Cyber Security Evaluation of the Wireless Communication for the Mobile Safeguard Systems in Nuclear Power Plants

Sooill Lee\textsuperscript{a}, Yong Sik Kim\textsuperscript{a}, Song Hae Ye\textsuperscript{a}

\textsuperscript{a} Central Research Institute, Korea Hydro and Nuclear Power co., (KHNP-CRI), Daejeon, Korea

Abstract. This paper introduces cyber security evaluation results and a design of the wireless communication technology to apply to safety, safeguard, emergency prepared functions in nuclear power plants. While wireless communication technologies can generally make mobility and efficiency on plant operation, those have seldom been installed on the nuclear I&C systems due to the negative concern of unexpected outcomes that stem from electromagnetic interference and cyber attack. New design of advanced digital safeguard and I&C systems uses computer-based systems for those functions. On the other hand, those are being exposed to various types of new and existing cyber threats, vulnerabilities and risks which significantly increase the likelihood that those could be compromised. In order to employ the wireless communication technology in those functions, licensees should assess and manage the potential for adverse effects on safety and safeguard functions so as to provide high assurance that critical functions are properly protected cyber attack. It is expected that the safety and safeguard function, specifically on the area of real-time monitoring, logging, can be enhanced by employing the mobile devices (e.g., smart phone, laptop, smart pad, etc). In this paper, we deal with the cyber security evaluation, which consists of threat analysis, vulnerability test, establishment of security plan, and design solutions for the wireless communication on the basis of IEEE 802.11 (Wi-Fi) protocol. Proposed evaluation and design solution could be a basis for the design of wireless communication and mobile safety and safeguard systems in nuclear power plants.

1. Introduction

The three requirements, i.e., communication independence, cyber security, reliability in the noisy environments, i.e., EMI, etc., were requested to apply wireless communication to nuclear power plants (NPPs) by United States Nuclear Regulatory Commission (US NRC) and the Oak Ridge National Laboratory [1]. While a wireless communication provides the convenience of using various application services such as mobility increases, there is the fundamental weakness of the empty space is open, not closed conductor transmission medium. Therefore, it can be vulnerable to a variety of cyber attacks such as man-in-the-middle attack (MITM), packet spoofing, packet injection, sniffing, unauthorized tapping and transfer. Also, electromagnetic interference (EMI) is another important factor to employ seldom wireless communication in the instrumentation and control system (I&C System) to perform safety function. The wireless communication technology has been only used for some of the communication and monitoring areas related to the non-safety function in NPPs. The cyber security plan (CSP) for employing the wireless communication is needed through cyber security evaluation to apply wireless communication system, such as mobile devices (e.g., smart phone, laptop, smart pad, etc.), in Han-bit NPP at Korea. Advanced NPP, such as APR1400 (Advanced Power Reactor 1400 MWe), employs the fully digitalized I&C systems for the advantage of digital feature, whereas the vulnerability (e.g., unauthorized malicious access, unintentional access) is increased. US NRC and Korea Institute of Nuclear Safety (KINS) request the cyber security policy and plan by establishing the cyber security program for the entire plant life cycle of NPPs through cyber security

\* Present address : 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, Korea
evaluation process of the vulnerability, design features, security requirements on the I&C systems which perform important functions[2-6]. In order to employ the wireless communication technology in safeguard function, licensees should assess and manage the potential for adverse effects on safeguard and safety functions so as to provide high assurance that critical functions are properly protected cyber attack. In this paper, we introduce the criteria establishment, related regulation and application environment analysis, threat and vulnerability analysis, and countermeasures. Also, final plan will be reflected in I&C CSP through future additional test-bed based security evaluation.

2. Cyber Security Plan
2.1. Application Environment of Wireless Communication in NPPs

In order to employ the wireless communication, firstly, application environment was surveyed and defined as follows in consideration of whether to apply low power of less than 100mW, acceptance of wireless devices as a countermeasure for the EMI.

(a) Communication type: Wi-Fi communication (IEEE 802.11) networks
(b) Transferring data type: audio (or video data)
(c) Using area: nuclear Power Block inside
(d) Connection status to critical digital asset (CDA)
   - Voice and Video: no connection to existing systems and I&C system through a separate network configuration
   - Variable data: two-way communication to the variable server which separately configured, or one-way communication from non-safety system
(e) No direct connection to the Safety system

2.2. Criteria Establishment for the Cyber Security Plan

Criteria for the wireless cyber security was established as follows to reflect the existing I&C systems cyber security program.

(a) Communication type: reflect the security measures for the connection portion with the wireless communications network to the I&C CSP
(b) Apply the latest technology with enhanced security features, such as authentication, encryption, WIPS (Wireless Intrusion Prevention System), etc.
(c) Derived to security measures, such as technical, management and operational control measures
(d) Create wireless CSP, taking into account the time factor

3. Analysis of Nuclear Cyber Security Regulation
3.1. Cyber Security Program and Regulation Analysis for the I&C Systems

In the United States, March 2009, US NRC required a high level of cyber security for the safety, security and emergency preparedness (SSEP) functions by revising 10CFR73.54, January 2010, Reg. Guide 5.71 was issued. Since 2009, NEI has developed a guideline to meet the requirements of 10CFR73.54 and issued NEI 08-09 Rev.6, which was endorsed by US NRC in 2010[5]. In Korea, KINS issued GT-N27, Reg. Guide 8.22 and has requested the cyber security activities [6]. Life-cycle of NPP consists of a variety of phases (e.g., concept, requirement, design, implementation, test, installation, operation and maintenance, retirement). I&C cyber security program consists of policy and plan documents and configured by management, operational, technical security controls, as shown in Figure 1. Recently, the following strategies are reflected in the CSP [7-8].

