Street Art & Urban Creativity | Vol. 11, No. 7, 2025 | ISSN 2183-9956
Street Art & Urban Creativity. Scientific Journal
https://doi.org/10.62161/sauc.v11.6007

LoRaWAN Reliability Improvement Using Calibration of RF Planning and Redundancy

Field Results for DIN Flood Alarm System

Johnny J Mafra Jr [1], Diogo Carneiro Ribeiro Bueno Martins [2]
[1] Fitec, Brazil
[2] Cemig, Brazil

KEYWORDS
LoRaWAN
Reliability
Availability
Flood Alarm
Site Survey
Sniffer
RF Simulation

ABSTRACT
Brazil reached an all-time high of 118 dams in emergency in 2023, which warranted the development of an alarm system. Since LoRaWAN lacks reliability, mainly regarding downlink messages, this work presents a solution to take the availability to the highest levels. Alarms were 100% delivered within 5 minutes and FUOTA transmitted a firmware split into thousands of fragments reliably. It is also presented an approach to calibrate the RF simulation to make it fit better with the measurements. This took the availability from 77% to 91%. For SNR above -10 dB the availability is as good as 95%.

RECEIVED: 01/ 09 / 2025
ACCEPTED: 28/ 09 / 2025

1. Introduction: Previous history of dam failure and related work review

When it comes to the history of dam failures, we can pinpoint two major milestones: the Mariana dam failure, in November of 2015, and the one in Brumadinho, in January of 2019. These two tragedies, which caused hundreds of deaths and extensive environmental damage to river basins, have brought the issue of dam failures to the headlines ever since. Notwithstanding the 2010 Brazilian law No. 12,334 establishes the National Dam Safety Policy, which defines the Self-Rescue Zone as the area downstream of the dam where there is insufficient time for authorities to intervene in emergencies. In these areas, the responsibility for notifying and alerting the population falls directly on the dam developer.

The revision of the National Dam Safety Policy by Federal Law No. 14,066/2020 requires: "provision for the installation of a sound system or other more effective technological solution in alert or emergency situations". Traditionally, emergency alarms at dams are provided by high-powered sirens, but their infrastructure demands robust characteristics, such as reliable remote activation, supervision, and batteries. Therefore, each siren station is expensive.

Later, Resolution No. 95/2022 of the National Mining Agency (ANM) established that for dams with high or medium Associated Potential Damage the developer must implement automated siren activation systems, along with other effective warning mechanisms in the self-rescue zone. These systems must be installed in safe locations, preferably outside the flood zone, and have safeguards to ensure they operate properly even in the event of failure. Furthermore, the Emergency Action Plan for Mining Dams must include specific measures to alert and evacuate the population residing in the self-rescue zone, ensuring that everyone is aware of the procedures to follow in case of emergencies.

The National Water and Sanitation Agency (ANA) has been registering and classifying dams in the country since 2011. Dams are classified according to what they´re being used for, like hydroelectric power, irrigation, flood protection, recreation, animal watering, flow regulation, industrial waste containment, mining tailings containment, industrial use, and environmental protection. They are also classified by categories such as risk, associated potential damage, and reservoir volume. As of 2023, there were 25,943 dams registered in the National Dam Safety Information System. 1,591 of them are classified as medium or high risk having great potential for associated damage in the event of a rupture (ANA, 2024). With that in mind, the number of dam related emergencies in Brazil reached an all-time high of 118 in 2024, which shows a significant increase compared to the 94 cases recorded in the previous year. This increase is partly explained by the implementation of new resolutions by the ANM, such as Resolution No. 175/2024, which establishes stricter standards for the safety of tailing dams (ANM, 2024).

Cemig, a major Brazilian company focused on energy generation, transmission, distribution and commercialization company was a pioneer in developing emergency plans for dam ruptures for its hydroelectric plants, having begun studies on the topic as early as 2003. The company has procedures for field inspection, collection and analysis of instrumentation data, preparation and revision of dam safety plans, as well as for planning and monitoring maintenance services, analyzing results, and classifying its civil structures. Specific emergency plans are currently available for each dam. Since 2018, the company has maintained its policy of strengthening relationships with external stakeholders focused on emergency situations, specifically the Municipal Civil Defense and Protection Coordination Offices.

The case of hydroelectric dams is unique, because they are also used for river flow regulation. That said, this poses a potentially serious side effect, as controlling the dam's level, albeit to ensure its own safety, can eventually recreate the process of natural flooding during the rainy season. Moreover, every year, excessive raining that happens close in regions to a hydroelectric dam, can make the area susceptible to a flood. That is, there is not even the need for a catastrophic event in the dam itself for it to constitute an emergency, thus demanding an alert emission.

LoRa is a technology specifically designed for sensor data gathering. This way, most of the studies are related to sensor design and optimization, such as the uplink Automatic Repeat Request proposed by Choi (Choi et al., 2020). Anyway, some studies embrace the disaster

management area, ranging from sensor data gathering to warning transmission. Even fewer studies are dedicated to the improvement of the reliability of RF communications.

Zhang presents the design and evaluation of a real-time IoT-based emergency response and public safety alert system tailored for rapid detection, classification, and dissemination of alerts during critical incidents (Zhang et al., 2025). It uses several types of RF, such as Wi-Fi, 5G and LoRa. LoRa is specifically a fallback for rural or low connectivity environments, since it is based on secure MQTT over TLS. A prototype system was deployed in a controlled environment to simulate real world emergency scenarios. Alerts are dispatched to mobile devices, dashboards and control rooms.

In emergency situations, mobile communication service might not be available. For these cases, Sciullo proposed a system which consists of a mobile application connected to a LoRa transceiver via Bluetooth Low Energy (BLE) (Sciulo et al., 2020). Through the app, users can send emergency requests that are re-broadcasted by other peers until reaching a rescue personnel who is able to handle the emergency.

For RF communications reliability improvement, an interesting approach is presented in the paper by Sisinni, which replicates messages in the data link layer using different chirp durations. This repetition scheme is a proposed protocol called LoRa-REP. It increases the chance of at least one message copy being received correctly (Sisinni et al., 2022).

