Application Methodology of Wireless Communication Technology for Nuclear Power Plants

Taejin Kim[1], Myunghoon Ahn[1], Jongsoo Kwon[1], and Joohwan Lee[1]

1. I&C department, KEPCO E&C, 111 Daedeok-daero 989beon-gil, Yuseong-gu, 34057, Republic of Korea (taejin0128@kepco-enc.com)

Abstract: Wireless communication technologies have been continuously studied due to their flexibility and cost efficiency in nuclear industry. In order to apply wireless technologies into nuclear power plants (NPPs) for communication purpose, electromagnetic Interference (EMI) with the installed instrumentation and control (I&C) equipment in NPPs should be considered. In this paper, we have investigated characteristics of various wireless technologies and proposed a Terrestrial Trunked Radio (TETRA) technology as an adequate wireless one for NPPs through rigorous review. Also, we suggest an applicable method to apply TETRA technology into NPPs by minimizing EMI on the existing equipment. Upon investigation of the I&C equipment in the Shin-Kori NPP Unit 3 (SKN3) which is the first-of-a-kind (FOAK) plant of advanced pressurized water nuclear reactor 1400 MW electricity (Advanced Power Reactor 1400, APR1400), the standards of RS103 in MIL-STD-461E and IEC 61000-4-3 are used for EMI testing. Based on the regulatory position in Reg. Guide 1.180, the exclusion zone is presented by calculation for the equipment qualified by RS103. To set up the exclusion zone of the equipment qualified by IEC 61000-4-3, the intensities of interference to the existing equipment for the test signals of RS103 and IEC 61000-4-3 are compared by analyzing the electric field intensities and the bandwidths of the test signal's spectrums. Moreover, electromagnetic waves from the wireless devices are simulated to compare the electric field intensities between free space and cabinet-installed environment.

Keyword: Wireless technology, Electromagnetic Interference (EMI), Terrestrial Trunked Radio (TETRA) technology

1 Introduction

Wireless technologies have been actively investigated to utilize them in NPPs because of their benefits. The benefits of wireless technologies in NPPs are (a) lowering the cost of cables and wires, (b) improving the flexibility of layout design of components and equipment without limitation of cable routing, and (c) shortening installation and maintenance duration.

Currently, wireless technologies, such as Wi-Fi (IEEE 802.11, IEEE 802.11b), VoIP (Walkie-talkie system), and wireless paging system, have been deployed for communication and monitoring purposes in a few nuclear power plants[1]. However, wireless technologies have not been applied yet to NPPs in Korea because of EMI concerns coming from wireless systems.

In this paper, an application methodology of wireless technology in NPPs is introduced only for communication purpose. TETRA technology is chosen as an appropriate wireless one through the review of current wireless technologies. The methodology to apply the TETRA technology is proposed by analyzing the case of SKN 3 NPP. The electric field change of the wireless system in free space based on Reg. Guide 1.180 is compared with that in cabinet-installed environment through simulation.

2 Wireless technology for NPPs

2.1 Comparison of various wireless technologies

Many wireless technologies are currently used in industries, so an user can have various options to choose a proper wireless technology depending on its purpose. Since most of state-of-the-art wireless technologies provide high performance, such as low power, broad coverage, high data rate, good connectivity, etc., security characteristics of wireless technologies become one of main factors to be considered in NPPs. After reviewing many different wireless technologies among personal area network (PAN) and local area network (LAN) which are adequate for plant network, Bluetooth (IEEE 802.15.1) and WiFi (IEEE 802.11) are chosen to be compared with TETRA in perspective of security.

In security perspective, there are six traditional security primers: authentication, encryption, confidentiality, authorization, non-repudiation, and availability.

Bluetooth is an open standard for short-range radio frequency communication to establish PAN[2]. Security review is conducted to Bluetooth 2.1 and earlier one since most of the available devices are implemented to these versions[3]. Bluetooth provides the following security services: authentication, encryption, confidentiality and authorization, but it is primarily vulnerable to all physical layer Denial of Service (DoS) at attack like channel jamming because it operates in the 2.4 GHz frequency band[2]. Moreover, non-repudiation is not provided by Bluetooth[2].

WiFi (IEEE 802.11) is broadly used for LAN. In order to provide enhanced security for wireless networks, IEEE 802.11i ratified on June 24th, 2004[2]. IEEE 802.11i provides the following security services: authentication, encryption, confidentiality, authorization, and non-repudiation[2][4], but it appears not to emphasize availability as a primary objective, leaving many DoS vulnerabilities[4].

