ANTI-VANDALISM SYSTEM FOR MONITORING SMART LEVEL CROSSING PROPERTY: A COMPREHENSIVE REVIEW

SISTEM ANTI-VANDALISME UNTUK MEMONITOR PROPERTI SMART LEVEL CROSSING: KOMPREHENSIF REVIEW

M. Rosyidi[1], Thiya Fiantika[1], Novi Irawati[1], Sinung Nugroho[1]

[1] Center of Technology for System and Infrastructure of Transportation
Agency for the Assessment and Application of Technology
e-mail: m.rosyidi@bppt.go.id

Abstract

This research addresses the problem of vandalism incident related to the smart level crossing technology. Smart level crossing system is essential as a safety system inside the level area, because of that any failure related to the System will endanger the railway and road user. Another subsystem that protects smart level crossing property is critical. This research will show the plan for applying anti-vandalism technology and analysis another possibility of technology related to the System.

Keywords: Vandalism, Smart, Level crossing, Subsystem, Railway.

Abstrak

Penelitian ini membahas tentang permasalahan vandalisme yang terkait dengan teknologi smart level crossing. Sistem smart level crossing sangat penting sebagai sistem keselamatan di dalam tingkatan area, karena itu setiap kegagalan yang terkait dengan sistem akan membahayakan pengguna kereta api dan jalan yang bersinggungan dengan rel kereta. Sub-sistem lain yang memberikan perlindungan terhadap properti smart level crossing itu sangat penting. Penelitian ini akan menunjukkan rencana pengaplikasian teknologi anti-vandalisme dan menganalisis teknologi lain yang berhubungan dengan pengamanan ini.

Kata kunci: Vandalisme, Smart level crossing, Sub-sistem, Rel kereta api.

Received: 13 April 2020, Revised: 03 August 2020, Accepted: 07 August 2020

INTRODUCTION

The local government of Indonesia is handling quite large of the level crossing railway system. By the time, increasing the number of the railway planning area, level crossings are also growing and become social expense burden[1,2)]. Many peoples die, and a vast number get injured over the accident, especially related to the manual and unmanned gate system.

Usually, the level crossing is guarded by an officer if it is considered traffic on the level crossing is quite busy. In this regard, to assist and ease the task of supervisors in the field, the development of early warning equipment becomes something that is needed, to minimize accidents[3)].

Smart Level Crossing (SLC) is a system that developed for safety and early warning technology at railway level crossing. The System can detect train arrival of the train at certain places, informed to the next gate of the railroad crossing, and cannot disturb the current railway system.

Current manual level crossing system technology must be replaced using an automatic system. Simple technology like IR sensor, radar sensor, IoT technology[4-6)]. The mechanism is very much programming based. The basic idea of smart level crossing system is capturing the arrival of

the train using radar sensors, send the signal to the micro-controller and active warning Variable Message Sign (VMS) and light. The manual System still as a backup alongside the automatic System in the case of system failures.

Smart level crossing running without man-guard System, the problem to keep the control and other mechanical equipment will arise. Especially, vandalism event problem that frequently occurs in Indonesia. Vandalism incident begins from trespassing activity. Trespassing incidents result from the violation of the rail track access rules by pedestrians. Although in many cases trespass is just a non-malevolent crossing violation, among the individual motivations to trespass on railway property, there are also those related to criminal actions, like theft from trains or of line-side equipment and execution of vandalism and graffiti. Whilst vandalism refers to the intentional damage or destruction of property owned by others. Vandalism includes acts of seat slashing, breaking windows, window etching, putting objects onto the tracks, throwing things at trains, littering and damaging other railway assets[7].

SMART LEVEL CROSSING COMPONENT

A. Design System

Smart level crossing consists of three main components; input of the train detection, data processing, and information warning system. Figure 1 shows the general design of smart level crossing system.

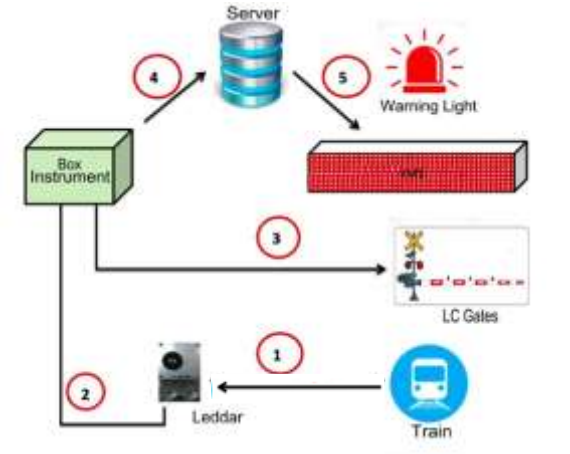

Figure 1.
General Design of Smart Level Crossing

The design system of SLC that is shown in Figure 1 can be explained as follows.