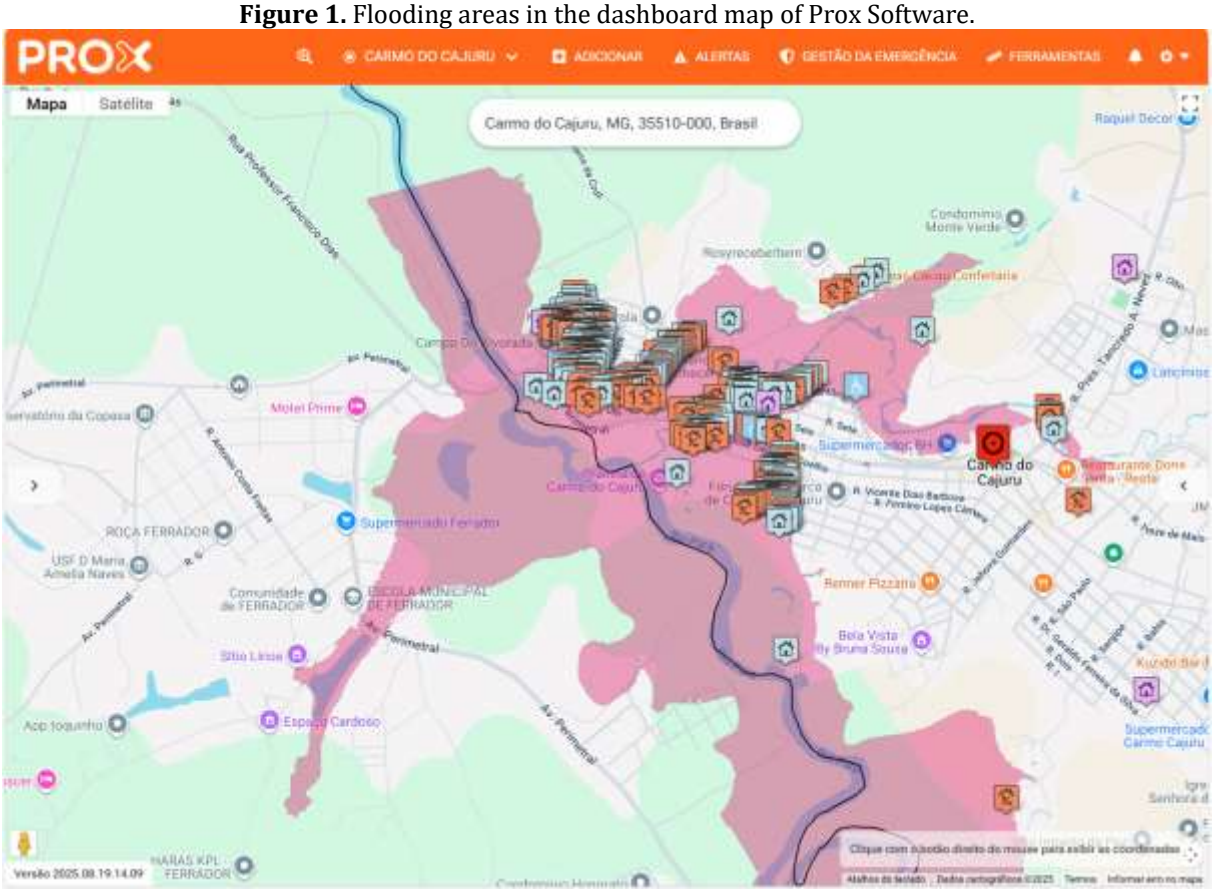
The study by Rayess based on simulations introduces blind repetition in LoRaWAN: a packet is retransmitted a fixed number of times regardless of its good reception. Leveraging on existing data link layer functionalities, it compares this redundant mode to two existing modes, namely the unacknowledged mode and acknowledged mode (Rayes et al., 2023).

A paper by Coutaud about ADR (Adaptative Data Rate) algorithm optimization presented experimental results about packet delivery rates in function of SNR similar to the results obtained in this work (Coutaud et al., 2020).

1.1. Emergency alarm solution implemented

The system designed to provide emergency alarms is called Prox. The process of its development consisted first in the 3D mapping of the self-rescue zone and the downstream river valley, in order to determine the flooding areas for each type of event, ranging from a light rainfall to a critical storm, as well as dam overtopping and dam collapse. The operation squad has a dashboard with this mapping, showed in Figure 1. In their first approach to implementing an emergency alarm they took the traditional route, which was to install sirens. It was done in 6 of the 32 powerplants of Cemig. Considering its high cost and limited effectiveness, the second step was to include an alarm through a smartphone application, which is when an app also called Prox was made available to everyone through the traditional appstores. The app reads the GPS position of each smartphone and in case of an emergency, provided that the position is inside the flooding area, an alarm is sent out. to the applicable ones. When developing the app, something kept in mind was the importance of creating a relationship with the users, with the aim of making it known the vital nature of being aware about the alarms.

Figure 1. Flooding areas in the dashboard map of Prox Software.



Source: Own elaboration, 2025.

Seeing as the dams and their self-rescue zones are normally in remote rural areas, it is most common that there is no 4G coverage, due to both the distance and the topography. This way, it was initiated the development of a coverage solution for these areas in 2020. The technology chosen was LoRaWAN due to its long range, low energy consumption and low cost. Because of the high power needed for the sirens, several horns must be used, as well as high-power amplifiers, big batteries, and their respective high-power charge controllers. All of which are inside big electrical boxes installed in a robust pole. All of this combined leads to a high cost for the siren option. Meanwhile, the cost of the LoRaWAN solution is around 5 to 10 times smaller, providing attractive payback. With that in mind, the solution described in this work has been installed in 11 dams.

An end-to-end LoRaWAN system was developed for this purpose. The same Prox software manages the system, registers the end users and sends the alarms. The LoRaWAN infrastructure uses the opensource network server Chirpstack, standard LoRaWAN gateways, end devices called DIN (Devices for Individual Notification) and a LoRaWAN application called SND (System for Notifications to DIN). The application SND terminates the application protocol, handling the alarms and managing DIN network. This solution is called DIN System.

