System Architecture for Physical/IT Security Event Integration

Seon-gyoung Sohn and Jungchan Na

Cyber Security-Convergence Research Department,
Electronics and Telecommunication Research Institute (ETRI), Daejeon, 305-705, Republic of Korea

Summary

Both physical and IT security are necessary to guarantee the safety of industrial facilities; however, the two elements are operated separately in most organizations. To solve the security problems caused by this segregated operation of security systems, studies on the integration of physical and IT security are being conducted actively. To that end, event integration technology, which collects events from various items of security equipment to create security state alarm for analysis, is required. This paper suggests a structure that integrates physical and IT security events, with the aim of dealing with the differences and promoting interaction between physical and IT security systems, and describes the related interface and data exchange.

Key words:

Event Integration, Convergence Security, Event Normalization

1. Introduction

Recent threats against the information assets of industrial facilities include the leakage of internal assets from physical space by portable storage media, and unauthorized intrusions, and from cyber space by hacking, worm viruses and malicious bots. In other words, these threats assume both physical forms such as intrusion, stealing, and terrorism, and IT forms such as information leakage, forgery, and hacking, all of which could result in a national disaster including the shutdown of social infrastructure and/or utilities.

Industrial facilities, which are organic combinations of people, information, infrastructure, and systems, are composed of both physical and cyber spaces, and their information assets cannot be protected by fragmentary technologies such as conventional physical and IT security. To protect information assets under such convergence security in a business environment, a technology designed to organically integrate physical space (work space) and logical space (cyber space) in order to detect and prevent security violations is needed [1]. Convergence security is defined as a system wherein the security elements of an organization are integrated for interaction to reduce costs, improve operational effectiveness and efficiency, and implement organization-wide control of threats [2]. Turner [3] defines it as something related with cooperation among, and not unification of, various environments.

The Alliance for Enterprise Security Risk Management (AESRM) summarized the necessity of convergence security as follows [4]:

- Rapid Expansion of the Enterprise Ecosystem
- Value Migration from Physical to Information-Based Assets
- New Protective Technologies that Blur Functional Boundaries
- New Compliance and Regulatory Regimes
- Continuing Pressure to Reduce Costs

The necessity of convergence security changes the role of security in industrial facilities and the entire business processes through functional intercrossing in the security domain [5].

This paper proposes an architecture that can integrate physical and IT security events, and which will provide convergence security services to organizations by monitoring acts on the basis of an analysis of the relations among security events, in order to cope with and promote interaction between physical and IT security systems. The proposed architecture does not require the replacement of existing physical and IT security systems, but it is expected to help protect industrial facilities from various security threats in the physical/IT convergence environment and to provide more efficient security performance based on centralized and normalized surveillance and tracing.

This paper consists of the following: Chapter 2, in which the related works on convergence security are discussed; Chapter 3, in which the concept of convergence security is described; Chapter 4, in which the architecture for physical/IT events integration is proposed; and Chapter 5, in which the conclusion is presented.

2. Related Work

There have been many studies on and R&D activities related to the integration of physical and IT security technologies, while recent studies have mainly focused on convergence security solutions. Figure 1 shows various convergence security solutions classified according to the categories of linkage equipment, event analysis, and monitoring interfaces.