1) Leddar sensors detect the train.
2) Leddar sends current information to the Box instrument.
3) Data received from box instrument directly sending to the level crossing gate.
4) Another subsystem inside box-instrument sends data to the server.
5) Server-side applications do the processing and send information as a warning to the variable message sign and warning light.

B. Installed Devices

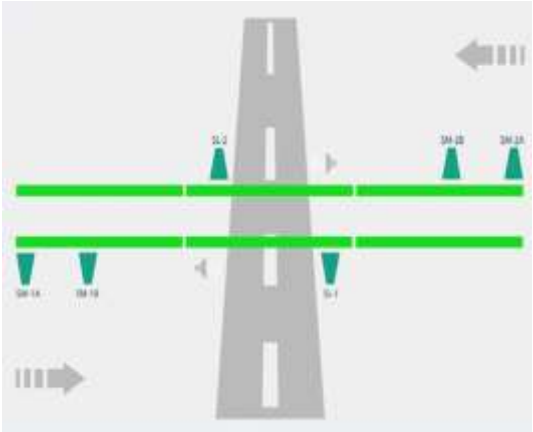

Figure 2.
Smart Level Crossing Installed Devices

In general, there are three parts of SLC part must be secure from vandalism action. Two main-systems must be protected, the main priority is the on-site part system, and the other is the off-side part system. Figure 2 shows the position of the installed device in Pekalongan city:

1) Electrical Part
   SM *(Sensor Muka)* is entrance radar sensor that detects train when entering the area of radar monitored. Four sensors dispatched SM1A, SM1B, SM2A, SM2B. SL1 *(Sensor Lewat 1)*, SL2 *(Sensor Lewat 2)* are pass radar sensor that captures pass train near the area of a level crossing. Pass sensor near these area box instrument installed that consist micro-controller, level crossing gate, VMS, and warning light.
2) Mechanical Part
   The mechanical part of the SLC system consists of mechanical-System of level crossing gate and infrastructure that support the electrical component.
3) Data and Application Layer Part
   Data and application layer installed on the sensor part and level crossing

P-ISSN 1410-3680 / E-ISSN 2541-1233

management system that provided at the ATCS (Automatic Transportation Control System) area, managing by Dinas Perhubungan (Dishub).

C. Potential Vandalism on SLC Part

Main parts of SLC are shown in Table 1, most of the elements consist of the electrical component, and few of them are a mechanical part. These parts are vulnerable to vandalism action. In this table, the application parts are not included, but these parts play an essential role in the whole SLC system.

Vandalism at the application layer is a little bit different compare to the on-site part of SLC. Application layer related to the security of the application system. The list of the application layer can be explained as follows:

- Sensor logic application for potential penetration is using LoRa (short for long range) communication tapping system. A LoRa is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology.
- Data halting and termination: the process, when a data sensor transmits from the sensor position to the main-controller or data from the sensor to the SLC database system.
- Wireless interference and jammer: the problems of interference or totally, cut off the wireless communication system.
- Data hacking: data hacking of the Level crossing management system.

Table 1.
Main Mechanical and Electrical Part of SLC

No	*Part*	*Item*	*Function*
1	Mechanical	Electric Motor AC	Open and close gate
2	Mechanical	Power Transmission	Transmit power from electrical to mechanical
3	Mechanical	Gate	Indicator to open and close System
4	Electrical	SX1276/SX1278 Wireless Modules	
5	Electrical	Horn Speaker	As an item for warning voice, a complement of warning light and VMS
6	Electrical	Leddar Sensor	The main-sensor to detect train integrated to the entrance component (SM1A, SM1B, SM2A, SM2B) and pass part (SL1, SL2)
7	Electrical	P10 DMD	Warning running text
8	Electrical	Solar Panel	Gather energy from solar System and convert it to electricity to powering SLC component.
9	Electrical	Panasonic Battery	Supplying electric power
10	Electrical	Teensy USB module	To get data that saving on-site component
11	Electrical	CPU Module	Control all activity from sensor and docking communication module
12	Electrical	Lora and CDMA-GSM communication box	Communication module to send data from a sensor to control panel, CDMA GSM to send data from control panel to the data management system at ATCS
13	Electrical	Battery and Charger	To save the energy/ electricity from solar panel