The DIN device was carefully designed with the objective of harmonizing with the households in which it will be present (Horta & Damas, 2022). It has an e-paper display to show messages, a buzzer for the alarm and a high intensity red LED light that glows within its whole coverage to reinforce the alarm. Additionally, it has a battery that keeps it working for at least 24 hours without energy, something that could happen in emergency events, and a GPS to provide its location in real time, just like the smartphones used in the Prox system, allowing it to send alarms solely to the devices inside of the flooding area. When operating normally, the display shows the date and the weather forecast for the current day as well as the next three days. This is done to build a relationship with the users and gain their confidence, as it shows that the system is reliable and assures the users that emergencies will be met with an adequate response (Figure 2).

However, any communication system is prone to lose data. Especially LoRaWAN, which is designed for resource-constrained networks and optimized to send uplink messages (de Carvalho Silva et al. 2017). This means that there is no guarantee that the message would reach the destination, and that the downlink messages could be lost more easily, since they are not the main concern of LoRa. This is a paradoxical situation, seeing as an alarm system must be reliable. Therefore, the whole point of this paper is to show the solution designed, implemented and validated to increase the reliability of LoRaWAN communication. It comprises the improvement of RF coverage and the package delivery guarantee for alarms and new versions of firmware.

Figure 2. DIN device showing weather forecast and alarm.

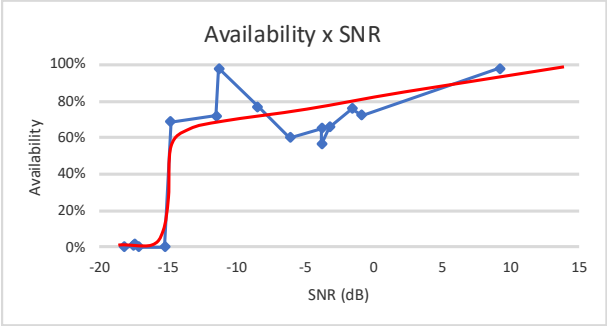
Source: Own elaboration, 2025.

2. Method

2.1. RF coverage improvement

LoRaWAN is highly sensitive, consequently posessing a huge range. That being the case, with only a few gateways a wide area could be covered. However, even being within the specifications, the sensitivity is still limited by the reliability needed. In a previous work, it was observed the behavior of reliability against the quality of the signal. Reliability is represented by the availability of the communication packages, which is measured by the ratio of received packages by the ones that were sent. The quality of the LoRaWAN signal is represented by its SNR. This is preferred over the RSSI because it is used to control SF (Spreading Factor) in the ADR (Adaptive Data Rate) algorithm. In Chirpstack, the open-source network server used, the primary parameter controlling ADR is the SNR margin. It calculates an SNR margin for each uplink as the maximum received SNR across gateways minus the required SNR to demodulate the current data rate (which depends on the spreading factor). It then takes the maximum SNR margin over a history of recent uplinks (typically the last 20, though configurable). After subtracting a configured installation margin (default 10 dB), the remaining margin determines the number of steps the data rate can be increased (each step is approximately 3 dB, allowing a shift to either a higher data rate or lower spreading factor) and optimizes the transmission power index. If the margin is insufficient or uplinks are lost (inferred from frame counters), it decreases the data rate to improve reliability (Chirpstack, 2025). Figure 3 (Leitão, et al., 2022) presents the availability observed in a sample of almost 20 end devices out of the 40 deployed in the field, all presented with different distances, building obstacles, and relief. The avaiability is relative to the uplinks of an AMI (Advanced Metering Infrastructure) system, therefore, it differs from the case of this paper, which is associated with the downlink. It can be observed that the availability increases from around 70% to close to 100% as a function of SNR except below -15 dB. Below this threshold it falls abruptly to close to zero.

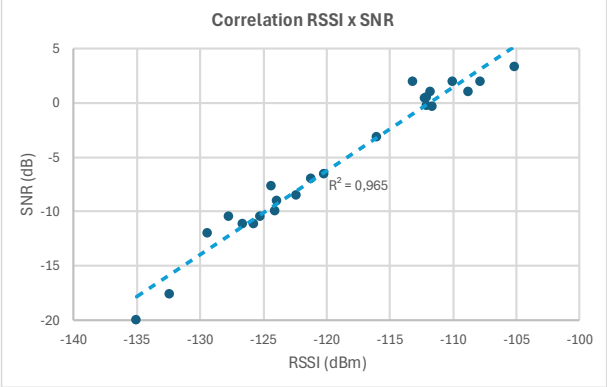
Figure 3. LoRaWAN availability as a function of signal quality.



Source: Leitão, et al., 2022.

This limiting behavior was considered in the RF estimation. SNR can be linearly related to RSSI as can be seen in the results obtained by measurements made in this work in the field, shown in Figure 4. This way, the limit of -120 dBm was selected, which corresponds to a SNR between -10 and -5 dB, leaving a safety margin to -15 dB limit, and an availability close to 80% according to Figure 3. The simulation model was configured by implementing model ITU-R P.1812.6, which is widely used in the detailed evaluation of signal levels in terrestrial point-area services. This model is applicable to frequencies between 30 MHz and 6 GHz, covering distances from 250 m to 3.000 km, and it takes the terrain profile into consideration in the propagation calculation (ITU-R, 09/2021). To ensure a safety margin in coverage prediction, the temporal and spatial availability parameters were set to 95%, which means that 95% of the time (throughout the year) and in 95% of locations, the signal level will be above the predicted value, reducing the likelihood of shadow areas or service unavailability. The simulator can be easily parametrized with this RSSI limit to generate the heat maps, allowing the evaluation and optimization of the placement of the gateways.

Figure 4. LoRaWAN availability as a function of signal quality.



Source: Own elaboration, 2025.

2.2. Calibration of the simulation

After the first deployment of the system, it was made clear that there was a sensible difference between the simulation and the measurements in the field because the observed RSSI and SNR at network server were different from the calculated ones, as they were unfortunately worse. In order to counter that, it was developed a process to calibrate the simulation. It consists of a mobile LoRaWAN gateway assembled in a 14 m high telescopic pole and a sniffer (Figure 5). The sniffer is simply a LoRaWAN DIN end device with a special firmware. It works in a way similar of an ICMP ping. It sends 10 requests to the application software and waits for the responses. Then it presents the number of responses, as well as the minimum, average, and maximum value of the measured RSSI and SNR. It operates fixed at SF12, or DR0 to make the results comparable by eliminating this variable. The downlink DR is a function of the uplink data rate (LoRa Alliance, 2017). Since the uplink is fixed in DR0, it will be fixed in DR8 as the specification AU915 used in Brazil in the downlink, that is, always the most sensitive one in each direction.

