital operator, fire department, etc.).

- First, the reference or application scenario of the ROBUST earthquake early warning system was fundamentally developed in a user workshop with potential users of the earthquake early warning and response system and iteratively refined in further coordination. In the application scenario, different actors should be able to interact with the communication platform (e.g., subscribe to or feed in messages) so that the ROBUST system can provide support in the event of an earthquake event.
- Based on this, stakeholders and the use cases of the communication infrastructure were identified, prioritized and selected in several workshops together with potential users of the future earthquake early warning and response system. These use cases were further analyzed and deepened in a further analysis workshop.
- In the final step, functional requirements were derived from the specified use cases. These functional requirements describe what the communication platform should do.

In the following, the use cases will be outlined and the essential functional requirements will be described in grouped form.

Use cases

The identified use cases for the communication platform are shown in Figure 2 as a UML use case diagram.

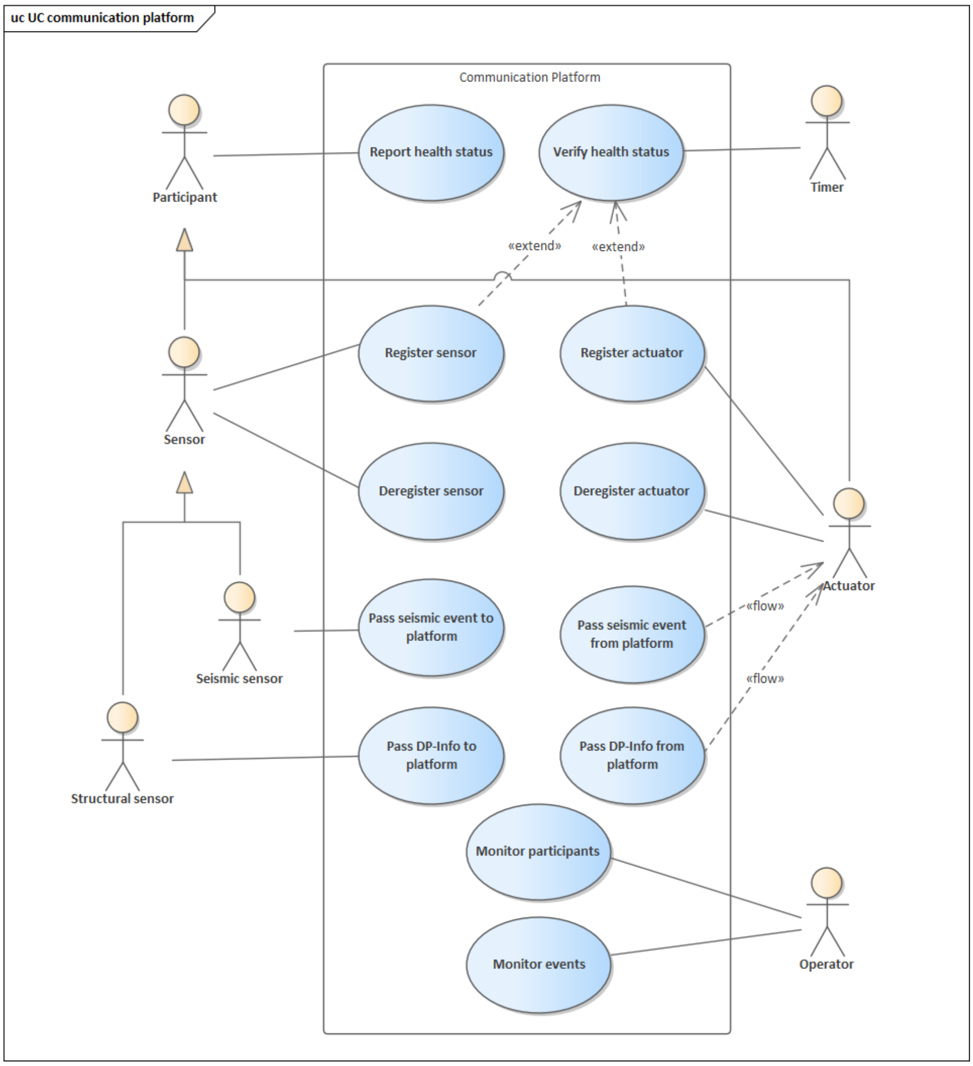


Figure 2. UML use case diagram of the communication platform

The actors (in the sense of users) of the communication platform are:

- above all the "participants", i.e. the actuators and sensors, whereby a distinction is made between seismic and structural sensors,
- the "timer", which activates the "verify health status" use case at specific times or intervals,
- the operational staff ("operators") who monitor the system and want to have an overview of existing participants, their activity, and occurring events.

The identified use cases can be divided into four areas:

- Register and deregister participants (sensor, actuator) in subnet(s),
- Event (seismic, building) passed to or from platform,
- Report and verify health status,
- Monitor system (participants, events).

Functional requirements

All identified use cases of the communication platform (CP) are described in more detail as functional requirements.

Registration of a participant: The CP should ensure that a participant can register. The CP should - after successful registration of a new participant - inform all previously registered participants in the relevant subnets about it. The CP should ensure that a new participant is informed about all other participants.

Formation of subnets by participants: The CP should offer the possibility to organize subnets hierarchically. The CP should enable "private" groupings/subnets. The CP must ensure that participants can organize themselves into different groupings/subnets or connect with each other. The CP must ensure that participants belong to at least one grouping/subnet.