Manuscript received January 5, 2012
Manuscript revised January 20, 2012

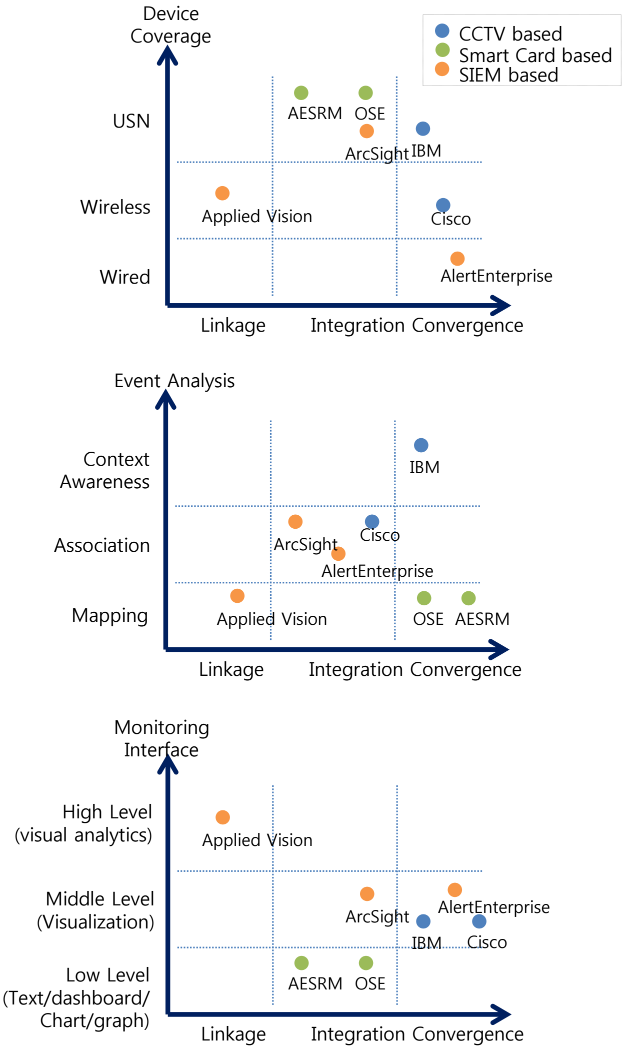

Figure 1. Classification of Convergence Security Solutions

The Open Security Exchange [6] is conducting studies on a method of widely converging physical and IT security systems to reduce costs and ensure more efficient human resources management in business. AESRM [4], which was established to provide business circles with a methodology for converging the traditional physical security and cyber security systems of the ISACA (Information System Audit and Control Association) and ASIS (American Society for Industrial Security) International and to facilitate application of the converged security system, is conducting studies on the integrated management of business security covering employees and assets, as well as physical and IT security.

ArcSight [8] is offering solutions, based on the SIEM platform used by ESM, which collects security events from various sensors of the access control system and network security devices and detects intrusions by monitoring users' behaviors in logical and physical spaces in conjunction with the IdM (Identity Management) system.

In addition, it has been offering the Physical and Logical Security solution, which converges IT security events, SCADA, HVAC, and RFID, since 2006.

Cisco [10] advanced into the physical security solution market with its launch of a video surveillance product line in 2008. Its activities include the development of solutions which integrate network security and physical security utilizing the IP network infrastructure, and constructing the business providing ideal, eco-friendly residential environment by grafting advanced network infrastructure onto transportation, safety, security, education, and medicine.

IBM [11] is offering a framework which can analyze the relationship between various events including RFID, GPS, meta data, transaction records, and 911 call records on the basis of CCTV video analysis technologies and a smart surveillance solution capable of modeling the user's business procedures and linking them with video and other security sensors.

However, since most of the solutions perform events integration or events relationship analysis with the events obtained from individual security devices, proper judgment can be made for the individual security devices, but the security states, which are severe intrusion cases in convergence security aspects are difficult to be identified.

3. Concept of Convergence Security

In industrial facilities, which are organic combinations of people, information, infrastructure and systems, both physical and cyber spaces exist. The security issues which may occur in an environment in which physical and IT security are converged are as follows:

- Security of tangible/intangible information assets
    - Evaluation of information value and risk monitoring of assets
    - Monitoring of the security and risk states of carried in/out information assets
    - Surveillance of unauthorized access to information assets by employees

- Security of access-controlled spaces
    - Surveillance on intrusion into sensitive spaces (access-controlled spaces, limited spaces by user classification, access-controlled servers, sensitive cyber spaces)
    - Monitoring and predicting space log linkage (image, access/human affairs/user log)

- Securities related with information asset leakage and abnormal behaviors
  - Detect information leakage by user and host profiling
  - Monitoring the behaviors of users and hosts (copying, printing, network transmission, etc.) and abnormal statuses
  - Linked monitoring of abnormal leakage activities (shooting, copying, printing, network transmission, etc.).

It is difficult to solve the abovementioned security problems with the use of individual security devices only, and rather requires convergence security which responds promptly by linking and analyzing events from various devices.

Figure 2 shows the concept of convergence security designed to provide security services in an environment in which physical and IT security are converged.

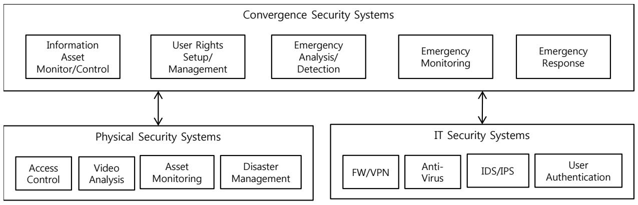

Figure 2. Convergence of Physical Security and IT Security

Physical security systems are focused on the protection of facilities, employees and assets from potential threats, as well as on controlling both employees and assets in and outside the facilities. The functionalities of a physical system mainly comprise the following: control of access to facilities and spaces, video surveillance using CCTV, monitoring of assets including carrying in and out, and position control; and disaster control to prevent damage by disasters such as fire.