CURRENT ANTI-VANDALISM SYSTEM

The security of all layers of the SLC system, current subsystem has been implemented. The detail of current anti-vandalism System will be explained as:

1) Mechanical/physical layer secured by trellis mechanism; the person that enters the area needs a lot of time to commit vandalism intention.
2) Electrical layer secure by a warning to the level crossing management system. This system warning will be detected in ATCS and admin mobile application.
3) Application layer; vandalism inside this part related to the data hacking, the developer has inserted security technology and unknown activity preventive inside the System.

Figure 3.
Level Crossing Management System

ANTI-VANDALISM UPGRADE SYSTEM

The existing SLC System is not enough to support current smart level crossing system. Sending warning is too long to counter vandalism action. The upgrade of the System is needed to solve this problem, with proven technology and an affordable price. Advancement of the anti-vandalism System is including camera upgrades, additional types of brackets for sensors, and security upgrades on *Smart Level Crossing* servers.

A. Camera Upgrades

The installed camera on the site of a box instrument and sensor area is needed to monitor the situation inside the level crossing area. A standard surveillance camera is not enough for the SLC system, but it is required through the camera system with rich features. Some industrial camera system[8)] provides rich, tough camera for vandal-resistant and tampering alarms. The features camera system probably needed to support vandal resistance, explain as:

1) Coverage area
   Coverage area specification of the camera sensor must be exposed widely, so the camera can be modified to the smart camera system and monitor the human activity, regular activity or come up to the vandal action.
2) Face-recognize system
   Image processing, including subsystem to detect the face of human that related to the vandal-action. Face recognizing is a part of image processing, and some researcher has conducted many experiments for a robust algorithm. Figure 4 shows that the process of face-recognize System by Olszewska et al. [9)] This research utilizes dataset from various human face database.

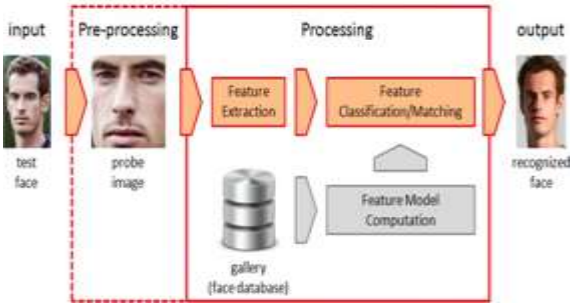

Figure 4.
Face recognize System

3) Vandal-resistant
   The design and position of the camera are essential to reduce the change of vandal-action success. Cameras are also at a greater risk of vandalism when they are placed at easy-to-find locations for deterrence. The tough camera allows to minimize vandalism damage and to save time and money while recovering from the cracks. The camera that protected by another layer of though the material is an ideal type that can be implemented to the smart level crossing system.
4) Touching and tampering alarms
   Alarms that detect a person who touches the sensor or tampering the vital object of a smart level crossing system included the camera. The focusing mechanism in the camera is designed to avoid images deteriorating from external mechanical shocks. Auto Back Focus (ABF) enables readjusting the focus remotely from an operation centre if the camera becomes out-of-focus. The robust camera can absorb shock information from tampering action,

Figure 5 shows a reliable camera that absorbs shock from tampering action.

P-ISSN 1410-3680 / E-ISSN 2541-1233

Figure 5.
Absorb the Shock of Tampering Action

5) Light adjustment
   Light adjustment is needed to reduce light at the day and add the light effect at night. This feature is crucial for the camera secure so that the System can operate 24 hours.
6) Vibration reduces
   Vibrations sometimes blur images. When large, heavy trailers or trains pass by, they may cause vibrations that travel through the ground to cameras on poles and negatively affect image quality. Machinery such as pressing machines, strong winds and storms also cause vibrations and pole swinging. Building poles utterly unaffected by these vibrations and swinging costs.

B. Additional Bracket Protection

Bracket protection must be upgraded from old bracket system to the new bracket system that more tough and compact. Bracket refer to the casing that protected sensor and another SLC instrument. The robust-casing provides protection that will withstand extreme abuse[10].

