

Research Article

Development and Implementation of an RFID-Based Tunnel Access Monitoring System

**Kai Kordelin,¹ Jaana Kordelin,¹ Markku Johansson,² Johanna Virkki,¹
Leena Ukkonen,¹ and Lauri Sydänheimo¹**

¹*Department of Electronics and Communications Engineering, Tampere University of Technology, P.O. Box 692,
33101 Tampere, Finland*

²*Elcoplast Oy, Tykkitie 1, 36240 Kangasala, Finland*

Correspondence should be addressed to Kai Kordelin; kai@kordelin.eu

Received 8 June 2016; Revised 19 August 2016; Accepted 23 August 2016

Academic Editor: Eugenijus Ušpuras

Copyright © 2016 Kai Kordelin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Due to safety reasons, the exact number and location of people working in an underground tunnel need to be known all the time. This work introduces the development and implementation of an RFID-based access monitoring system for the ONKALO nuclear waste storage facility. This system was taken into use in 2010 and was systematically monitored for one year. The system principle and the used equipment are presented in this paper together with the reliability evaluation results of the implemented system. According to the field use evaluation of the ready system, the reading reliability at the end of the monitoring period was 100%. In addition, even after the successful monitoring period, the system has been updated and new features for safety improvement have been created based on fire department guidelines and achieved user experience. In the future, the RFID system has been planned to be used also in the final depositing of the used nuclear fuel and buffer materials.

1. Introduction

The growing demand for safety in workplaces around the world has resulted in tighter regulations and continuous development of safety systems. Keeping track of people and equipment for safety and security is one of the most important aspects.

The spent nuclear fuel accumulated from the Finnish nuclear power plants in Olkiluoto, Eurajoki, and in Hättholmen, Loviisa, will be disposed in Olkiluoto. A complex with two nuclear waste facilities will be constructed in Olkiluoto [1]. Posiva is an expert organization responsible for the final disposal of the spent nuclear fuel. Posiva started to construct ONKALO tunnel system in 2004. The purpose of ONKALO is to ensure that the bed rock in Olkiluoto is suitable for the final storage of the used nuclear fuel. Versatile research has been conducted there since the beginning of its construction. The nuclear waste facilities consist of an encapsulation plant, constructed to encapsulate the spent

nuclear fuel, a disposal facility, consisting of an underground repository and other underground rooms, and the above ground service spaces. Access routes to the disposal facility are an inclined access tunnel and vertical shafts. As underground tunnels are usually structurally nonuniform, with a network of interconnected tunnels, crosscuts, shafts, escape ways, first-aid stations, alcoves, and tunnel blockages [2], monitoring the access to the tunnel plays a critical part in the work safety [2]. In the deposition area of ONKALO, two parallel central tunnels connect all the deposition tunnels and these central tunnels are interconnected at regular intervals [1].

The original access monitoring system in ONKALO was manual, and it was based on hooks (see Figure 1). All staff members had their own hook on the wall and the washer was put on the hook when going into the tunnel. Entering ONKALO and moving inside the area happen always by a vehicle. The main reason why the old manual access monitoring system needed to be upgraded to an electronic

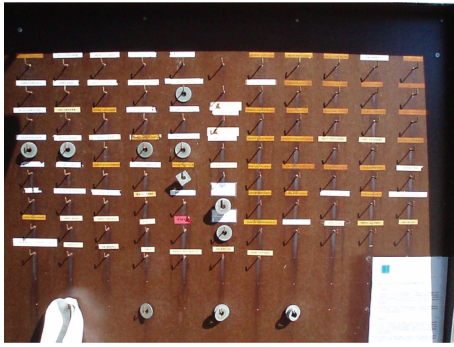


FIGURE 1: The old manual access monitoring system.

monitoring system was to reliably identify the vehicle and also the people inside. In emergency situations, underground personnel and equipment identification and localization are critical [3].

RFID (Radio Frequency Identification) is a wireless identification technology that provides efficient solutions for identification, warehousing, and logistics and also for reliable and easy access monitoring [4–6]. For further information on the RFID technology, [7, 8] are presenting very early investigations. A comprehensive survey of the RFID technology's history is presented in [9, 10] and a comprehensive introduction to today's systems and standardization is provided in [11–14].

In this paper, the new RFID-based access monitoring system developed for ONKALO is presented. The basis of the development of the new access monitoring system has been to improve occupational and company safety. This work describes the ONKALO access monitoring system and its features during normal day to day use. The system functionality will first be introduced together with the used equipment. Next, the application logic program is presented with its web interface. Then, a field use evaluation of the system will be done and the reading reliability will be discussed. Finally, further improvements after the monitoring period are presented together with future plans.

2. Access Monitoring System

The system functionality will now be introduced together with the used equipment. There are seven information reading points: five reading points have one reader and an antenna and two points have two readers and two antennas. In addition, there is one screen for information and almost 500 identification cards programmed into the system. See Figure 2 for the reading points in ONKALO.

The used application logic, presented in Figure 3, is Windows (SQL Server Express) that does not have its own user interface. The programs settings are loaded from a configuration file once the service starts. The application logic executes the required operations demanded by the application and stores this data into the database. The area and registry information can be viewed with a separate web application by searching the data from the database.

2.1. System Operation Principle. There are two different information reading areas at ONKALO (see Figure 2). One reading area consists of reading points that give information from both directions of traffic. The first reading area is at the entry of ONKALO. It monitors the traffic going in and out of ONKALO. This reading area has four reading points. The second reading area, with two reading points, is located at the “dead end” and it controls the traffic going in and out of that area.