Deregistration of a participant: The CP should ensure that a participant can deregister. The CP should allow all relevant participants to be informed about the deregistration of an individual participant.

Health status of participants: The CP should regularly check the health status of all registered participants to detect "lost" actuators or sensors to deregister them.

Query of the circle of participants: The CP should offer the possibility to query the current circle of participants.

Take over event: The CP must enable sending different types of information. This includes seismic information as well as structural diagnosis and prognosis information.

Pass on event: The CP must ensure the distribution of the information passed - seismic information and structural diagnostic and prognostic information - according to the notification criteria of actuators (if notification criteria of actuators exist). The CP must fundamentally send the information of a sensor intended for dispatch to all actuators in the respective group.

Access control: The communication platform (CP) must ensure that only authorized participants (sensors/actuators) can log on. The CP must ensure that information does not leave the boundaries of the respective associations/subnetworks.

Monitoring system (dashboard): The operator should see an overview of all existing participants (sensors and actuators) with their heartbeat (status message). The operator should see the state of a participant (health monitoring). The operator should see messages exchanged by the participants (communication).

COMMUNICATION PLATFORM CONCEPT

This section describes the concept of the communication platform for the ROBUST earthquake early warning and response system. For this purpose, the overall architecture of the communication platform and the tasks of the individual components of the architecture are presented, and critical design decisions (e.g., regarding inter-node communication and demand-driven subscriber-specific communication) are explained.

Overall architecture

The main components of the communication platform architecture are: Nodes, end devices (peripherals) and Rendezvous servers (cf. Figure 4).

The communication platform is formed by a network of so-called nodes. A node is operated by an organization participating in the ROBUST network and serves as an access point for the active end devices (sensors, actuators, hereinafter also referred to as peripherals) of this organization. Each node provides the entire functionality of the communication platform relevant to the end devices. Nodes network with each other and forward messages from their end devices to each other to enable communication of end devices across organizational boundaries.

End devices only communicate directly with the node to which they have been registered and logged on. Each node is responsible for assigning and managing the access data of its end devices. The distribution of messages across different nodes is transparent for the end devices. From the perspective of an end device, the entire ROBUST communication platform behaves like a single "large" node.

Nodes initially log on to the Rendezvous server and receive the address data of all other nodes in the network from it. Further communication then takes place directly between the nodes and is only routed via the Rendezvous server as a backup.

Node

A ROBUST node is a self-sufficient unit of the ROBUST communication platform and represents a kind of intelligent message broker. In essence, it serves as an intermediary instance of a publish-subscribe model for exchanging messages between a publisher (the issuer of the messages), and the subscriber.

A node consists of several microservice-like components that are grouped around the message broker and a persistent data store (see Figure 3).

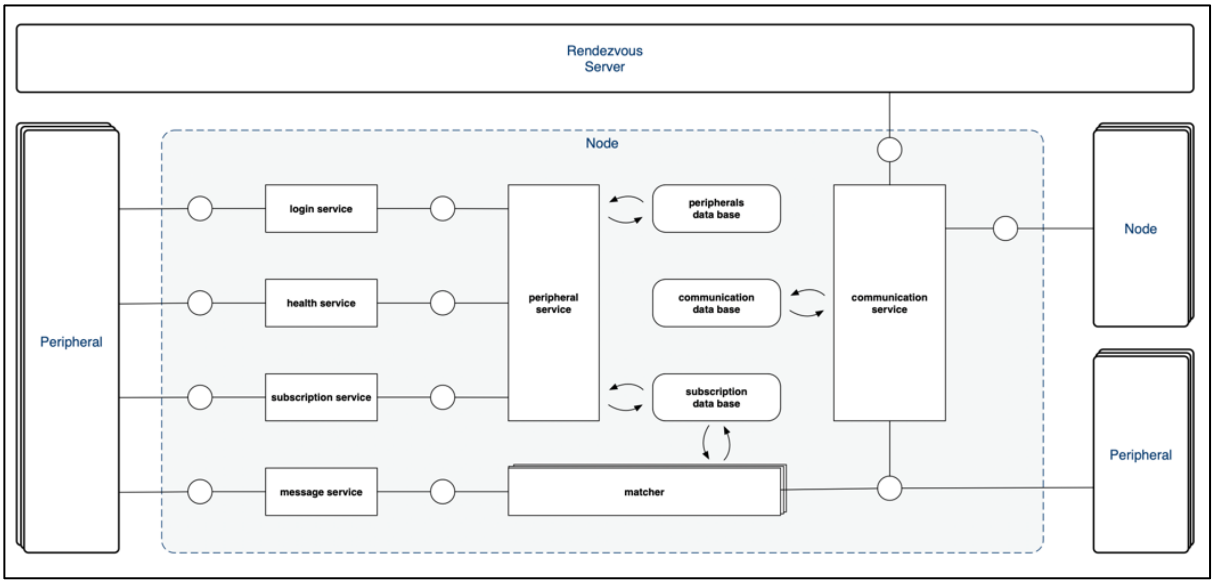


Figure 3. Node architecture and interfaces

The tasks of a node include the assignment and management of access data for end devices, session management for end devices, the management of content-related message subscriptions, and the subscription-specific distribution of messages to the end devices.