C. Secure System

Smart Level Crossing is a part of the Internet of Things (IoT) system. Anti-vandalism for application layer based-on secure of IoT concept. Secure System follows the general goal[11]:

1) Establish a security architecture of smart level crossing to protect a building management system using sensor network by using standards and best practices, including the communications channel/network used to transmit sensor data to the Level Crossing Management System (LCMS).
2) Promote the reliability, integrity, and availability of LCMS of the smart level crossing.
3) To secure the System concerning the risks using a specific security model inside the LCMS server.

To upgrades, the security of the smart level crossing system must be implemented using *High-Level Security System* (HLSS). Level of this System defines as[12]:

1) Secure Group Management was usually in large scale networks when the SLC implementation increased use. The System split into small groups of nodes for efficient communication.
2) Intrusion Detection: Wireless networks are susceptible to many forms of intrusion. Every node of the SLC must be monitor to detect the possibility of an intruder.
3) Secure Data Aggregation: One benefit of a wireless sensor network is the fine-grained sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic being sent back to the LCSM.

Secure System for smart level crossing is essential to handle data-vandalism. The regular secure System consists of the network perimeter protection, network policy violation detection, logging activity, incident recording/reporting, response procedures during (after the incident), mitigation procedures, optimization scheme (improvements from the incident), recovery procedures (during or after the incident), and optimization scheme execution.

CONCLUSION

Three layers of SLC must be monitor from vandalism action, mechanical layer, electrical layer, and application layer. Mechanical and electrical layer security level using a similar security system and application layer adopts the computer system security. Establish a security architecture needed for mechanical and electrical layer and concern the risk of specific security model inside the LCSM server. Both of the layers must be promoted to the reliability, integrity, and availability to realize the anti-vandalism to secure that System is running well. The application layer is focused on the counter intrusion, data and group management secure. The last important thing is handling the security planning before the incident, recovery and improve System after the incident.

AUTHOR CONTRIBUTIONS

Main contributor of this work is M. Rosyidi. The other authors, Novi Irawati, Sinung Nugroho, and Thiya Fiantika are supporting contributors.

ACKNOWLEDGEMENTS

Thanks to PTSPT, BPPT that fully support this research related to the technical support and research funding.

REFERENCES

1. VTP Institute, *Safety and Health Impacts*, April 2018.
2. Camkurt, M., Ay, D., Aksu, N., and Günalp, M., 10-year Evaluation of Train Accidents, Turkish Journal of Trauma & Emergency Surgery: TJTES, Vol. 17, Issue: 5, p. 440-444, September 2011.
3. Alam, M., et al., *EEE 499 – CAPSTONE PROJECT: Automatic Level Crossing System*, Project Report, Department of Electrical and Computer Engineering, North South University, Bangladesh, November 2015.
4. Chandolu, Y.S.V., Dharaa, C., and Prakash, P., *Railway Gate System: Railway Gate Status Detection*, International Journal of Recent Technology and Engineering (IJRTE), Vol. 7, Issue: 6, p. 523–525, March 2019.
5. F. Traffic, *Special Edition Paper*, no. 33, pp. 43–48, 2014.
6. Akhil, M., Ashwin, M., Nathaniel, J., and Mary Anita, E.A., *A Study of Technologies for Supervising Unmanned Level Crossings*, International Journal of Engineering Research & Technology, Vol. 6, No. 3, p.1-4, May 2018.
7. Offler, N., Thompson, K., Hirsch, L., Thomas, M., and Dawson, D., *A review of the literature on social non-technical deterrents for vandalism in the rail industry.* No. RT 106, Brisbane: CRC for Rail Innovation, 2009.
8. Panasonic, Tough outdoor cameras Panasonic Video surveillance systems.
9. Olszewska, J.I., *Automated Face Recognition: Challenges and Solutions*, Pattern Recognition - Analysis and Applications, S. Ramakrishnan, IntechOpen, 2016, DOI: 10.5772/66013.
10. Cruz, A.P.S., *Preventing graffiti and vandalism*, Journal of Chemical Information and Modeling, Vol. 53, No. 7, p.1689-1699, 2013.
11. Cichonski, J., et al., *Security for IoT Sensor Networks: Building Management Systems Case Study*, National Institute of Standards and Technology, White Paper (Draft), February 2019.
12. Stavroulakis, P., and Stamp, M., *Handbook of Information and Communication Security*, Handbook of Information and Communication Security, January 2010.