In addition to the given reading areas, there are additional three reading points. One is located in the demonstration area (the area of ONKALO where all the tunnels are excavated for prototype testing) and another at the technical level. The third reading point is at the beginning of the drive ramp before the entrance to ONKALO. This is called the forced out-reading point. Its only purpose is to read all vehicles and people that leave ONKALO.

In practice the system works so that when a vehicle, as well as people inside it, comes to a reading point area, the reader identifies the ID-numbers of the vehicle and the people and records them to the system database. After the reading process, the system sets a time limit when other reading points cannot record these IDs to the database. The purpose of this time limit is that the system cannot record the ID as going to the wrong direction. The forced out-reading point is an exception to this rule, as it does not take notice to the time limit set by the system and always records all tags it reads out.

2.2. The Process of Identification. The process of identification is the same at ONKALOs both reading areas and all reading points. The identified vehicle and the people inside move through the identification area and the database receives information of the vehicle and the people (going in/going out and level). The reading occurrence is represented in a flowchart in Figure 4.

2.3. Initializing the System. The testing phase of the ONKALO electronic access monitoring system started in January 2010. At this time, the in-reading and out-reading points were commissioned. During the test phase, 20 identification cards were added to the system.

Before the system initialization, all staff members who received an identification card got training for the system. In the organized training, the purpose of this system, the operation principle, and the system limitations were explained. During training, it was emphasized that this system is not an actual work time related monitoring system, linked with work hour time stamps, but rather all access monitoring is done for work safety reasons.

The system was taken into full use in May 2010. After this, the access monitoring system has been systematically further developed and the development has concentrated on reading accuracy improvement. The locations of the readers have been improved and the personnel instructions have been clarified. In addition, more equipment and readers have been taken into use. An important part of the system development process has been to study the possibilities of RFID technology and further development possibilities.

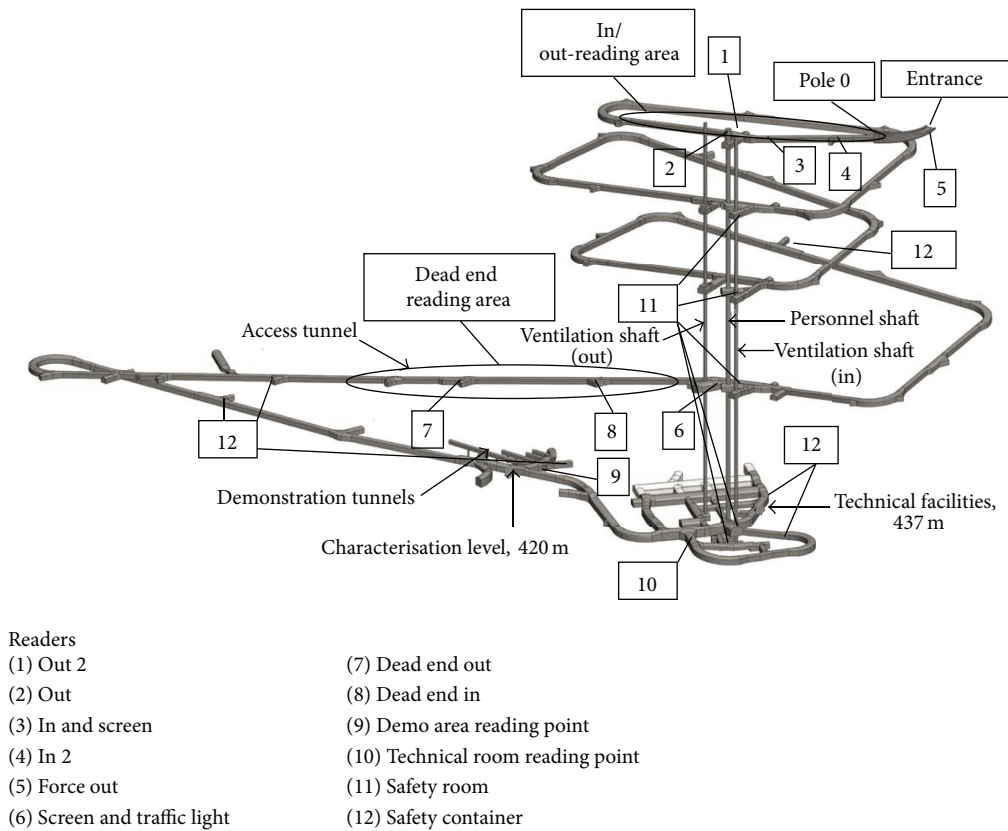


FIGURE 2: The reading points and reading areas in ONKALO.

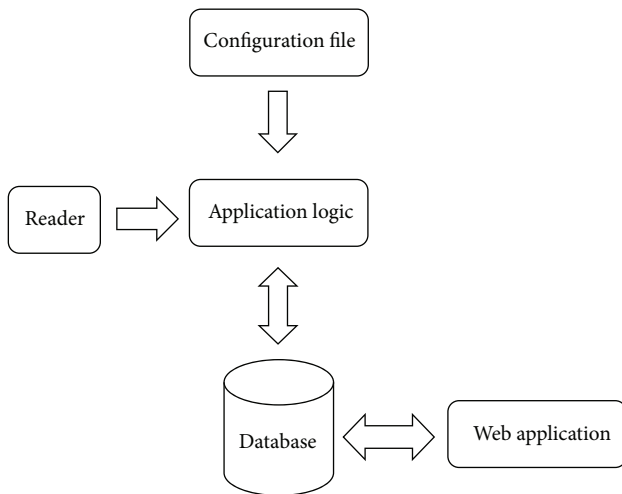


FIGURE 3: The system description.