The node also communicates with the rest of the ROBUST network by logging on to the Rendezvous server and attempting to form a peer-to-peer network with other nodes. This is used to distribute messages from its own end devices and to receive messages from end devices of other nodes, which are then delivered to its own end devices on a subscription-specific basis.

(Inter-)Node communication

The nodes form a peer-to-peer network among themselves so that the communication platform remains functional even if individual nodes fail. If an individual node fails, only end devices directly connected to it are cut off from communication in the network.

Inter-node communication is realized by direct connections between two nodes at a time. A node receives the connection data of all existing nodes in the network from the so-called Rendezvous server, where nodes are registered and logged in to participate in the ROBUST network. The Rendezvous server thus represents a central component and a single point of failure - of the otherwise decentralized architecture. However, once the nodes are networked, they can maintain communication for a while even if the Rendezvous server fails.

Nodes always send messages redundantly over all available connection channels. Message duplicates are identified and discarded on the receiver side based on their unique Id. As a side effect of this strategy, the fastest available channel always "wins", which takes account of the earthquake warning scenario and the desired short response times. The somewhat increased network traffic due to duplicate messages sent can be accepted here without any problems.

Rendezvous Server

The Rendezvous server serves as the ROBUST network's central administration instance and switching point. It assigns and manages access data for the individual nodes. It provides the nodes with an HTTP-based interface to log into the network and obtain current address information of all other nodes in the network.

In addition, the Rendezvous server serves as a central message switching point that allows nodes to forward endpoint messages even if a direct peer-to-peer connection is not established.

Furthermore, the Rendezvous server collects information about the activities in the entire network. The nodes forward this information to the Rendezvous server in regular ping messages. This information collected by the Rendezvous server is made available to the operators for monitoring the system and visualized as a dashboard (e.g., as a web interface).

Complete self-organization of the nodes without a central switching point could only be achieved to a limited extent. An entry point into the existing network for new nodes would always be necessary; it would be conceivable to set up permanently and reliably accessible entry nodes. The degree of self-organization and robustness in the event of a Rendezvous server failure would, moreover, still be conceivable and could be based on the strategies of existing peer-to-peer networks.

Need-based participant-specific communication

End devices can subscribe to messages from the ROBUST network based on content criteria. The approach varies from the usual topic-based methods of many message-passing systems, such as MQTT. The result is greater flexibility in the design of subscriptions for the end devices, at the expense of greater complexity in the communication nodes. These must offer a kind of greatly reduced query language in which subscriptions are formulated and based on which the matching of messages to subscriptions takes place.

Furthermore, when providing information, it is possible for the peripherals (sensors) to control the distribution of this information directly. Each message/information transmitted to the node can be marked as private (no distribution by the node), protected (distribution only to peripherals of the own node) or public (unrestricted distribution) (see Figure 4).

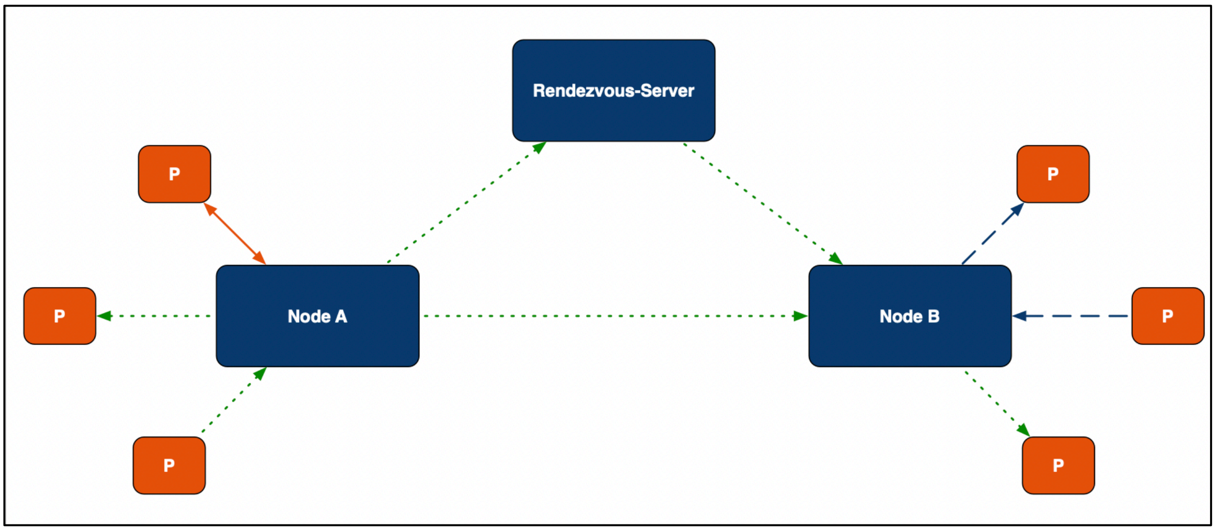


Figure 4. Control of information distribution and reach of nodes to their connected peripherals P (private: solid or red arrow, protected: dashed or blue arrow, public: dotted or green arrow)

REALIZATION

The presented concept of the communication platform for the ROBUST earthquake early warning and response system was implemented as a demonstrator application for practical use and testing in the ROBUST project. This section first presents the *technology stack* used to implement the individual components of the architecture and the communication between them. Subsequently, the implemented monitoring tool "*ROBUST Dashboard*" is described, which serves the operators for monitoring the function of the communication platform and occurring earthquake events.

