15

Remote Monitoring for Safety of Workers in Industrial Plants: Learned Lessons Beyond Technical Issues

Jose María Cabero Lopez

TECNALIA RESEARCH & INNOVATION, DERIO, SPAIN

1 Motivation

All tasks in a refinery can be classified in two main groups:

- Turnarounds for maintenance activities. They are characterized mainly by the high quantity of external workers from different contractors collaborating together to carry out the maintenance tasks as soon as possible. Maintenance activities comprise piecework tasks all along the refinery, from which a high percentage is inside confined spaces. A typical turnaround comprises more than 1500 workers from many contractors (normally more than 50), working 24/7 during and average period around two months.
- Daily tasks, comprising operational and maintenance activities. These tasks do not include activities inside confined spaces, which are close during regular season.

The former ones are especially risky because they require staff who is not used to specific company safety policies, in addition to exhaustive long shifts piecework. In 2015, we were contacted by a prestigious refinery worried about workers' safety during turnarounds. Half a year later they had planned a turnaround and they desired to check new technologies to let them increase workers' safety inside confined spaces and their localization all over the plant. Refinery's requirements focused mainly on remote monitoring, long autonomy and possibility of interaction between workers and supervisors to communicate aid-demanding situations (from workers to supervisors) and evacuation situations (from supervisors to workers).

Our design to satisfy their needs became a remote monitoring system for the safety of workers in industrial plants. A brief description of the system is described in Section 2.

In addition to technical performance, such a system must consider a plethora of issues related to sociological and logistic aspects difficult to estimate a priori, such as privacy and

Geographical and Fingerprinting Data for Positioning and Navigation Systems. https://doi.org/10.1016/B978-0-12-813189-3.00015-0

system maintenance. Thus, in order to consider these collateral but very important issues, the system development has evolved in parallel to several turnarounds (one per year since 2015), which has allowed us to understand real needs and facts that otherwise would have been missed. This chapter describes briefly the remote monitoring system and the lessons learned in three turnarounds so far.

2 Remote Monitoring System for Safety of Workers in Refineries

The remote monitoring system has been designed in the form of an open platform to monitor the location of workers in a refinery, both inside and outside confined spaces, and any emergency situation that may require external help, such as accidents and fainting situations.

2.1 The Architecture

This system is based on a three-level architecture consisting of: wearable devices, a fixed communication infrastructure deployed all over the monitored site and a control center in the Cloud. Next, the main functionalities of every part are explained.

2.1.1 Wearable Devices: The Wristband

The monitoring system is based on a set of wearable devices to capture information related to people that wear them. So far, the wearable device used in refineries is a customized antiexplosive wristband that provides two main functionalities: localization of workers and detection of aid-demanding situations, with the following approaches:

a. Localization at two levels:
   i. Presence information: through the usage of a NFC tag that is used to record the exit and entry of the corresponding worker in a confined space.
   ii. Localization information: the wristband provides periodical communications which are used by the control center to estimate their localization in the refinery. These communications are based on Bluetooth Low Energy (BLE) for proximity-based localization (based on received signal strength) and UltraWideBand (UWB) for accurate localization (based on time of flight of the received radio signal). The control center runs a localization engine that is able to determine their position based on this periodical information.

b. The wristband includes two mechanisms to detect aid-demanding situations:
   - No motion: a reactive mechanism, based on an automatic motion detection algorithm that uses the information collected by a built-in accelerometer.
   - Panic button: a proactive mechanism, based on a built-in alarm button that must be pressed by the worker in case of need.

c. Additionally the wristband has a led and vibrator to interact with the worker.

The wristband is battery operated and it has an autonomy of more than one year. It can operate in explosive environments, which is critical in refineries (antiexplosive (ATEX) certified). Next figure shows a detail of the wristband.

The aim of the system is to monitor people rather than devices; so it is important to detect those situations where the device is not with the person. The system considers three possibilities: wristband forgotten in the plant, outside the plant, or broken. Based on wristbands activity and mobility, these situations are automatically detected and reported to the control center in the form of an alert that will be sent to the supervisors of the refinery.

With respect to the flexibility of the system, the monitoring platform is designed to allow the connection of any commercial wearable devices or sensors with WiFi or Bluetooth Low energy communication capabilities. This is possible through the capabilities of the communication infrastructure explained next.