3. System Equipment

As mentioned previously, ONKALO has two reading areas and three other reading points (shown in Figure 2), and both reading areas consist of two or more readers. The first reading area is the area between poles 0 and 180 (distance in meters

from ONKALO entrance). The other reading area is between poles 3050 and 3300 (dead end).

3.1. Readers. With the demonstration area reader, it is monitored that no unauthorized personnel can enter when prototype testing is undergoing. The purpose of the reader in the technical levels is to verify personnel locations in the ONKALO tunnel. The forced out-reading point is located at the ramp upper end, leading to the ONKALO entrance, and it is equipped with a multidirectional antenna. The reader is only for reading outgoing traffic and the sole purpose of this reader is to check out personnel that are near the entrance and have been signed inside. In Figure 5, an example of an ONKALO reading point and related equipment is presented.

Initially all readers were interlinked by WLAN (Wireless Local Area Network) to the application logics. The components of the reader are installed in a Fibox EK164H-6-casing (shown in Figure 6). The casing has a Fibox EKIV64H installation plate where components can be attached. The reader is Wavetrend RX1000 and gets its operational voltage from a Mascot 9061 12 V/7,5 V inverter. The readers' operational voltage is 7.5 V. In case of a power outage the casing has a Satel APS-15 12 V/1,5 A DC-UPS that contains a 12 V/7 A lead battery. In addition, the casing has a Stego CSF060 heater. The maximum power of the heater is 50 W and a fixed 15-degree thermostat has been installed to it. A 230 VAC feeder

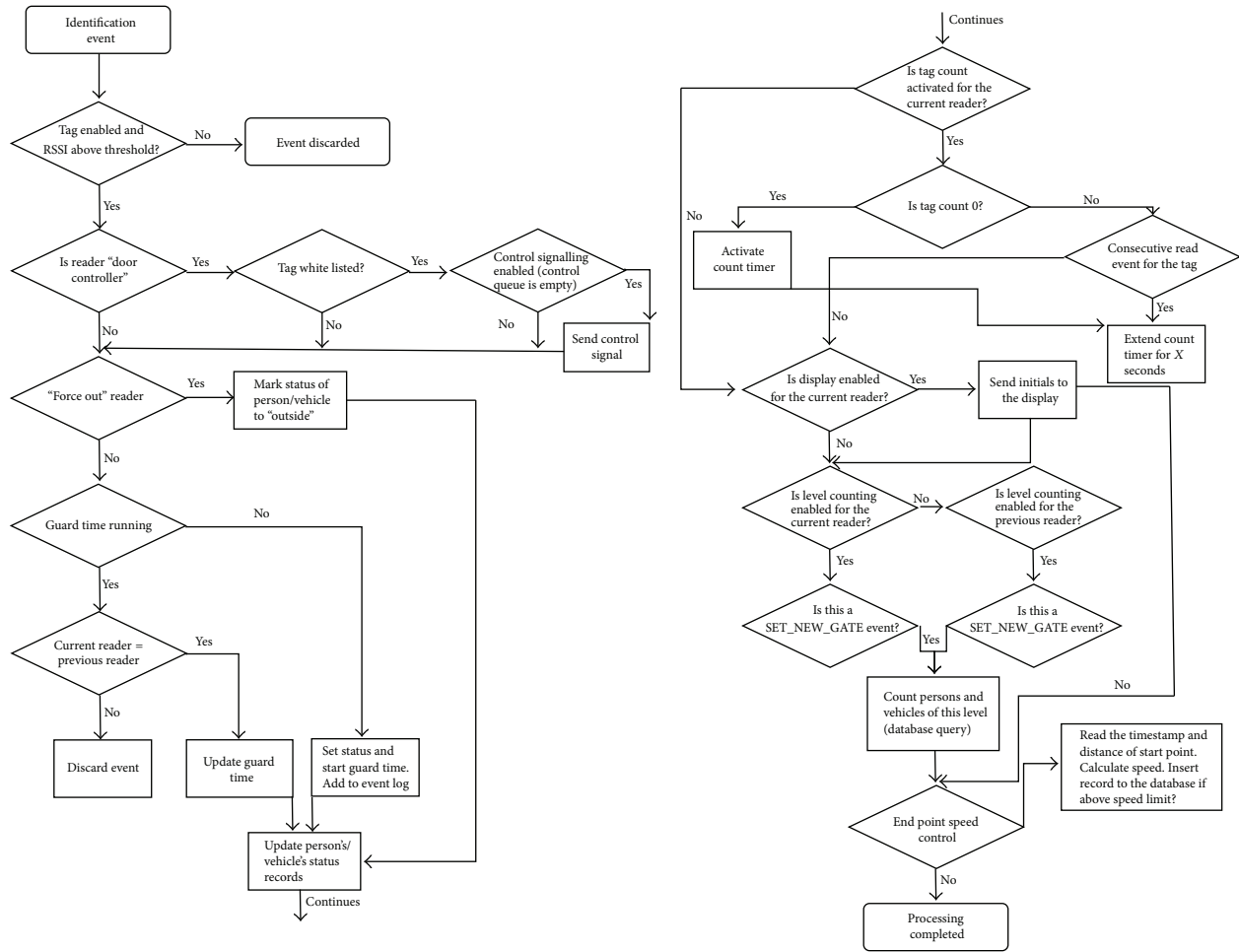


FIGURE 4: The reading occurrence.

voltage is brought through a PG11 inlet to the cable protection automat that is in the casing.