Technology stack

This section presents the technology stack used to realize the individual components of the architecture and the communication between them (see Figure 5).

Based on the conceptual node architecture (cf. Figure 3), necessary adjustments were made to the technical design. Adjustments were necessary at various points. For example, the conceptual architecture included rights management in the peripherals. Due to the technical implementation using MQTT, this is now designed as a separate service in the technical architecture (incl. MQTT Access Control List ACL file), which makes rights management more flexible.

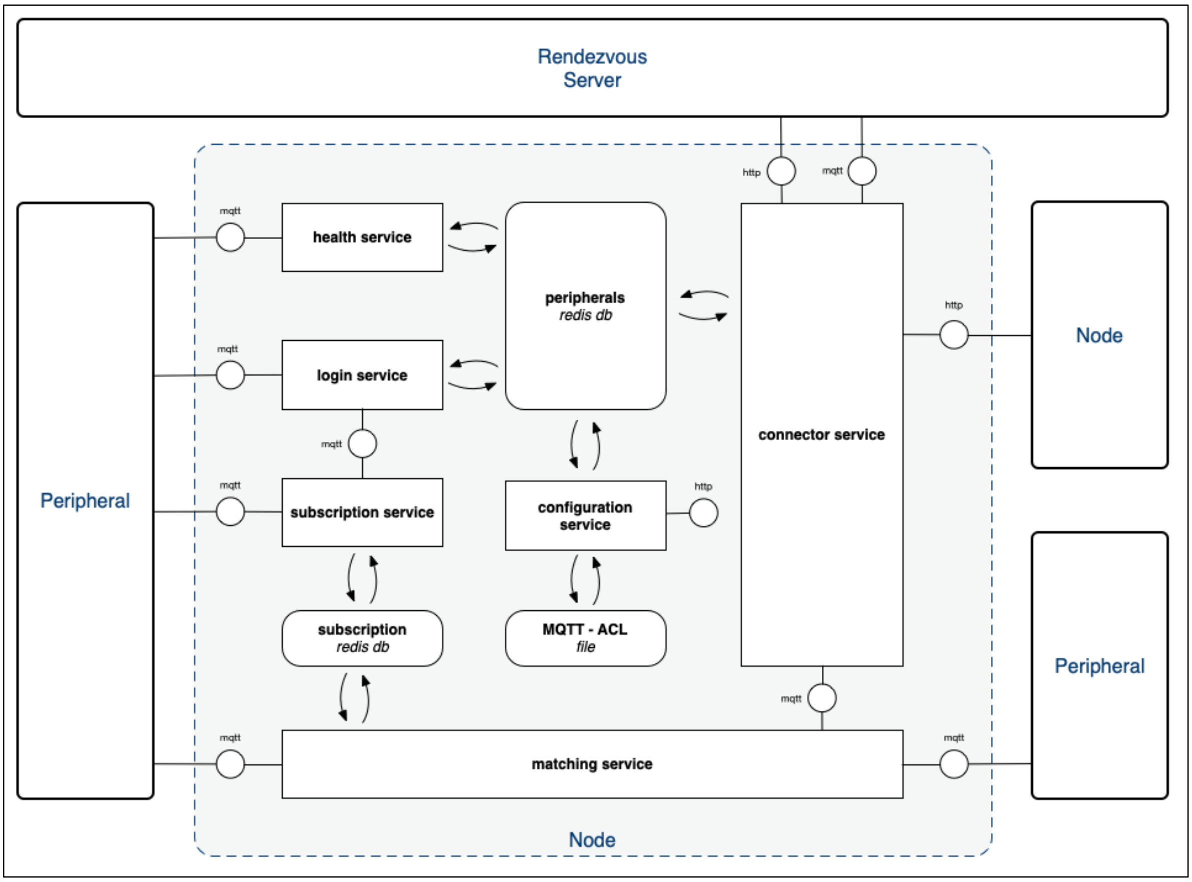


Figure 5. Technical implementation architecture of the communication platform

The software of the communication nodes and the Rendezvous server, was implemented predominantly in JavaScript as the programming language with NodeJS as the runtime environment.

The Rendezvous server consists of a single component that provides a REST API (http based interface) for managing the nodes' credentials and logging them in and out of the ROBUST network. The nodes themselves each consist of several functional components, represented by independent NodeJS processes, each of which covers only a narrowly defined task area within the node. These tasks include, for example, the handling of login information and session management, managing message subscriptions of the end devices, receiving and distributing messages, and connecting to the Rendezvous server and other nodes in the ROBUST network.

This modular design allows the individual components and their respective tasks to be maintained separately, expanded, or replaced as needed. This flexibility was particularly advantageous in the course of the research process with evolving requirements for the software. In production operations, too, the modular software offers advantages in terms of maintenance and further development.

The communication of the components within a node as well as with the end devices was realized via the MQTT protocol, which is specialized for Internet of Things (IoT) applications. The open-source message broker Mosquitto provides the heart of communication within each node, which also manages access rights to individual communication channels for internal components and end devices via access control lists (ACLs).