Figure 5. Mobile 14 m gateway pole and sniffer

Source: Own elaboration, 2025.

One of the sites (in which the system was installed) chosen to exercise the calibration procedure was the one with the larger amount of end devices, as it would provide a good statistical effect. Thus, the following discussion is related to the region of Carmo do Cajuru, State of Minas Gerais, Brazil, which possesses a dam of a hydroelectric power plant, operated by Cemig. After the first step of the simulation and selection of the gateway sites, site surveys were done at the sites. The mobile gateway was placed in each one of these sites while the sniffer was taken to several points of interest to make RSSI and SNR measurements. The result shown in Figure 4 was obtained this way.

The second run of the simulation had its parameters modified to ensure that the prediction aligned with actual environmental conditions. Adjustments were made iteratively, refining the model until the values obtained were within an acceptable margin of accuracy relative to field measurements. This way, the fading margin was adjusted through the change of one of its components, the confidence margin. The cable and connector loss were also adjusted to a higher value, as to include, besides their own losses, the effect that the end device is indoor in normal use. Once the model was validated, a new study was conducted simulating an updated set of installation points.

2.3. Ensuring alarm delivery

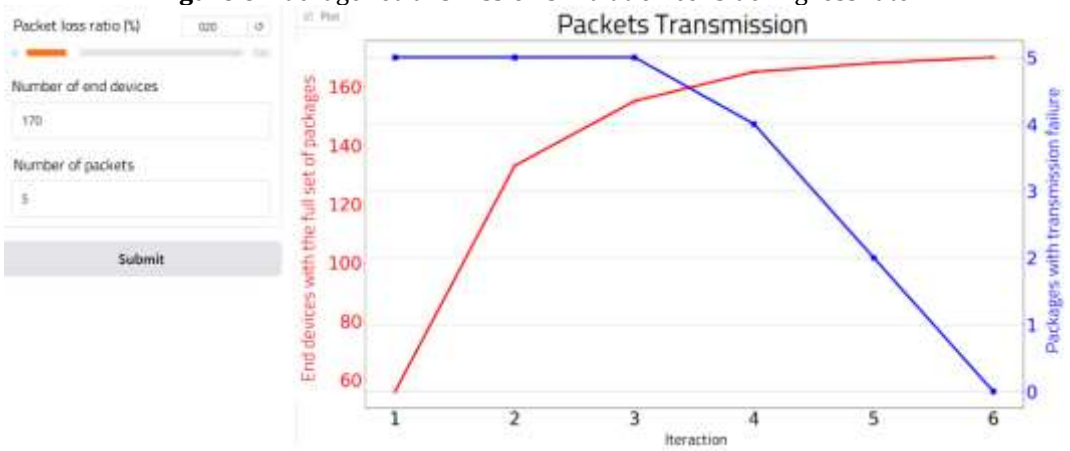
The improvement of coverage provided good results, but there may still be package loss. And even if further improvements were made, it could still happen. This makes it mandatory for an alarm system to provide means of ensuring delivery. This requirement led to the development of the redundancy scheme described in this work.

An alarm in the DIN System consists of a download multicast packet from SND application containing the alarm and the compacted list of the end devices inside the flooding area, plus up to four packets containing the text message to be displayed. This is because the display allows messages up to almost 200 bytes, and the worst case of LoRaWAN package is around 50 bytes. This way, there would be a maximum of five packets. As discussed above, the RF simulation was done considering a limit in SNR that provides an availability around 80% in the worst case. This means that up to 20% of the packages could be lost.

Then the number of retransmissions needed to guarantee 100% probability of receiving all the packages considering that each time a transmission is done there is a probability of loss of 20%

was calculated. The figure found was 6 retransmissions. To check if this would work before field deployment a simulator was implemented finding the results of Figure 6.

Figure 6. Package retransmission simulation considering loss rate.



Source: Own elaboration, 2025.

To further improve the reliability of the alarm, once an end device receives one, it sends uplink an ACK message. Since it is comprised of only one package, the calculated repetitions were 5. This was also confirmed in the simulator presented above.

To double check this, the end device's ACK uplink package loss probability due to collision was verified. The ACK is approximately 10 bytes long, and in DR0, with a transmission rate of 250 bps, it will generate a packet lasting 313 ms, which we rounded to 500 ms for use in the collision simulator, another tool developed in this work. This simulation showed a collision probability smaller than 20%, which is our reference, for ACK transmissions within 60 s in a population of 100 end devices in an 8 channel LoRaWAN system.

On the SND application side, the alarm packet duration at the slowest downlink transmission rate, DR8, is 980 bps to transmit 53 bytes, which is 474 ms, which we'll round to 0.5 s. This is consistent with the 0.493 s measurement obtained. In other words, transmitting 5 packets takes at least 2.5 s. We'll assume 5 s, since there's an unknown delay between each transmission. It was implemented to send twice the calculated, sending 12 times the 5 packages with a 50 s interval between each one, taking 10 minutes to complete the task.

The algorithm implemented in the end device side considers that from the moment the end device receives the first alarm packet, it must begin transmitting ACKs with confirmation request, randomized within 60 s and ignoring any similar alarms received in the next 50 seconds. This will be repeated 5 times, up to a time period of 5 minutes, and can be interrupted upon receiving the first confirmation.

To stop the alarm, this same process must be repeated for a stop alarm command.

This way, after 6 alarm transmission in 300 s, it is certain that all the DINs must have received the alarm, as presented in the calculation and simulation above. The requirement is that this timespan must be shorter than 5 minutes in the self-rescue zone, due to the estimated time for a wave caused by the dam rupture to arrive. The ACK transmission is there just to increase even more the system reliability. Additionally, the DIN system management software, SND, has the exact information of each DIN that hasn't received the alarm. Since lives can be at stake, the operator can make a decision regarding the contingency action in this case, which could even be to send rescue.