Traffic between the reader and the application logics is done by TCP/IP and UDP protocol. The readers have a buffer memory for the ten last reading instances. If a power outage occurs, the buffer memory will provide this data to the database.

Currently all readers, except two, are LAN-readers (Local Area Network) that are connected via cable to the program logics. The reader is a WaveTrendin LRX 201 RFID reader that is connected to the system with an integrated computer (see Figure 7). The operating voltage of the integrated computer is 12 V, so there is no need for a converter after the DC-UPS.

The WLAN and LAN-reader parts are interchangeable, except for the reader itself and integrated computer. This enables the possibility of having replacement parts for ONKALO's entrance readers, even though actual spare parts are not available for these units. Spare parts can be borrowed from the technical level reader, for example.

Further, the newer LAN-reader types, in the demo area and technical room, have an expansion circuit board connected to the integrated computer: 1 * opto-isolated input, 1 * relay output, and state information LEDs (state of data

transfer and IO) (shown in Figure 8). The readers' setting files are on the integrated computers SD card. This enables the possibility of replacing a damaged unit with a new one by swapping the SD card. These new readers do not need to be configured separately. In the future, all readers will be replaced with this type of reader.

3.2. Antennas. A directional antenna (shown in Figure 9) supplied by Elcoplast Oy is used because it is the only possibility for gathering directional information in the challenging ONKALO conditions, where the humidity level changes and also mud, together with dust, causes major reliability challenges. The reading area of the directional antenna is a bit elliptical: in the vertical direction, the reading area is 120 degrees and horizontally 80 degrees. The antenna operates in a frequency range of 433–435 Mhz. The operational temperature is from -30°C up to $+85^{\circ}\text{C}$. The antennas protection class is IP65 [15]. The distance between the antenna and the reader is determined by the length of the antenna cable, which should not exceed ten meters. At the forced out-reading point, an omnidirectional antenna is used (see Figure 9). This reading point is only for reading outbound traffic so no directional information is required from the antenna.



FIGURE 5: An ONKALO reading point and display screen.

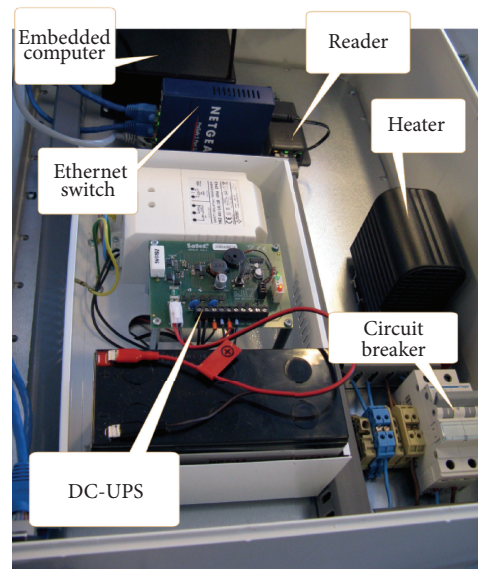


FIGURE 7: A LAN-reader with integrated computer.

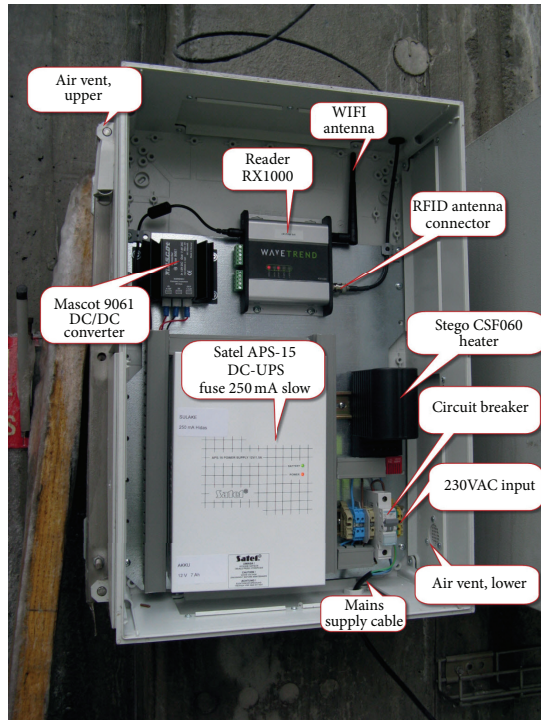


FIGURE 6: A WLAN-reader.

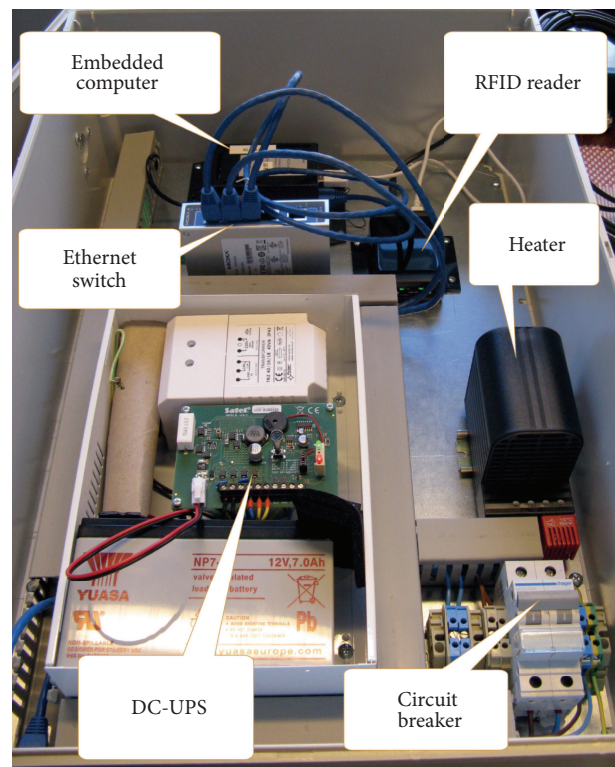


FIGURE 8: A new type of LAN-reader with SD card and integrated computer.