A further security layer was implemented through cryptographically signed session tokens for the end devices as well as cryptographic signatures attached to all exchanged messages. These procedures could be adapted more flexibly to the project's specific requirements than would have been possible purely with the integrated security mechanisms of MQTT and Mosquitto.

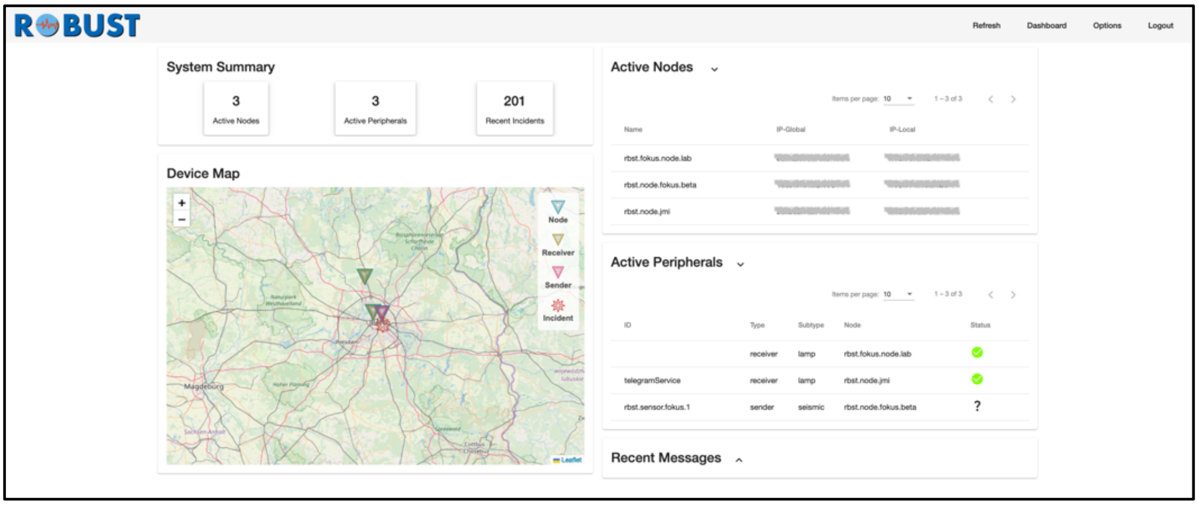
The Redis key-value store is used for persistent data storage (e.g., peripheral access data) and for caching recently processed messages. The Rendezvous server is also equipped with a Redis store and a Mosquitto broker, the latter for switching messages between nodes that cannot establish a direct connection to each other.

Deployment and process management within the nodes is done via npm packages and the pm2 process manager or via Docker containers and the Docker Compose orchestration tool. Here, too, attention was paid to flexibility and compatibility with as many potential hardware platforms as possible. Communication nodes can be run equally well on a virtualized server as on a RaspberryPi single-board computer, for example.

ROBUST Dashboard

The ROBUST dashboard was designed according to the requirements analysis as a central monitoring tool for the ROBUST network. It was implemented as a web-based single-page application with the Angular web framework and is operated alongside the Rendezvous server, whose data storage is also used as the basis for the data displayed in the dashboard.

The dashboard is mainly used to monitor the active components in the entire ROBUST network. Information about active nodes, their active end devices, and recently processed messages is regularly collected via the so-called ping messages from the nodes to the Rendezvous server (see Figure 6).



System Summary

3	3	201
Active Nodes	Active Peripherals	Recent Incidents

Active Nodes

Items per page: 10 1 – 3 of 3

Name	IP-Global	IP-Local
rbst.fokus.node.lab	[redacted]	[redacted]
rbst.node.fokus.beta	[redacted]	[redacted]
rbst.node.jmi	[redacted]	[redacted]