2.1.2 Communication Infrastructure

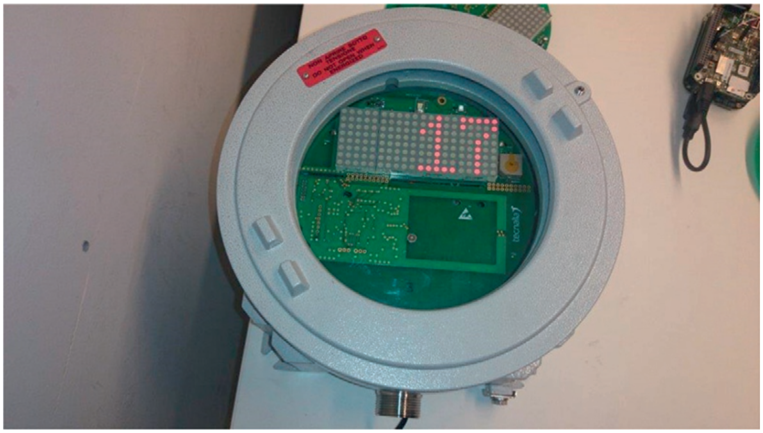
The monitoring platform is based on a wireless communication infrastructure that is deployed all over the zone of interest. This infrastructure consists of a set of nodes called anchors that act as communication bridges between wearable devices and the control center in the Cloud. This communication is bidirectional, to collect data from wearable devices (upstream), and also to carry out remote configuration tasks in anchors and wearable devices (downstream).

An anchor consists of the following modules:

- **Communication module:** the anchor is designed to be highly flexible and reliable in terms of robustness. From the communication perspective, this means the possibility to deploy the communication structure in any type of environment, with and without previous communication infrastructure in the specific site. The anchor consists of WiFi and 3G for direct connection between anchors and the control center in the Internet. Both wireless interfaces switch according to the dynamic conditions of the site, that is, if WiFi access points were available in the deployment site, every anchor could connect directly to this WiFi infrastructure to reach the control center. If WiFi infrastructure failed, every anchor would switch automatically to communicate through 3G network. The approach would be similar in case of 3G network as primary network and WiFi as back-up resource.

- **Visualization module:** it consists of a set of alphanumeric displays to show relevant information at the place where they are deployed. It consists also of a buzzer that beeps to alert the workers around of specific events that require attention.
- **Localization module:** it consists of a NFC reader for detection of workers in confined spaces, and two wireless communication modules for the communication with wearable devices in the surroundings. These modules are BLE for proximity-based localization (based on received signal strength) and UWB for accurate localization (based on time of flight of the received radio signal).

Whereas wearables are designed to be intrinsically safe from the ATEX perspective, in the case of anchors, the electronic design is being encapsulated inside ATEX metallic enclosures. Next figure shows an anchor with an antideflagration ATEX enclosure.



2.1.3 Control Center

It stores and processes the collected data coming from the communication infrastructure in the refinery. It shows permanently the current status of the refinery (localization of workers, active alarms…). Additionally it alerts the supervisors of any aid-demanding situation.

The control center is designed to deal with thousands of simultaneous connections. Additionally, it is completely backed-up to assure continuous service in case of failure. The control center runs in the Cloud, being physically located in different machines, also located in different countries, which assures an effective load balancing process in case of need. On the other hand, its location in the Cloud provides as many resources as necessary in case of exponential growth of system deployments.

The control center consists of the following modules: the database, the processing module, the remote configuration manager, the alert manager, and the graphical user interface, which are explained next:

- **The database:** it stores collected data coming from anchors in the site. Currently this information comes originally from wristbands, but it could come from any sensor connected to the anchor infrastructure through WiFi or Bluetooth Low Energy, or even any other sensor connected to the Internet (through 3G for instance).
- **The processing module:** it runs algorithms to transform raw data into high level information. The most important part of this module is the localization engine, which, based on the incoming information from the wristbands, provides their localization in the area of interest.
- **The remote configuration manager.** This is the part of the system that controls, configures, and updates remotely the infrastructure of anchors and wristbands in the field.
- **The alert manager:** this module receives and generates all alerts in the platform. There are two types of alerts: those generated by the wearable devices to inform supervisors, and those generated from the control center to inform workers.

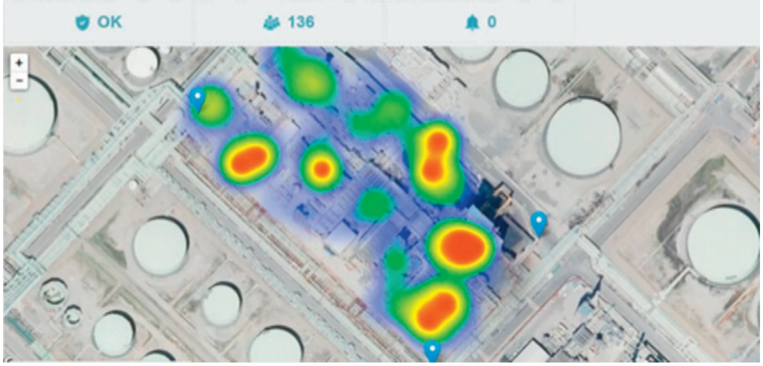
  When alerts come from workers, this module informs supervisors of the type of alert, where it is coming from, when it happened, and who has generated it.