IT security systems are designed to protect sensitive information and information systems from unauthorized access, usage, and damage by disclosure and alteration. IT security systems are represented by the following: user authentication control, which permits or rejects access to classified services; firewall and VPN, which detect and interrupt attacks and intrusions via the network; and anti-viruses, which are designed to protect the system from IDS/IPS, worm, malicious codes, and hacking.

A convergence security system aims to control personnel and information assets and to detect and prevent intrusion incidents in an environment converging physical and IT security by integrating the events from physical security and IT security systems. The system provides a security service which converges physical and IT security services by collecting, normalizing, and analyzing the relationship among the events generated from various security devices. A convergence security system is a physical/IT security convergence control system which enables the detection of and response to information asset intrusion incidents by integrating and analyzing the security events occurring in the convergence space of physical and IT security. The system should be able to remove the dead-angle of security by events integration from access control to IT system (from Door to System), as well as detect and respond to information asset intrusion incidents on the basis of the access by and behavior of users based on a given physical space.

4. Architecture of the Event Integration System

4.1. Components

The structure of the events integration system for convergence security comprises a security devices layer, a convergence security engine layer, and an application layer, as illustrated in Figure 3.

The security device layer comprises the physical and IT devices and systems used in industrial facilities, while the engine layer comprises an engine for processing the physical/IT security integrated events, an engine based on security event integration for detecting intrusions, an engine for response to intrusion incidents, and an integrated user interface which visualizes the performance of the entire system in an intuitive way and provides a convergence security service. The application layer comprises physical/IT convergence security services that utilize the functionalities of the convergence security system.

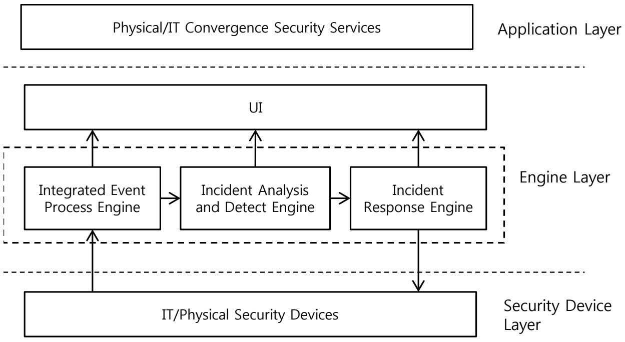
Physical/IT Convergence Security Services
Application Layer
UI
Integrated Event Process Engine
Incident Analysis and Detect Engine
Incident Response Engine
Engine Layer
IT/Physical Security Devices
Security Device Layer

Figure 3. Convergence Security Framework Structure

4.1.1. Security Device Layer

− Physical security devices

Physical security devices include CCTV or other video monitoring systems, access control systems, environment monitoring sensors, position sensors such as GPS and RTLS, and other devices for the security of personnel and facilities in a physical space. The security events obtained from physical security devices include image data, access information, environmental information such as temperature, humidity and intensity of illumination, and position information.

− IT security devices

IT security devices include security systems such as IDS/IPS, FW, Anti-Virus, ESM, and DLP, and general network devices including routers and DB servers, and other security devices for information assets in the logic space. The events obtained from IT security devices include information on system access and intrusion, defense log, virus-related log, information on the creation, modification, deletion and transmission of important files, network traffic and system log.

4.1.2. Engine Layer

The engine layer provides the core elements for convergence security services by performing the filtering, storing, and normalizing of the security events obtained from various physical and IT security devices linked with the security device layer. This layer detects intrusion incidents by analyzing the performer, space and time of event occurrence from normalized events; evaluates the degree of risk facing the host and user by performance analysis; and undertakes the appropriate response against detected intrusion incidents by controlling the pertinent physical/IT security devices according to the incident type. The layer also provides a user interface for visualization of the procedures of processing, analyzing, detecting and responding to events, and for convergence security service configuration.

4.1.3. Application Layer

This layer provides various convergence security services via the functionalities of the event integration system and user interface, including the monitoring/control of information assets and the detection, analysis, tracing, response and forensic services required to respond to intrusion incidents.