2.4. FUOTA

Considering that the end device DIN has somewhat complex firmware, it is prone to bugs. In order to maintain confidence in the solution, it is mandatory to have the possibility of remote firmware update without recalls. It is even necessary to comply with new regulations, like EU CRA (European Union Cyber Resilience Act), that demand the possibility of the application of patches

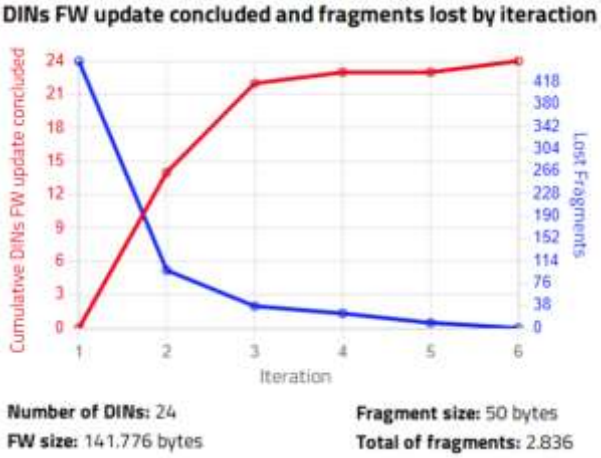
when a vulnerability is found (The European Parliament and the Council of the European Union, 2024). The situation becomes even more complex due to the firmware being considerably large, in the order of close to 200 kB. Since in the worst case of LoRaWAN package sizes they are as small as 50 bytes, it would take around 3.000 packages to transport the whole firmware. As mentioned above, the parameter considered in this work, which has dimensioned the alarm procedure, led to the package loss ratio of 20%. But there could be individual DINs with ratios worse than that. With that in mind, the firmware update scheme must be capable of handling all these challenging requirements.

The choice was to take the redundancy scheme presented previously to the limit. Despite LoRaWAN having a FUOTA (Firmware Update Over The Air) specification, it must be configured estimating the package loss. Moreover, as stated at the specification, it is not designed for very small data blocks nor for very large ones due to constraints on the link layer (duty cycle limitation and longtime on-air) (LoRa Alliance, 2022). Seeing as the package loss ratio can change for different sites and even for individual DINs, it is not applicable to use a worst-case ratio that fits for all. It would be too big for several sites, making the time spent on firmware update unnecessarily long for many of them or too short for critical ones. The developed algorithm was based on one used in previous work on Wi-SUN, which had a proven solution and was deployed in thousands of units in the field (Mafra et al., 2015).

The implemented algorithm for FUOTA sends the opening of the process with information such as the version identification, the number of packages and the hash for verifying the firmware integrity at the end of the process. Then, it makes the first transmission of each one of the thousands of packages. This first step can take days, considering the interval needed between each one to avoid collisions. When finished, SND sends a request for missing packages. To guarantee its receiving, the downlink is sent 20 times in 30 s intervals, totaling 10 minutes. Then each DIN answers with the missing packages, which are limited to 25 at a time, since the size limit of each package is around 50 bytes. This is done by sending confirmed uplinks up to 5 times, since it is just one package. SND then organizes all the missing packages, removing the repetitions and retransmits them. This process is then repeated as many times as necessary, informing up to 25 missing packages, until the last DIN receives all of the packages. At the end, the firmware integrity is verified, and its execution is started. One advantage of this process over the one specified by LoRaWAN is that it needs only the size of the firmware for extra memory instead of its size plus the estimated package loss ratio.

Figure 7 presents the evolution of FUOTA for an average package loss ratio of almost 2% obtained in laboratory environment, contemplating 24 DINs and a firmware to be updated split into 2.836 packages. The first steps can comprise the totality of the packages, which takes a long time. After that, there is a decrease in the number of packages, which also decreases the time, making the process accelerate even further in each pass. It took only 6 iterations and 28 hours to finish the update. This is because 2% is a very low package loss ratio, and having only 24 end devices allowed an interval of 30 seconds between the transmission of each package without degradation because of collision. Anyway, if collision occurs causing package loss the algorithm would selfheal it.

Figure 7. FUOTA evolution for 2% of package loss in lab environment.



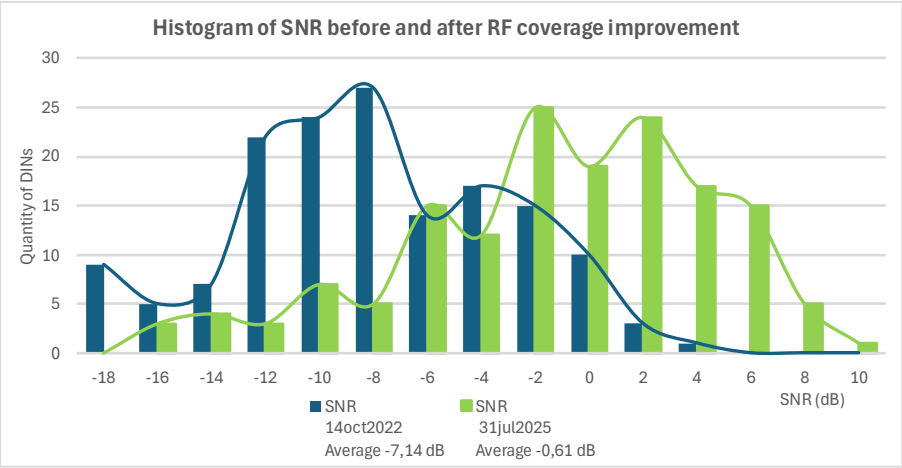
Source: Own elaboration, 2025.

3. Results

3.1. Field results of the improvement of coverage

As previously stated, in the first attempt, the RF simulation considered the -15 dB limit for SNR that was found in the previous work and two gateways were installed in the region. But the results weren't as good as expected. In fact, communication was established, just not with the availability needed for an alarm system. After the calibration and the new simulation, three new gateways were installed. Figure 8 presents the Histogram of SNR before and after their installation for the roughly 180 end devices distributed in the region. It became clear that before the -15 dB limit was reasonably well observed, there were only a few end devices below the limit. So the limit was moved from -15 dB to around -10 dB and the average moved from -7,14 dB to -0,61 dB.