  So far, there is only one alert that is sent from the control center to the workers, which is an evacuation alert. This situation is broadcasted by the system toward all anchors (it generates a loud and continuous beep from every anchor) and wristbands, making these vibrate.
- **The graphical user interface:** this module shows collected information to end users. It consists of maps of the monitored site, heating maps of activity to show density of workers per area, active alerts, statistics of activity, etc. Next figure shows a specific moment of the activity in a zone of the refinery during the last turnaround, with 136 workers and without active alerts.

2.2 Data Anonymity

Our system collects data from wearable devices, so, linking wearable device ID's and its owner is necessary in most cases if the system must translate between devices and people. Knowing which person wears a specific wearable device offers personalized functionalities that optimize system response to every situation, such as granting or denying access to zones depending on workers' profiles.

The system allows three different strategies from data anonymity point of view:



- Complete anonymity: there is no information related to wearable devices and workers. Any rule applies to everyone without exception, for example, access to a zone is granted or denied to everyone no matter who is trying to access.
- Medium anonymity: the system knows who is wearing what device, system user interface does not show any personal identification (name, surname); anyone who is watching the user interface can check only wearable devices identifications (IDs), but system administrator can know who is wearing every device. Rules can be personalized without showing who is whom in the user interface. In the end, if it were necessary, any infraction could be tracked down to the specific worker.
- Low anonymity: the user ID (name, surname, and contractor) is shown in the user interface. This profile implies full availability about personal data to any user watching the system user interface. Full functionality of the system can be applied (personalization).

There are three critical reflections to be done before choosing the level of anonymity. The output of these reflections will determine the success of failure of the system:

- What the regulation says about personal data management: it depends tremendously on the country and region where the system will be deployed, and there is not much to do either technically or socially, but to choose the right level of anonymity.
- What the system is applied for: although the system is originally thought for safety, the system could also be used to monitor people for other purposes: productivity and control. The former aims at an increase of productivity by analyzing data as a whole, without considering specific IDs of the monitored people. The later aims at analyzing who is doing what and where.
- Who monitors information: information can be at disposal of the owner of the plant (all staff or just a set of people), or be extensible for all stakeholders: owner, contractors, and even workers.

3 Learned Lessons in the Field

The system has been developed and is being validated in different turnarounds. Beyond technical evolutions of the system to cope with specific harsh environments in refineries, there are a set of crucial nontechnical aspects that can be extrapolated to other industrial sectors, that are key for the success of these type of services based on monitoring people with wearable devices. Since the first version of the system in 2015, two nontechnical aspects have been our system main threats: person related aspects and logistics. These aspects and potential solutions are explained next.

3.1 Person Related Issues

In the end, workers, as entities to be observed, are key in the success or failure of any monitoring service. They must be convinced about the goodness of the service for their own safety or, at least, be convinced about the system not being a threat. Based on our experience, some aspects are cornerstone to get workers' acceptance:

- *Transparency and privacy:* workers need to understand what the system is used for; it should be a tool open to them; they should be able to watch it running. The objective should be even to have the system operated by them or someone they trust in. In addition, the plant owner should establish a policy to assure and show them that their data are not used for controlling purposes.

  Originally, all industrial deployments had demanded remote monitoring services for safety purposes, although lately, along with the Industry 4.0 movement, more and more industry is demanding remote monitoring services for productivity purposes. So far, all companies have understood that the usage of the system to control workers would make the system fail (be rejected by workers). Our experience shows this aspect as the biggest problem for the system acceptance by workers. The system cannot be considered by workers as a control tool, otherwise it would be condemned to fail.

  Our experience with managers in industrial plants took us to discuss about this aspect many times, sometimes joking, less times seriously, but in the end everyone understood that controlling is out of scope, and the system objective must be only safety and productivity.

  So far, we have deployed the system in industrial plants by applying the medium anonymity approach focused on safety purposes. This way, the system knows who is wearing a wearable device that is being monitored, but the user interface does not show that information to supervisors. Workers are usually shown as numbers (e.g., Worker1, Worker2, etc.).