3.3. *Screens.* There are two information screens: one is located next to the ONKALO entrance inbound reader and the other one at the dead end.

The first information screen shows all read identifications. From this, the driver of the vehicle can verify that the vehicles and all people have been identified in order to enter the ONKALO tunnel (Figure 10). The information screen is a LED point matrix type meant for outdoor conditions. Power usage is 450 W. The information screen is directly connected by a LAN cable to the information network and has been

programmed into the program logic. The resolution is ($W \times H$) 64×64 pixels. The LED screen size is 960×960 mm. The screen outer dimensions are $1110 \text{ mm} \times 1150 \text{ mm}$.

The second screen (Figure 10) was used to tell how many people were located at the dead end, which was extremely important for safety reasons, as the safety areas located there were supplied only for 24 people. The traffic light (shown

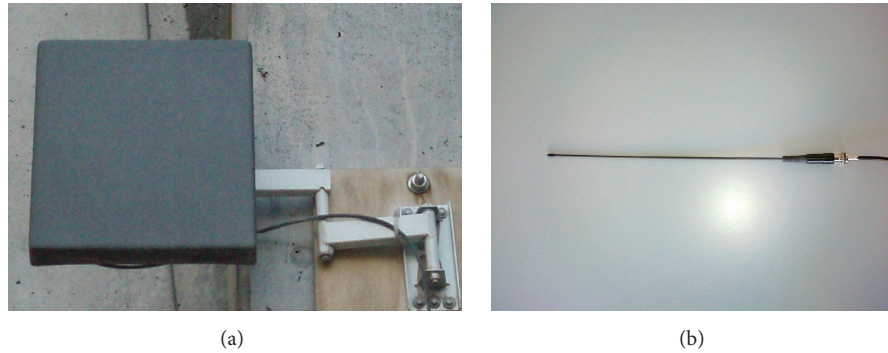


FIGURE 9: A directional antenna (a) and an omnidirectional antenna (b).



FIGURE 10: The information screen at the entrance of ONKALO (a) and the dead end information screen and traffic light (b).

in Figure 10) was connected to the system in a way that it turned yellow when amount of people at the dead end was 17. When the yellow light was on, only personnel whose work required it were able to enter. Once the amount of people was 20, the red light went on. The red light went on already after 20 people, because the reader was located after the traffic light and information screen, and there was the possibility that people were in between the light and the reader. At the moment, ONKALO no longer has a dead end with no additional passage, so these functions are no longer in use.

The information screen is ALGE-TIMING manufactured, model D-LINE150-1-4-E0 information screen. The screen has room for four 150 mm high numbers. The information screen height is 250 mm, width is 730 mm, and depth is 60 mm. The required power is 10 W and it can use 100 to 250 V voltage and 50 to 60 HZ frequency.

The components required for the data transfer between the information screens and the application logic are located in their own casing (presented in Figure 11). The casing has a MOXA NPort W 2150 plus WLAN/Ethernet RS232-converter, MURR Elektron DC-power source, and two 3 A fuses before the power source. The operation of the traffic light is done by a programmable logic. The casing for the logics is the same size as the casing for the readers. The casing also has the same DC-UPS device and Stego heater. The logics unit is a MOXA E 2210 logics controller that is connected

to the information network with a MOXA EDS 205 network switch.

3.4. Identification Cards. The Wavetrend active identifier is used as the identification card. The identification card is 85 mm long, 55 mm wide, and 5 mm thick sealed plastic casing that contains the identifier, an antenna, and a power source. Each identification card (shown in Figure 12) is supplied with a unique ID number that the system detects. The identifier sends its own ID number on a frequency of 434 Mhz. All people and all vehicles have their own identifier.

4. Application Logic Program and Web Interface

The ONKALO tunnel system and the readers integrated there are part of the nuclear plant. Due to the information security of a power plant, the ONKALO access monitoring system works in its own closed local area network and is not accessible remotely. The server for the access monitoring system is located in a controlled server room, which is the only place where the database can be accessed.

4.1. HorusWindow Program. The tunnel identification program is HorusWindow applications logic program by Elcoplast. The purpose of this program is to upkeep network

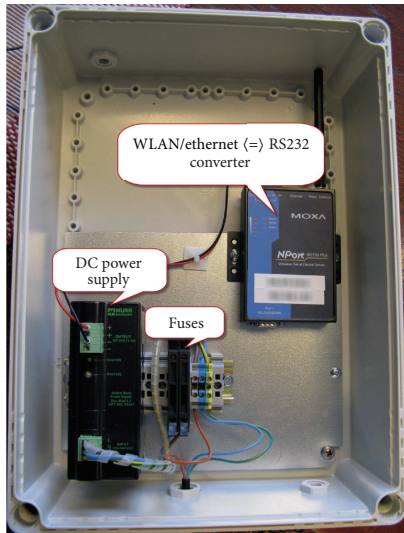


FIGURE 11: An information screen data transfer casing.