4.2. Main Functions of the Event Integration System

4.2.1. Event Processing

The Integrated Event Process Engine collects, stores, and normalizes the events from various physical and IT security devices of the security device layer, and sends the result to the Incident Analysis and Detect Engine. 4W1H (Who, When, Where, What, How) context-based normalization is conducted to normalize the events from the various devices in a unified format. 4W1H context-based normalization analyzes the context of the event fields to extract information on the object (Who), time (When), physical/logical position of the device (Where), major content (What), and the path (How) of the event and maps the information into a format which the intrusion incident analysis detector can process. Context-based normalization enables easier analysis of the state of security by linking different types of security events.

4.2.2. Incident Analysis and Detection

The Incident Analysis and Detection Engine identifies intrusion incidents by analyzing the relationship between the various security events occurring in the convergence environment, and determines the level of the security threat to the user/host/space in order to identify intrusion incidents which are difficult to identify using a physical or IT security system. To this end, the engine assesses the value of the information assets by taking the distribution and access frequency into consideration; analyzes the security events; estimates the risk to the user, host and space; judges intrusion by event relationship analysis; and determines the level of risk of transmitting intrusion incident detection information to the Incident Response Engine. The intrusion incident information message includes the incident identification information, such as the type, place, and time of the incident, and the level of threat posed.

4.2.3. Security Response Management

The Incident Response Engine performs the response process in accordance with the security policy and controls the physical/IT security devices. For this, the engine defines the policies and processes for the response according to the content of the intrusion incidents and carries out the procedures. The engine also presents a security device related with the incident on the basis of the space where the incident has occurred and provides multiple, simultaneous-mode control. With workflow-based-processing of the response process according to the type of incident, a comprehensive response against an intrusion into the convergence security space, and a prompt response according to the spatial phase relationship between the space of intrusion and the security devices and the spatial characteristics, can be implemented, and the spread of the incident can be prevented. The response information message, which provides the integrated user interface with the procedure and the results of the response process, includes information on the response process, the device under control, the control content, and the state of implementation.

4.2.4. Integrated Graphic User Interface

The Integrated Graphic User Interface displays the results of the event process and analysis from the engine layer comprising the event integration system and the incident detection/response information, in order to facilitate interaction between the security manager and users and to support the configuration of various convergence security services.

5. Conclusion

This paper proposes an event integration system architecture which can provide convergence security services in industrial facilities by collecting the security events from various physical and IT security devices and analyzing the relationship between those events. The proposed system enables the protection of the information assets of industrial facilities in the convergence environment – something which cannot be solved with conventional, fragmentary technologies. The system also provides such functionalities as early-stage warning, condition recognition, condition analysis, and emergency response by mapping, monitoring and controlling the events with the real information assets of industrial facilities.

The system is expected to be applicable to security products which integrate physical/IT spaces and automate identification of the responsibilities to the entities responsible for intrusion incidents, in an environment integrated with security, disaster, and facility safety.

Acknowledgments

This study was conducted as a part of the Industrial Original Technology Development Project (10035237 / The development of an intrusion detection and response technology based on security convergence for protecting the information assets of industrial facilities) sponsored by the Ministry of Knowledge Economy (MKE) and the Korea Evaluation Institute of Industrial Technology (KEIT).

References

[1] Watson, James, Physical and IT Security Must Go Together, Computing, May 4, 2005.
[2] Physical/IT Security Convergence: What It Means, Why It's Needed, and How to Get There, Open Security Exchange, 2007.
[3] Geoffrey W. Turner, Trends 2007: Physical and Logical Security Convergence, Forrester Research, 2007.
[4] Booz, Allen, Hamilton, Convergence of Enterprise Security Organizations, The Alliance for Enterprise Security Risk Management (AESRM), 2005.
[5] J.D. Kim, K.W. Kim and Y.D. Lee, The Concept and the Methodology for Approach to Convergence Security, Review of KIISC, Vol.19 No.6, 2009.
[6] http://www.opensecurityexchange.org
[7] http://www.arcsight.com/
[8] http://www.appliedvision.com/
[9] http://www.cisco.com
[10] http://www.ibm.com

Seon-gyoung Sohn received her B.S. and M.S. degrees from Chonnam National University in 1999 and 2001, respectively. Since 2001, she has been working at the Knowledge-based Information Security & Safety Research Department at the Electronics and Telecommunications Research Institute (ETRI), where she is a senior member of the research staff. Her research interests lie in the areas of network security, network traffic analysis, and security situation monitoring.

Jungchan Na received a B.S. degree from Chungnam National University in 1986, an M.E. from Soongsil University in 1989, and a Ph.D. in Computer Science from Chungnam University in 2004. He has been a principal member of the engineering staff at the Electronics and Telecommunications Research Institute (ETRI) in Korea since 1989. His research interests include network security management, network security visualization, and security situational awareness