  Originally, the remote monitoring service was designed to be used by the industrial plan owner. In our experience in industrial plants, many contractors demanded access to its user interface claiming that, this way, any emergency alert related to their workers would be quickly attended by them. This request, combined with privacy-related issues, made us consider the remote system as an open service for all stakeholders in the plant, providing access to the user interface to contractors and workers, being transparent for workers (to disassemble suspicions about privacy) and providing a monitoring tool for contractors as well. Next lines show some of the lessons learnt according to different aspects.

– Ergonomics: wearable devices must be transparent or at least comfortable for them. The remote system is based on a wristband as wearable device for workers. Some complaints have been received about the wristband not being comfortable enough for some tasks, and even seen some workers taking the wristband somewhere else (in their pocket for instance).

  In addition, even for comfortable wearable devices, including a new device to the ones they already wear may not be a good option. Industrial sites where the wristband has been used, clients from now on, are reluctant to include new equipment because of the implicit complexity for workers, and they prefer to expand the functionalities of the existing ones, if it is possible, being totally transparent for workers. To this respect, the concept of smart clothes seems to be the best option for future evolutions of the system.

– Simplicity: ideally, system usage should not require workers actuation. They should keep oblivious to the monitoring system. They already have plenty of procedures to comply with; new ones should be avoided. Our system requires very few instructions for workers: basically panic button usage and confined spaces in/out. Although it is hard to quantify, in the last turnaround supervisors detected many confined spaces in/out protocol infractions, mostly for two reasons: they did not remember the procedure or they did not understand what the system was for. The technical roadmap of the system considers the design of an automatic mechanism to detect confined spaces in/out.

– Technical and procedure robustness: any system deployed in an industrial environment must be adapted to a harsh context. Additionally, in a turnaround, service must be assured without interruptions. If any link of the chain fails, the credibility of the whole system will be put at risk. On the other hand, all relevant procedures, such as installation of the system, maintenance and monitoring must be very clear for all the stakeholders participating in the service. Otherwise, even when the system is technically robust, the service will fail.

  Along the system development, in previous turnarounds, the monitoring system suffered from system technical failures, such as servers down, broken wristbands, partial blackouts, and failures in the procedures, such as problems with logistics and supervisors who did not know the system procedures. The price to pay is that as soon as the system started failing, workers had a good excuse for stop using wristbands.

  After these initiatives and to avoid these problems, it has been decided that any new installation include two initial activities:

  - Intensive training on system functionalities for client supervisors, and integration of the system functionalities on client’s safety procedures.

- Incremental installation of the system: start by a pilot to check client's requirements and validate all relevant procedures, and afterward make the system scalable to the whole plant.

An example of the necessity of clear instructions and procedures for those who must run the system is shown in the next subsection.

3.2 Logistics

A remote monitoring system based on wearable devices requires a thorough process of device assignment, replacement and, in case of uninstallation, collection of equipment. When the service is deployed in a turnaround, with plenty of workers performing piecework tasks, the system must be up and running quick and transparently for workers' daily activities. One very important part of the installation is the assignment, distribution, maintenance, and collection of wearable devices. This task is critical, and usually underestimated, which can end up in a completely unreliable system.

In a turnaround, most workers participate partially, that is, they fulfill their task, that usually take them several days, and leave to other turnarounds. It is normal for the plant owner to require less wearable devices than workers and reuse them as they come and go. A critical part for the system performance is the distribution, assignment, maintenance, and especially the reassignment of wearable devices.

For these phases it is crucial to have a clear process about how to act and, if possible, just one person and company in charge. This process is especially needed with the scalability of equipment. Our experience in this matter was especially painful in a turnaround with 700 wearable devices; the assignment/reassignment of wearable devices in the control center was carried out by the client, and their distribution to the corresponding workers by a contractor.

After four weeks of turnaround, the client realized that they were watching on the plant map of the user interface, workers who had already left. How was this possible? At the beginning, both assignment and distribution of wristbands were synchronized; after some days and many new workers, the big mistake arose: the contractor had redistributed wearable devices used by workers who had already left to new workers without informing the client, that is, without reassigning the wearable devices to the new workers.

Both client and contractor declare afterward that they did not have clear how the assignment/distribution process worked, which was our very big mistake: be confident about something we considered clear enough and technically easy. We underestimated the necessity of a procedure for these tasks.

4 Conclusions

Monitoring the activity of workers in a refinery can be done with localization techniques and communication technologies. Beyond technical issues, this chapter summarizes our experiences in turnarounds in refineries; it focuses on two aspects that are critical from our point of view: person-related issues and logistics.

Beyond specific technical features, privacy, simplicity, ergonomics, transparency, training, and integration with client safety procedures are presented as factors for the success of any service for human monitoring. Some tips and approaches to these aspects are described based on our experience.