Active Peripherals

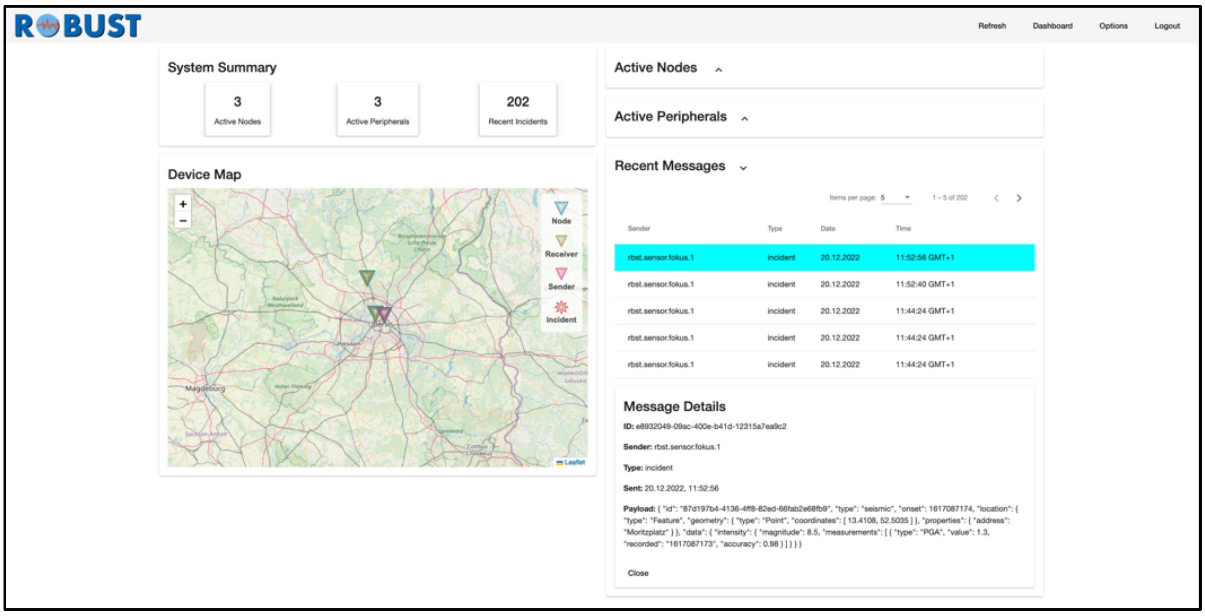
Items per page: 10 1 – 3 of 3

ID	Type	Subtype	Node	Status
	receiver	lamp	rbst.fokus.node.lab	✓
telegramService	receiver	lamp	rbst.node.jmi	✓
rbst.sensor.fokus.1	sender	seismic	rbst.node.fokus.beta	?

Figure 6. Dashboard with overview of registered devices

The dashboard is updated in real-time and thus also allows the immediate display of earthquake events on an interactive map (see Figure 7). Connection and status information of nodes and end devices allow monitoring and analysis of fault conditions.

Implementing the dashboard as a local, individual instance on the communication nodes would be possible with little technical effort. This would allow more targeted and detailed monitoring of their own end devices by the operators of a node.



Sender	Type	Date	Time
rbst.sensor.fokus.1	incident	20.12.2022	11:52:56 GMT+1
rbst.sensor.fokus.1	incident	20.12.2022	11:52:40 GMT+1
rbst.sensor.fokus.1	incident	20.12.2022	11:44:24 GMT+1
rbst.sensor.fokus.1	incident	20.12.2022	11:44:24 GMT+1
rbst.sensor.fokus.1	incident	20.12.2022	11:44:24 GMT+1

Message Details

ID: e8932049-09ac-400e-b41d-12315a7ea9c2

Sender: rbst.sensor.fokus.1

Type: incident

Sent: 20.12.2022, 11:52:56

Payload: { "id": "87d197b4-4136-4ff8-82ed-66fab2e68fb9", "type": "seismic", "onset": 1617087174, "location": { "type": "Feature", "geometry": { "type": "Point", "coordinates": [13.4108, 52.5035] }, "properties": { "address": "Moritzplatz" } }, "data": { "intensity": { "magnitude": 8.5, "measurements": [{ "type": "PGA", "value": 1.3, "recorded": "1617087173", "accuracy": 0.98 }] } } }

Figure 7. Dashboard with detailed view of a recently processed message

EVALUATION

The implemented communication platform (see Section Realization) was evaluated in an initial laboratory test. The aim of the lab test was to verify the feasibility and functionality of the communication platform concept.