Figure 8. Histogram of SNR before and after RF coverage improvement.



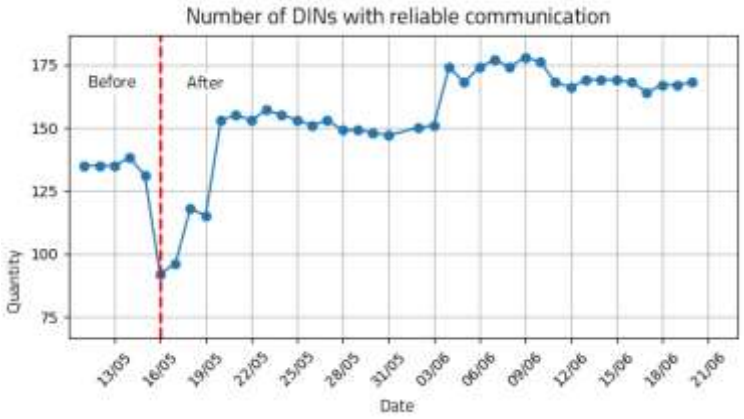
Source: Own elaboration, 2025.

The availability was calculated using data provided by SND software which manages the end devices. The number of how many packages transmitted by SND actually reach the end devices is controlled. This is done by SND counting and registering how many packages were sent each day. On the other hand, the end devices keep a cumulative register of how many packages they received and send this figure uplink in the hourly heartbeat package. Because of this, it is possible to calculate the availability for each end device daily, with a month average or a location average.

The number of end devices with reliable communication was stable around 130 before the installation of the three new gateways, which started on May 16th. During the process it decreased a little due to the change in the configuration needed on the network. When the last new gateway was operational on June 4th, the system reached a new stable condition, with approximately 170

DINs online (Figure 9). It was also calculated that the average availability for this location before the gateways installation was around 77% and after that it improved to 91%.

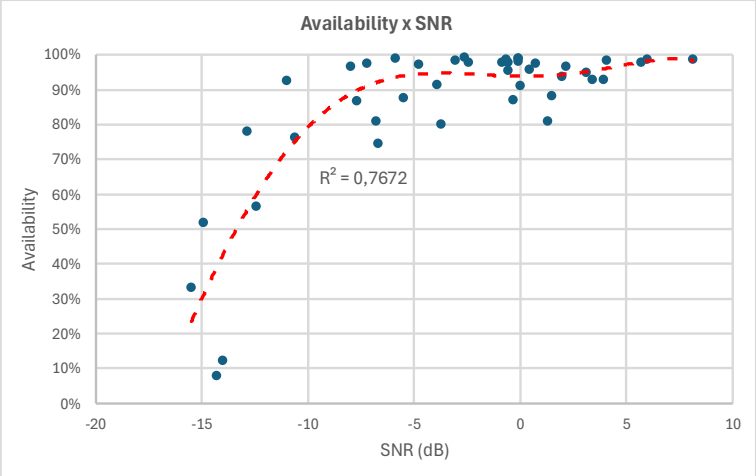
Figure 9. Number of DINs with reliable communication.



Source: Own elaboration, 2025.

The availability for each end device was also calculated, taking into consideration all the periods, as in before and after installation of the new gateways, to obtain data with weak and strong SNR values. This way, the result presented in Figure 10 was obtained.

Figure 10. Availability observed after coverage improvement.

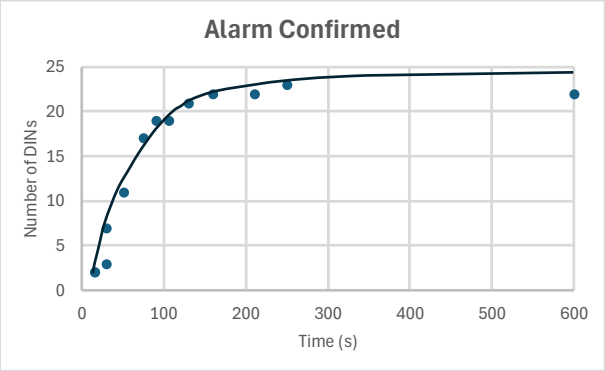


Source: Own elaboration, 2025.

3.2. Field results of the alarm

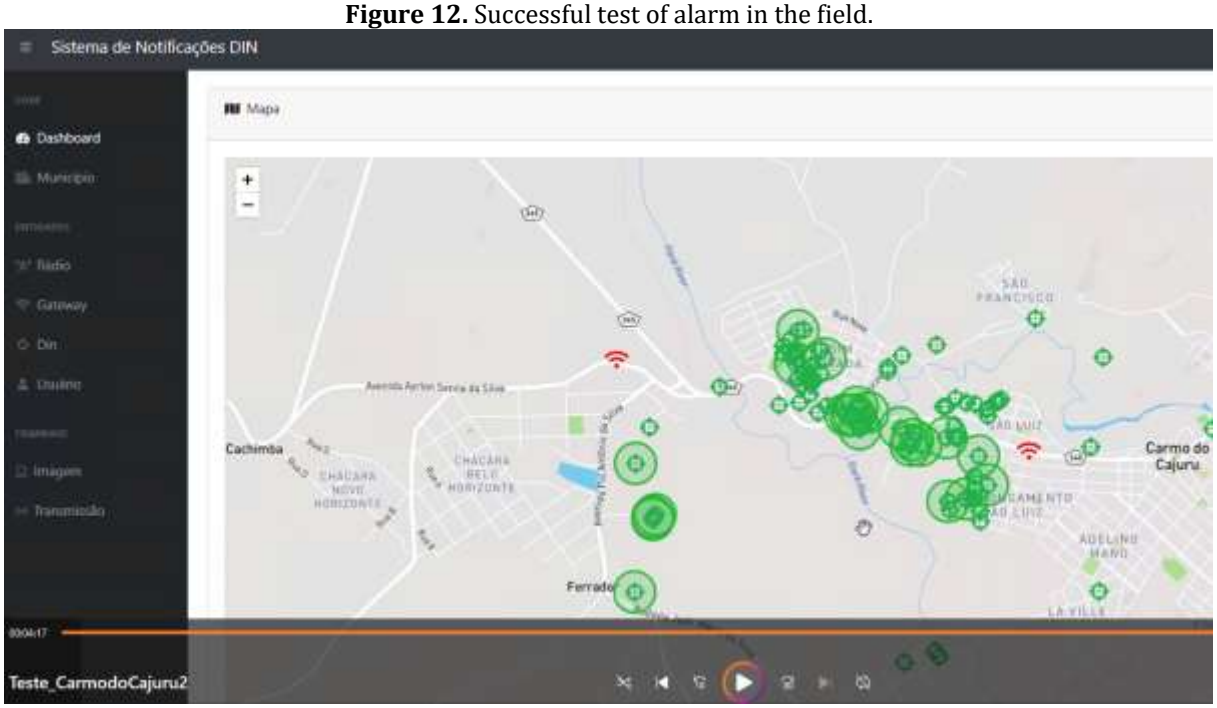
The location of the field test of the alarm is the same as the validation of the calibration of RF simulation, Carmo do Cajuru. As previously stated, its average availability with the new gateways installed is in the range of 91%, that is, a package loss of 9%. Under this condition, an alarm was sent to 23 selected end devices. This illustrates the feature that allows sending alarms only to the users that are affected by flooding, for example. Figure 11 shows the time evolution of the alarm receiving confirmation and Source: Own elaboration, 2025.
Figure *12* presents the print screen of alarm confirmation by all of them ealrier than 5 minutes.