FIGURE 12: An identification card.

connections to the readers, collect identification information from the readers, make movement direction decisions based on the identification information and previous history of identification, and save the event information to the database. The upkeep responsibilities for the connections are with the integrated computers of each reading point. This gives a better scalability for the system.

Normally the program is always running and the user can see the current reading status of all readers. If the connection to the reader is lost, the program tries to secure it again by itself. However, sometimes the program must be rebooted to secure a lost connection. During rebooting, the program resets itself, starts the reading points, and configures the traffic light. Quitting the program is protected by a password to avoid any accidental program termination.

On the bottom of the information screen are green and yellow squares (see Figure 13). Only the first nine squares contain information. The squares can be green, yellow, or red, and the color tells if one of the antennas is working properly, has temporarily lost connection to the network, or has lost connection completely, respectively.

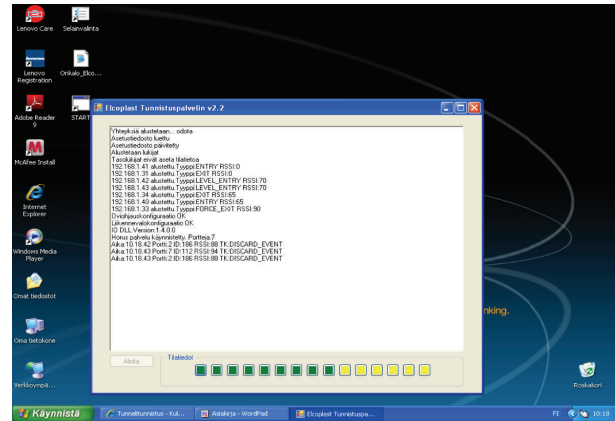


FIGURE 13: The HorusWindow application logic program.

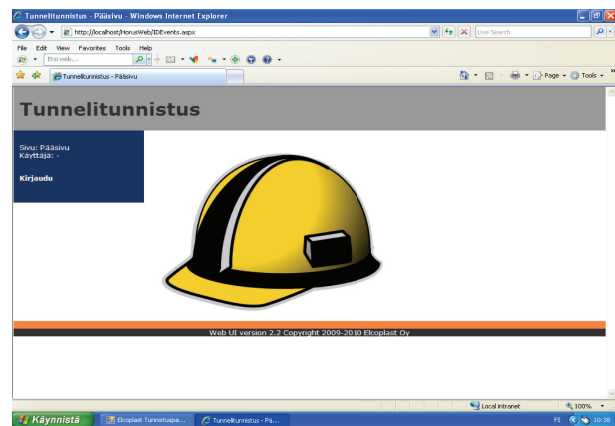


FIGURE 14: The start page of the tunnel identification program.

4.2. Web Application. The application logic does not have its own interface, so a web application has been created. The web application and the application logic are not directly connected, as all data goes through the database service (SQL Server).

The web application has been tailored according to Posiva's requests. The starting point in the development of the web application has been to achieve quick accessibility to monitor the people inside ONKALO. The web interface language is Finnish, as it is the official language of ONKALO. Next, some basic features will be introduced.

4.2.1. Tunnel Identification Program Start Page and Sign-In Page. The tunnel identification programs start page loads automatically when the browser is opened. At the left hand side of the start page, there is a link to the "sign-in" page (shown in Figure 14).

Login and password are typed at the tunnel identification program "sign-in" page. After giving login information and password, the user can enter the actual program.

4.2.2. The Tunnel Identification Programs Main Page and Its Menu. After logging in, a navigation menu panel will appear

on the left side of the page. The menu will contain thirteen different page options. Logging off can be done at any page with the “log-out” button.

All allowable actions are displayed in the menu. There are three different user groups preset in the program: basic user, advanced user, and administrator. Only the top two menu options appear for the basic user. The top three options appear for the advanced user and all thirteen menu options appear for the administrator user.

Only basic user rights are normally given for the tunnel identification program. Basic users are the security personnel and foremen. Only the monitors at Posiva have advanced user rights. Administrator level privileges are given only to six persons. A personal login and password must be created to all users. In addition, the first name and surname of the user must be given.

4.2.3. Search Person/Vehicle-Page. This page is used to type in the name of the person or vehicle registration number and the program searches the database. The program can automatically search from incomplete data, like partial name or registration number.

4.2.4. Current State Page. This is the most used page of the program and possibly the most important. From the current state page all the personnel and vehicles that have entered the ONKALO tunnel system can be viewed. Also the personnel or vehicles level information and last ID reading time can be viewed.

There are currently six official marked levels in the ONKALO tunnel system. However, in the program there are only two levels: 0 and -290. Here 0 means that the person or vehicle is between the ONKALO entrance and the dead end reading zones. Level -290 means that the person or vehicle is at the dead end area. These two levels are sufficient enough for work safety.

4.2.5. Map Page. On this page there is a 3D map of the ONKALO tunnel system, where the initials of all people and vehicles are shown, together with the information of the level they are on. An example map page is shown in Figure 15.

4.2.6. Access Event Page. From this page, it is possible to view the access information by certain time frames. There are four preset time frames: today, past 7 days, past 30 days, and all, and it is also possible to select the dates from what the access events will be viewed. There are several access events during a day, at some days even more than 1000.