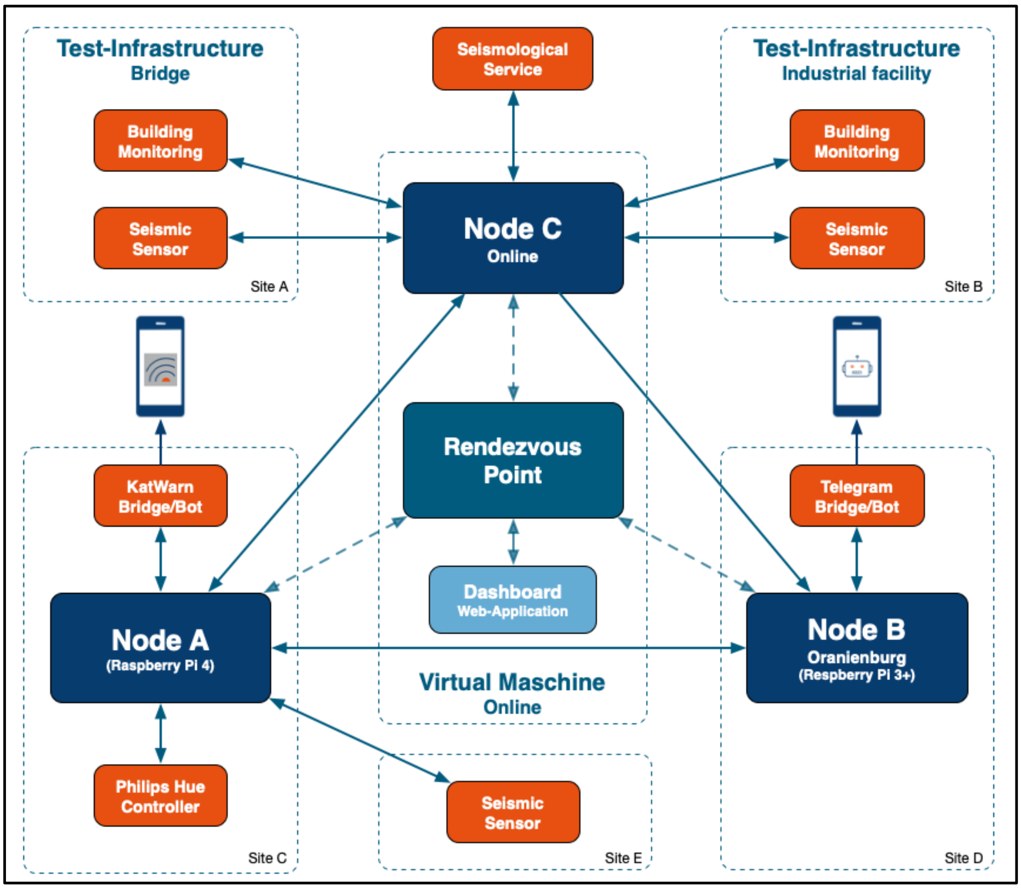


Figure 8. Setup of the test environment for the laboratory test

For this purpose, a test setup was set up that integrates several peripherals at various partners distributed across Germany (see Figure 8). The test site comprises five locations, some of which do not represent a real physical location. At two of these five locations, there is one communication node each, installed on RaspberryPi single board computers. A third node, accessible from everywhere over the internet, is deployed on a virtual machine in the cloud. Each peripheral is connected to one of the nodes. The "sensor/emitter" category of peripherals is represented by three seismic sensors and an earthquake early detection service. The "actuators/receive" category is represented by a Telegram bridge (Telegram is a cross-platform instant messaging service), a KATWARN bridge (KATWARN is a German warning system), a Philips Hue controller (Philips Hue is a smart light that could be controlled remotely), and two building diagnostic services, located at a road bridge and at an industrial plant. The test site was set up (in parts) in October 2022 and successively expanded. Since then, the communication platform has been running continuously and error-free so that the permanent functionality (continuous operation) could be verified.

In November 2022, several tests were conducted on the current test site that represents the ROBUST application scenario (see above). During the trials, the seismic sensors report earthquake events. Based on these events, the earthquake service detects an earthquake and sends an intensity forecast to the communication platform, which distributes it to all subscribers via inter-node communication. Actuators react to this information in different ways. The Telegram bridge sends out a warning message, the building diagnostic system creates initial predictions based on BIM and distributes them, KATWARN informs and warns users. With the help of own measurement technology on structures (bridge, building), which is activated on the basis of the first earthquake message, effects on the buildings are measured and diagnoses regarding possible damages and dangers are derived and distributed via the communication platform.

The initial laboratory tests carried out were successful. The various components distributed across Germany were successfully integrated and operated according to specification. In the tests carried out, the components of the communication platform functioned and cooperated and the desired ROBUST application scenario was successfully realized. Thus, the feasibility of the concept and the functionality of the implementation of the concept could be proven. This also laid the foundations for further developments, a long-term test (permanent functioning of the platform), and field tests with potential users planned for later stages of the project.

SUMMARY AND OUTLOOK

This paper describes the requirements, the concept and the technical realization of the ROBUST communication platform - a decentralized and distributed communication platform with target group-specific real-time information components for use as an earthquake early warning system. Within the scope of a laboratory test, the developed prototype was successfully operated and examined in 5 locations over a period of 4 months.

The next step is to test the system in practice. For this purpose, seismic sensors and ROBUST nodes will be installed in infrastructures such as a bridge and an industrial plant and tested by artificially triggered earthquakes. In particular, the key challenges - real-time communication, resilience and on-demand and targeted communication - will be investigated. The application scenario, the solution approach and the use cases of the communication platform were developed together with representatives of the target groups, potential users and stakeholders. The next step will be to deploy, test and evaluate the communication platform in a field test involving these target audiences.

In addition to evaluating the functionality and usability of the communication platform by later users, alternative technical concepts will be developed and tested. These include:

- Alternative approaches to the chosen on-demand communication scheme. Distributing the subscriptions of end devices via broadcast in the network would enable pre-filtering of messages at the producer node and as a result, more efficient distribution of messages between the individual nodes. While this approach adds complexity to the platform, it avoids the current flooding of the network with messages. Weighing these two approaches against each other in terms of performance and reliability appears interesting and will be explored in more detail in future analyses and simulations.
- Alternatives to the current inter-node communication protocol based on websockets will be explored. Non-IP-based wireless communication methods (e.g. LoRaWAN) are an interesting option to enable the communication platform to compensate to a certain extent for a large-scale failure of the IP-based network infrastructure (i.e., the Internet). The modular design of the nodes and the independence of specific hardware allows for such functions to be added flexibly for further analysis and comparison.
- The functionality of direct websocket connections between communication nodes was proven under laboratory conditions. However, additional development work is required for a reliable performance in the field, especially with regard to dealing with firewalls. Existing peer-to-peer technologies such as webRTC could be used as a model.

ACKNOWLEDGEMENTS

The communication platform presented here is currently being developed in the ROBUST research project with financial support from the German Federal Ministry of Education and Research (BMBF). We thank the ROBUST project partners, the project management & funder (grant number: 03G0892B, BMBF technical program GEO:N, Early detection of earthquakes and their consequences).

REFERENCES

UNDRR (2020) Human cost of disaster – An overview of the last 20 years (2000-2019). Centre for Research on the Epidemiology of Disasters (CRED) & United Nations Office for Disaster Risk Reduction (UNDRR), report, https://www.undrr.org/publication/human-cost-disasters-overview-last-20-years-2000-2019.

Clinton, J., Zollo, A., Marmureanu, A., Zulfikar, C. and Parolai, S. (2016) State-of-the art and future of earthquake early warning in the European region. *Bulletin of Earthquake Engineering*, 14, 9, 2441-2458. doi:10.1007/s10518-016-9922-7.