(a) CDA classification
(b) Defense-in-Depth protection strategy and graded approach to security levels
(c) Integration with physical protection program
3.2. Regulation Analysis for the Wireless Communication Systems

In January 2010, US NRC requested to ensure that the critical systems are adequately protected from cyber attack by issuing Reg. Guide 5.71 as follows. Although wireless communication is not used for SSEP functions, it must ensure no effect on the CDA by the wireless potential path [3].

(a) Only allowing wireless access through a boundary security control device and treating wireless connections as outside of the security boundary,
(b) Prohibiting the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions,
(c) Disabling wireless capabilities when not utilized,
(d) Establishing usage restrictions and implementation guidance for wireless technologies,
(e) Documenting, justifying, authorizing, monitoring, and controlling wireless access to CDAs and ensuring that the wireless access restrictions are consistent with defensive strategies and defensive models, and
(f) Conducting scans [no less frequently than once every week] for unauthorized wireless access points (AP), in accordance with this document, and disabling access points if unauthorized access points are discovered.

Also, KINS presents the assessment methodology and technical issues when applying wireless communication as follows, and requests to ensure that wireless communication does not affect the inherent function of CDA.

(a) Prohibiting the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions
(b) Permitting design the wireless CDA in non-safety systems, connection to the wire communication network by security control device, data transfer outside of the security boundary when only reliability is same as one of communication related to safety
(c) Do not use safety network when data are transferred from Level 4 to Level 3 in Figure 2 and do not use to play a decisive role.

![Figure 2. Architecture of cyber security defense-in-depth](image)


4.1. Vulnerability Analysis of the Wireless Communication

While wired equivalent privacy (WEP) based on the IEEE 802.11b standard has the number of exposed holes, the holes of Wi-Fi protected access (WPA) and WPA2 were complemented through IEEE 802.11i. Known vulnerabilities in terms of key setup and authentication, integrity, confidentiality and availability were reviewed, the example of analysis results is illustrated in Table 1

<table>
<thead>
<tr>
<th>Key setup, authentication</th>
<th>Type</th>
<th>Feature</th>
<th>Attack type</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SSID exposure</td>
<td>Unauthorized associations</td>
<td>Can access AP by copying the SSID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAC address exposure</td>
<td></td>
<td>Specifying with MAC address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(WEP) dependence on key setup mechanism same as shared SKA shared SKA28</td>
<td></td>
<td>Information collection attack by WEP key crack</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Example of threat analysis for the wireless communication

<table>
<thead>
<tr>
<th>Attack to internal network</th>
<th>Threat type</th>
<th>Details</th>
</tr>
</thead>
</table>
| Rogue AP                  | • Rogue AP connected to internal network  
• Use the wireless lan card in the company  
• Need to control the use of rogue AP by internal user |
| Soft-AP                   | • Use the Soft-AP by wireless lan card attached in PC  
• Hacking Soft-AP by outside hacker |
| Ad-Hoc Connection         | • Careless connection by internal user |
| Mis-Configured AP         | • Setting initialized AP  
• Mis-configured AP by manager |

Table 2. Example of vulnerability analysis for the wireless communication
4.2. Threat Analysis and Countermeasures of the Wireless Communication

The types of wireless threat are mainly attack to the internal network, authorized AP, outside AP by internal user, internal network by unauthorized outside user. Table 2 shows example of internal network attack in the threat analysis. The strategy which protect the connection with authorized AP by authorized user and control the connection with unauthorized, or authorized AP by unauthorized user, should be established, depending on the type of threat.

The countermeasures, which were reflected in the CSP, were configured by management, operational, technical security controls and those security controls were interconnected to employ defense-in-depth concept. For example, for the vulnerability of SSID (Service Set Identifier) broadcasting, technical controls (e.g., hidden SSID method, 802.1x authentication, WIPS (Wireless Intrusion Prevention System)), operational controls (e.g., periodic scanning, AP stopping) can be considered.

5. Conclusion

The cyber security program is being developed and applied in Korea NPPs not to affect inherent functions of I&C systems against the increase of cyber security threat and vulnerability due to application of digital technology. In order to take advantage of mobility and convenience by using wireless communication, cyber security evaluation is needed in terms of wireless communication itself and the connection portion with the wireless communications network to the I&C systems. Therefore, in this paper, we are establishing the wireless CSP through threat analysis, vulnerability analysis, countermeasures in the area of wireless communication to assess and manage the potential for adverse effects on safeguard and safety functions so as to provide high assurance that critical functions are properly protected cyber attack. It is expected that the safety and safeguard function, specifically on the area of real-time monitoring, logging, can be enhanced by employing the mobile devices (: smartphone, laptop, smart pad, etc). Proposed evaluation and design solution could be a basis for the design of wireless communication and mobile safety and safeguard systems in nuclear power plants.

REFERENCES