4.2.7. Add Person/Vehicle Page. There is an input field that opens on this page, where a new person or vehicle information can be added. From the inquiry fields, surname/registry number and ID card specific number are mandatory. In addition, the group “person” or “vehicle” must be selected.

It is not possible to have multiple people or vehicles with the same ID number. If an ID number is reused, the previous data has to be erased. When this data is removed, it erases all the previous access data history linked to the card.

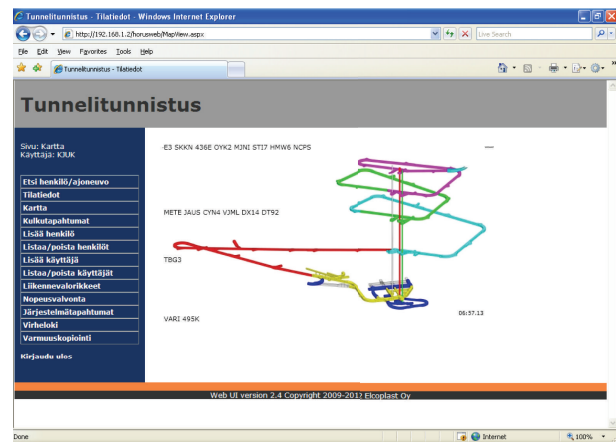


FIGURE 15: An example map page.

4.2.8. Traffic Light Violations Page. A traffic light violation occurs and is registered to the database, when the traffic light at the dead end has already changed to red but the reader at the dead end reads additional ID cards after this. The names of the people that have done this violation can be read from the web page. There are four different options: last 7 days, last 14 days, last 30 days, or all violations. The page also tells how many vehicles were at the dead end during this instance.

4.2.9. Speed Control Page. The speed control is based on the time taken to go the distance between two antennas. From this page it is possible to select the time intervals from which the possible violations will be checked. There are four different options: last 7 days, last 14 days, last 30 days, or all speed control violations.

4.2.10. System Event Page. Through this page, all the abnormal events that the system has recorded to the system event database can be viewed. These can be, for example, an unidentified ID tag at a reading area or adding a new user.

The system event register is kept by a database service (SQL Server). The database service enables that all events are recorded to the event register, no matter if it has been done through web interface, directly to the database, or through the system logics program.

4.2.11. Error Log Page. This page shows all the error log markings of the system logics. The program has an error reporting limit. This is because if an error stays on, it will fill the log fast. All error types have the same error reporting limit, which allows only one error log recording for each five-minute interval.

5. Evaluation

The RFID-based access monitoring system operation was systematically monitored for one year (1.5.2010–30.4.2011). Right from the start, the reliability of the initial system was found to be quite good. However, some reading errors

TABLE 1: The reading occurrences and the amount of errors during the monitoring period.

Done improvement	Monitoring period	Net error %	Reader error %	User error %	Errors in total	Reading occurrences in total
Time before any improvements	01.05.2010 to 14.07.2010	21.15%	65.39%	13.46%	52 pcs	8007 pcs
15.7.2010 Moving of the in-reading point	15.07.2010 to 22.09.2010	57.63%	6.78%	35.59%	59 pcs	7093 pcs
23.9.2010 Change from WLAN readers to LAN-readers	23.09.2010 to 15.11.2010	80.20%		19.80%	96 pcs	6971 pcs
16.11.2010 Tunnel dead end readers' program change	16.11.2010 to 03.09.2011			100%	32 pcs	16822 pcs
10.3.2011 Forced out-reading point	10.03.2011 to 22.03.2011			100%	2 pcs	2146 pcs
23.3.2011 Forced out-reading point's reading sensitivity adjustment	23.03.2011 to 30.04.2011				0 pcs	9421 pcs

occurred, and because of this, the first improvement area was the minimization of reading errors due technical reasons.

During the time the system was monitored, there were in total 201953 registered readings. Of these readings, 50460 occurred at the ONKALO entrance as "leaving tunnel." During the monitoring period, the reading reliability was generally over 99%. However, there was one short period, when the reading reliability was only 98.62%. The cause for the reading errors was found and eliminated during the monitoring time. During the last month of the monitoring period, there were no reading errors.

During the monitoring period, five changes were made to improve the reading reliability. The first change was made on 15.7.2010, when the in-reading point of ONKALO was moved from the entrance to pole 100. With this change, false identifications, in cases when there were workers near the ONKALO entrance, were eliminated. The second change was made on 23.9.2010, when WLAN-readers were replaced with LAN-readers. This change was made due to WLAN network instability. The next change was made on 16.11.2010, when the programming of the dead end readers was changed due to ONKALO network instability. On 10.3.2011 the forced out reader at ONKALO entrance was installed and on 23.3.2011 the reading sensitivity of the forced out reader was adjusted.

After the monitoring period, reading errors have occurred only due to human error. In order to eliminate these, special attention has been put into user instructions. Currently the ONKALO RFID system reliability is an average of 99.998%. Table 1 shows the reading occurrences and the amount of errors. It also shows the net errors, reader caused errors, and user caused errors, both before and after each separate improvement.

6. Further Development

The access monitoring system was found to be reliable during its testing and monitoring phase. Next, it was further developed to serve the fire department and from the

site safety aspect. In addition to the previously mentioned readers, also the safety areas and safety containers have been equipped with readers (11 pcs in total). These readers have been installed by the suggestion of the fire department to improve personnel safety in case of an accident situation. These readers help the fire department to immediately know how many people have been able to make it to a safe area and thus how many people need to be rescued from there. In addition, there are four more readers implemented into the system together with the company safety personnel. These readers are part of the company site safety plan and their positions are not revealed.