Allen, R. M. and Melgar, D. (2019) Earthquake Early Warning: Advances, Scientific Challenges, and Societal Needs. *Annual Review of Earth and Planetary Sciences*, 47, 361–388, https://doi.org/10.1146/annurev-earth-053018-060457.

Allen, R. M., Gasparini, P., Kamigaichi, O. and Böse, M. (2009) The status of earthquake early warning around the world: An introductory overview. *Seismological Research Letters*, 80, 5, 682-693, https://doi.org/10.1785/gssrl.80.5.682.

CWE (2023) ROBUST. Center for Wind and Earthquake Engineering (CWE), https://www.cwe.rwth-aachen.de/projekte/erdbebeningenieurwesen-projekte/robust/.

Najdahmadi, B., Pilz, M., Bindi, D., Razafindrakoto, H.N.T., Oth, A. and Cotton, F. (2023) Hazard-informed optimization of seismic networks for earthquake early warning – the case of the Lower Rhine Embayment (western Germany). *Journal of Seismology* (accepted).

ShakeAlert (2023) ShakeAlert: An Earthquake Early Warning System for the West Coast of the U.S.. USGS Earthquake Early Warning, https://www.shakealert.org/.

CEEWP (2023) Carliforia's Emergency Services. State of Carlifornia, https://www.caloes.ca.gov/.

Pittore, M., Bindi, D. Stankiewicz, J., Oth, A., Wieland, M., Boxberger, T. and Parolai, S. (2014) Toward a Loss-Driven Earthquake Early Warning and Rapid Response System for Kyrgyzstan (Central Asia). *Seismological Research Letters*, 85, 6, 1328–1340. doi: 10.1785/0220140106.

Megalooikonomou, K. G., Parolai, S. and Pittore, M. (2018) Toward performance-driven seismic risk monitoring for geothermal platforms: development of ad hoc fragility curves. *Geothermal Energy*, 6, 1. doi: 10.1186/s40517-018-0094-3.

Ostachowicz, W. and Güemes, A. (2013) New trends in Structural Health Monitoring. Springer Verlag, Wien, doi: 10.1007/978-3-7091-1390-5.

Yan, L. (2011) A survey on communication networks in emergency warning systems. Report WUCSE-2011-100. All Computer Science and Engineering Research. https://openscholarship.wustl.edu/cse_research/54.

Khaled, Z.El. and Mcheick, H. (2019) Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service. *International Journal of Distributed Sensor Networks*, 15, 2, doi:10.1177/1550147719829960.

SARMEX (2019) Sistema de Alerta Sísmica Mexicano (SASMEX). Centro de Instrumentación y Registro Sísmico (CIRES) A. C., http://www.cires.org.mx/.

Suárez, G. (2022) The Seismic Early Warning System of Mexico (SASMEX): A Retrospective View and Future Challenges. *Frontiers in Earth Science*, 10, https://www.frontiersin.org/articles/10.3389/feart.2022.827236, doi: 10.3389/feart.2022.827236.

IEEE (2023): 802.11 Wireless local area networks, http://www.ieee802.org/11/.

Zhang, H. (2017) Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. *IEEE Communications Magazine*, 55, 8, 138-145, doi :http://doi.org/10.1109/MCOM.2017.1600940.

Gündogan, C., Kietzmann, P., Schmidt, T.C. and Wählisch, M. (2019) ICNLoWPAN – Named-Data Networking for Low Power IoT Networks. *IFIP Networking Conference 2019 (IFIP Networking 2019)*, Warsaw, Poland, 2019, 1-9, doi: 10.23919/IFIPNetworking.2019.8816850, https://arxiv.org/pdf/1812.07025.pdf.

NDN (2010) Named Data Networking (NDN) Project. NDN, Tecnical report NDN-0001, https://named-data.net/techreport/TR001ndn-proj.pdf.

Shang, W., Yingdi, Y., Droms, R. and Zhang, L. (2016) Challenges in IoT Networking via TCP/IP Architecture. NDN, Technical Report NDN-0038, https://named-data.net/wp-content/uploads/2016/02/ndn-0038-1-challenges-iot.pdf.

Nolan, K.E., Guibene, W. and Kelly, M.Y. (2016): An Evaluation Of Low Power Wide Area Network Technologies For The Internet Of Things. International Wireless Communications and Mobile Computing Conference 2016 (IWCMC 2016), Paphos, Cyprus, 439-444, doi: 10.1109/IWCMC.2016.7577098., https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7577098.

Shang, W., Gawande, A., Zhang, M., Afanasyev, A., Burke, J., Wand, L. and Zhang, L. (2018) Publish-Subscribe Communication in Building Management Systems over Named Data Networking. *28th International Conference on Computer Communication and Networks 2019 (ICCCN 2019)*, Valencia, Spain, 1-10, doi: 10.1109/ICCCN.2019.8846951, https://named-data.net/wp-content/uploads/2018/10/ndn-tr-0055-1-ndn-ps.pdf.

MQTT (2023) MQTT: The Standard for IoT Messaging. MQTT.org, http://mqtt.org.

Redis Streams (2023) Redis Streams tutorial - A comprehensive tutorial on Redis streams. Redis Ltd., https://redis.io/topics/streams-intro.