Figure 11. Alarm confirmation evolution.



Source: Own elaboration, 2025.

Figure 12. Successful test of alarm in the field.

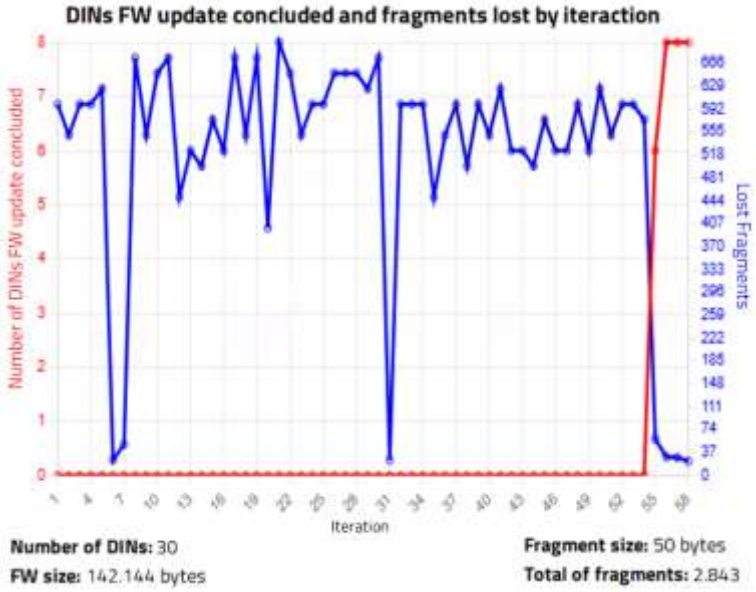


Source: Own elaboration, 2025.

3.3. Field results for FUOTA

The FUOTA field test was done in the same location as the previous field tests, however, in order to force the limits, it was done before the new gateways installation, when the average availability was around 77%, that is, the package loss ratio was in the order of 23%, slightly above the theoretical limit used in our dimensioning of the system. 30 of the end devices were used for the test. The result is presented in Figure 13.

Figure 13. FUOTA evolution for 23% of package loss in the field.



Source: Own elaboration, 2025.

The FUOTA process also counts the lost packages. Therefore, it was calculated for those specific 30 end devices, an average package loss ratio of 18%. Slightly different from the average of 23% in the location including all of its end devices.

4. Discussion

In Figure 8 was observed that the calibration fine-tuned the strength of the signal at the critical points and on that account, the signal generally improved in the other points, causing a increase in SNR average in the region were the new gateways were installed. This also led to an increase in availability from 77% to 91%, agreeing with the 95% configured in the simulation and validating the calibration process.

The result presented in Figure 10, is consistent with the previous work, of Figure 3 and the literature (Coutaud, Heusse, & Tourancheau, 2020). Figure 10 data points seem to be smoother than Figure 3 because the measurement was taken during a longer period, 35 days instead of 15, and with a bigger sample, 48 samples instead of 16. Anyway, the result is the same: above -15 dB of SNR the availability improves very sensibly. At Figure 10 it is slightly higher because it is related to downlink instead of uplink, which has a smaller sensitivity in LoRa. Due to the smaller noise in the measurement, is possible to observe in Figure 10 that above a value of SNR between -10 and -5 dB the average availability (red line) is approximately equal to 95%, just as parametrized on the RF simulator. This is certainly due to the calibration of the process. Furthermore, if above -10 dB practically all data points present above 80% of availability. This is an important parameter to measure the reliability of the protocols.

Figure 11 shows that in less than 180 s, or 3 minutes, 95% of the DINs have confirmed the alarm. Within 5 minutes all of them are confirmed, as presented in the print screen of Source: Own elaboration, 2025.

Figure *12*. The alarm itself might have reached the end devices long before that. This is the time that the acknowledgment takes to arrive. Since ACK is sent in 60 s windows, repeating up to 5 times to guarantee delivery, this explains why we observed this duration in the tests.

Figure 13 shows that it took a total of 60 iterations to finish the FUOTA process. This unexpectedly large number of iterations ocurred not only because of the large package loss ratio, but also due to the limited quantity of packages in the missing list of the end device, only 25. The end device could need as high as 600 fragments as shown in the figure, but can only ask for 25 at a time. Even so, the process was complete after almost 70 hours. Only in the fourth to last iteration,

6 end devices completed the firmware, and the remaining 8 completed in each of the last three ones, totaling 30 devices.