The first reader requested by the site safety team was installed in 2011 and the last site safety readers were installed in 2014. The first six readers requested by the fire department were installed to the safety containers during fall 2013. They proved to be working well during safety exercises so additional five ones were installed to safety areas during spring 2015.

The program has been constantly further developed and some additional features have been implemented by the request of the site safety team. The latest addition has been a tunnel time reporting form for occupational healthcare, which was done during fall 2015. To further improve work safety, there are plans to add readers to levels -90 and -180 in the near future.

In the future, the RFID-based system has been planned to be used in the final depositing of the used nuclear fuel. It has been envisioned that this system would be one of the selected systems to monitor the vehicle that transports and sets the nuclear waste capsule into the tunnel. It is required that the vehicle must be monitored by at least two separate systems (Radiation and Nuclear Safety Authority (STUK) requirements [16]). See Figure 16 for a prototype canister transfer and installation vehicle, the purpose of which is to enable the disposal of used nuclear fuel, enclosed into canisters. According to the plan, the device will be used to transport canisters from the interim storage facility, located



FIGURE 16: A prototype of a canister transferring and installation vehicle [17].

more than 400 meters below the ground surface, to the deposition tunnel [17].

It has been also considered that the flow of the buffer material used in ONKALO could be monitored from the stage it is manufactured up to until it is placed into the ONKALO tunnel system. The copper canister is isolated from the surrounding rock with a buffer material. A number of blocks of tightly compressed bentonite are installed as a buffer material between the canisters and the rock in the final disposal hole. The expanding bentonite fills the space surrounding the final disposal canisters [17]. The goal is to fulfill the STUK requirements for buffer material storage, transportation, and final deposition monitoring [16].

7. Conclusions

In this study, an RFID-based access monitoring system, for identifying people and vehicles, was developed and implemented into challenging tunnel conditions for a nuclear waste storage facility. The presented ONKALO access monitoring system has been highly reliable since it was taken into service for a monitoring period in May 2010. Still, during the monitoring period, the system was constantly improved to provide the best possible work safety.

At the final stages of the monitoring period, the reading reliability was 100%. Also after the monitoring period, the reading reliability has been an average of 99.998%. The only errors are user caused errors. This shows that the developed access monitoring system is working well in these challenging tunnel conditions. After the monitoring period, new features for safety improvement have been created to the system and it has been planned to be used also in the final depositing of the used nuclear fuel.

The next research topic is to optimize the reading areas of the RFID readers in ONKALO, which enables the readers to be installed immediately to the right places in the future.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

References

- [1] T. Saario, A. Ikonen, P. Keto et al., "Design of the disposal facility 2012," Working Report 2013-17, Posiva Oy, Eurajoki, Finland, 2012, http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/45/087/45087772.pdf.
- [2] P. Misra, S. Kanhere, D. Ostry, and S. Jha, "Safety assurance and rescue communication systems in high-stress environments: a mining case study," *IEEE Communications Magazine*, vol. 48, no. 4, pp. 66–73, 2010.
- [3] Z. Shi, Y. Li, and Q. Gu, "Based on TWA adaptive centroid wireless localization algorithm of area in underground mine," *Advances in Information Sciences and Service Sciences*, vol. 4, no. 19, pp. 191–196, 2012.
- [4] U. Farooq, K. M. Hasan, F. Rafiq, and M. U. Asad, "An integrated approach towards designing an embedded wireless monitoring and access control system using RFID and MMS technologies," in *Proceedings of the 16th International Multi Topic Conference (INMIC '13)*, pp. 182–188, Lahore, Pakistan, December 2013.
- [5] C. Hurjui, C. Turcu, and A. Graur, "Management system of the products on warranty based on RFID technologies," in *Proceedings of the 11th International Conference on Optimization of Electrical and Electronic Equipment (OPTIM '08)*, pp. 231–236, IEEE, Braşov, Romania, May 2008.
- [6] M. Anchan, W. Zongtian, and G. Mengji, "An access control and positioning security management system based on RFID," in *Proceedings of the International Conference on Intelligent Human-Machine Systems and Cybernetics*, pp. 537–540, Hangzhou, China, August 2015.
- [7] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, 1948.
- [8] A. R. Koelle, S. W. Depp, and R. W. Freyman, "Short-range radio-telemetry for electronic identification, using modulated RF backscatter," *Proceedings of the IEEE*, vol. 63, no. 8, pp. 1260–1261, 1975.
- [9] J. Landt, "The history of RFID," *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, 2005.
- [10] P. Nikitin, "Leon Theremin (Lev Termen)," *IEEE Antennas and Propagation Magazine*, vol. 54, no. 5, pp. 252–257, 2012.
- [11] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.
- [12] D. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, Newnes-Elsevier, 2008.
- [13] International Organization for Standardization, ISO/IEC 18000-6, <http://www.iso.org/>.
- [14] EPCglobal, Overview of the Ultra High Frequency (UHF) Regulations Worldwide, <http://www.gs1.org/epcglobal/implementation>.
- [15] IEC 60529 Standard, <http://www.iec.ch/>.
- [16] STUK—Radiation and Nuclear Safety Authority, Security of a Nuclear Facility, November 2013, <http://plus.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVLA-11>.
- [17] Posiva, <http://www.posiva.fi/en/>.