5. Conclusion

The main conclusion of this work is that any communication channel or technology is prone to package loss, and that the remedy for that is redundancy. This was demonstrated here through simulations, as well as tests in both the laboratory and in the field for small quantities of packages, as in the alarm case, and for massive amounts of them, as in the FUOTA case. If the system is slow enough to allow the time spent, then redundancy can be used. This is the case of the emergency system presented in this work. In case of flooding, it usually takes a couple of hours to deliver the alarm before the floodgates are opened. In case of dam collapse, the requirement is that the people must be warned up to 5 minutes after the alarm release. Because of all the lives at risk, reliability is paramount and the operator must have a reliable confirmation that it was successful.

The solution presented in this work can be used in any type of communication channel. For example, now that NB IoT is commercially available, it has been added to DIN and the alarm and FUOTA solutions were replicated with similar results. The advantage is that the packages are larger, being able to reach the standard ethernet size of 1500 bytes. NB IoT is a convenient option because it eliminates the need to install gateways. However, in a country with such a massive area, like Brazil, the dam region is usually in remote and mountainous areas, so it normally doesn't have commercial coverage.

The next steps consist of ending the validation of the NB IoT option for DIN, the development of an NB IoT sniffer to allow site surveys to verify the quality of signal in the candidate sites, and the improvement of some features. An example of that would be to improve the convergence of FUOTA, that was negatively impacted by the limit of 25 packets in the missing list when using LoRaWAN.

6. Acknowledgements

We'd like to thank André dos Santos for system tests and failure analysis, Camila Alcamim for RF design and field deployment of LoRaWAN gateways, Eugênio Daher for the project management, Evandro Aguiar for the firmware development, Fernando Silvestrow for the SND application development, Geraldo Caldas for hardware design, providing samples and making hardware tests and Samuel da Silva for system tests and field support. We also thank Aneel, which funded this work through its RDI program.

References

Agência Nacional de Águas e Saneamento Básico. (2024). *Relatório de segurança de barragens 2023*. https://www.snisb.gov.br/portal-snisb/api/file/download/714/4/rsb_2023_2024_06_27_11_01_28.pdf

Agência Nacional de Mineração. (2024, September). *Report mensal – Barragens de mineração*. https://www.gov.br/anm/pt-br/assuntos/barragens/boletim-de-barragens-de-mineracao/boletim-mensal-setembro-2024.pdf/view

ChirpStack. (2025). *Adaptive data-rate (ADR)*. https://www.chirpstack.io/docs/chirpstack/features/adaptive-data-rate.html

Choi, R., Lee, S., & Lee, S. (2020). Reliability improvement of LoRa with ARQ and relay node. *Symmetry, 12*(4), 552. https://doi.org/10.3390/sym12040552

Coutaud, U., Heusse, M., & Tourancheau, B. (2020). High reliability in LoRaWAN. In *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE. https://doi.org/10.1109/PIMRC48278.2020.9217220

Horta, A., & Damas, P. (2022). Design, tecnologia e segurança: Impactos da morfologia de um dispositivo individual de notificação sobre a percepção de usuários em zonas de risco de rompimento de barragens. *Revista Design & Tecnologia, 12*(24), 113-133. https://doi.org/10.23972/det2022iss24pp01-10

International Telecommunication Union. (2021). *Recommendation ITU-R P.1812-6: A path-specific propagation prediction method for point-to-area terrestrial services in the frequency range 30 MHz to 6 000 MHz*. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1812-6-202109-S!!PDF-E.pdf

Karthikeyan, R., Duraiarasu, E., Ganesh, K., & Bhagyalakshmi, L. (2024). LoRa and IoT based device for disaster and fleet management. *International Research Journal on Advanced Science Hub, 6*(5), 88–96. https://doi.org/10.47392/IRJASH.2024.016

Leitão, C. M., Strobel, F. de, Almeida, G. de, Mafra Júnior, J. J., Oliveira, J. J., & Xavier, R. C. (2022). *Solução AMI para áreas rurais dispersas e áreas urbanas com dificuldades de recepção de sinais utilizando tecnologia LoRa* [Conferência]. SENDI 2022 – Seminário Nacional de Distribuição de Energia Elétrica.

LoRa Alliance. (2017). *LoRaWAN™ regional parameters 1.1*. https://lora-alliance.org/wp-content/uploads/2020/11/lorawan-regional-parameters-v1.1ra.pdf

LoRa Alliance. (2022). *LoRaWAN fragmented data block transport specification TS004-2.0.0*. https://resources.lora-alliance.org/technical-specifications/ts004-2-0-0-fragmented-data-block-transport

Mafra, J. J., Jr., Hosami, M., Freitas, L., Martinelli, M., & Almeida, A. (2015). Hybrid communication module – Motivations, requirements, challenges and implementations. In *IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LA)* (pp. 25–29). IEEE. https://doi.org/10.1109/ISGT-LA.2015.7381124

Rayess, J., Khawam, K., Lahoud, S., Helou, M. E., & Martin, S. (2023). Study of LoRaWAN networks reliability. In *2023 6th Conference on Cloud and Internet of Things (CIoT)* (pp. 200–205). IEEE. https://doi.org/10.1109/CIoT57267.2023.10084880

Sciullo, L., Trotta, A., & Di Felice, M. (2020). Design and performance evaluation of a LoRa-based mobile emergency management system (LOCATE). *Ad Hoc Networks, 96*, 101993. https://doi.org/10.1016/j.adhoc.2019.101993

Silva, J. de C., Rodrigues, J. J. P. C., Alberti, A. M., Šolić, P., & Aquino, A. L. L. (2017). *LoRaWAN – A low power WAN protocol for Internet of Things: A review and opportunities* [Conferência]. 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, Croatia.

Sisinni, E., Carvalho, D. F., Ferrari, P., Flammini, A., & Gidlund, M. (2022). Adding redundancy to LoRaWAN for emergency communications at the factory floor. *IEEE Transactions on Industrial Informatics, 18*(10), 7332–7340. https://doi.org/10.1109/TII.2021.3124054

The European Parliament and the Council of the European Union. (2024). Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union, L series*. http://data.europa.eu/eli/reg/2024/2847/oj

Zhang, H., Zhang, R., & Sun, J. (2025). Developing real-time IoT-based public safety alert and emergency response systems. *Scientific Reports, 15*, 13465. https://doi.org/10.1038/s41598-025-13465-7