TETRA is a European Telecommunications Standards Institute (ETSI) standard. It is utilized in a professional mobile radio and two-way transceiver. TETRA provides the following security services: authentication, encryption, confidentiality, authorization, and non-repudiation[5]. For wireless communication system, air interface security is a primary factor to be achieved. TETRA provides a very high level of air interface security through air interface encryption and end-to-end encryption[6]. Moreover, there are relatively low security risks on availability compared to Bluetooth and WiFi. They are primarily vulnerable to all physical layer DoS because they operates in the unlicensed 2.4 GHz Industry-Science-Medical (ISM) frequency band[2]. However, the standard frequency band of TETRA is low in the range of 380 MHz to 400 MHz unlike frequency bands of other wireless technologies.

Thus, we suggest the use of TETRA for wireless communication technology in NPPs. Table 1 shows the comparison of security characteristics among Bluetooth, IEEE 802.11i, and TETRA.

Table 1 Comparison of wireless technologies

Primers	Bluetooth	IEEE802.11i	TETRA
Authentication	△ 1)	O	O
Encryption	O	O	O
Confidentiality	O	O	O
Authorization	O	O	O
Non-Repudiation	x	O	O
Availability	△ 2)	△ 2)	O

1) Authenticating the communicating devices, but no user authentication
2) Weak availability

2.2 Main characteristics of TETRA

The core technologies used in the TETRA standard provide the following three inherent benefits: digital communication, trunking technique, and time division multiple access (TDMA) technology [7].

Digital technology provides constant good quality voice communication throughout the coverage area independent of RF signal strength. On the other hand, analog technology provides good quality voice communication in high signal strength areas but this gradually degrades down to poor voice quality in low RF signal strength area[7]. In perspective of security, the best form of voice security against eavesdropping is provided by using digitally encoded voice encryption algorithms[7].

Trunking technique brings about the automatic and dynamic assignment of a small number of communication channels shared among a relatively large number of users[7]. Besides spectrum efficiency, the dynamic and random allocation of channels makes it more difficult for a casual eavesdropper to monitor conversations[7].

Four time slot TDMA technology was adopted in TETRA. It inherently supports four independent communication channels, so it increases network capacity and radio frequency (RF) spectrum efficiency compared to frequency division multiple access (FDMA) technology[7]. In considering EMI, total electromagnetic emission level of TETRA devices is same with that of a TETRA device.

3 Methodology for application of TETRA into NPPs

3.1 Introduction of TETRA infrastructure

The TETRA infrastructure for communication is comprised of network components, antenna system, and portable terminals. In a plant, base station repeaters, which are network components, are installed for the air interface access of TETRA terminals to the system, and each repeater allocates time slots for TDMA to allow four communication channels for a pair of frequencies. Indoor omni-antennas in frequency band of 380 ~ 395 MHz[8] are used as an antenna system, and are located in various locations to provide full coverage throughout a plant. Portable handheld terminals in frequency band of 380 ~ 430 MHz[9] are used for operator communication. Figure 1 presents a TETRA infrastructure.

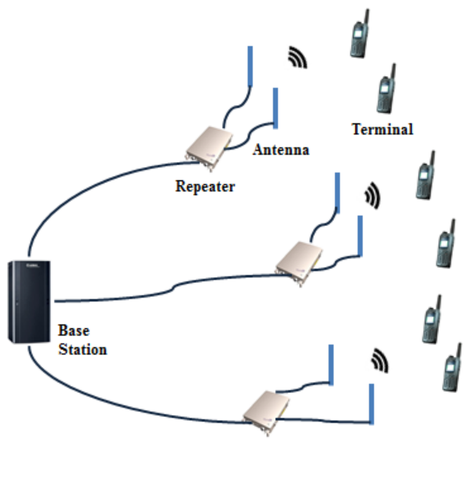


Fig.1 TETRA Infrastructure

The radiated electric field of TETRA components should be considered for administrative controls to prohibit the interference of electromagnetic wave emitters (Base Stations, Repeaters, Antennas, and Portable Terminals) in area where safety-related I&C systems are installed. For determination of minimum exclusion zones, the electric field emission levels of intentional emitters (Antennas and Portable Terminals) are considered.

3.2 NSSS I&C equipment in SKN 3

This paper for application methodology of TETRA sets bounds to NSSS I&C Equipment. To apply TETRA in nuclear power plants, it should be considered how NSSS I&C Equipment is susceptible to intentional emitters of TETRA.

NSSS I&C equipment can be categorized into safety I&C equipment and non-safety I&C equipment.

For electromagnetic qualification of susceptibility, all safety I&C equipment in SKN 3, which is the first Advanced Power Reactor 1400 (APR1400), complies with RS101 (Magnetic Field, 30 Hz ~ 100 kHz) and RS103 (Electric Field, 30 MHz ~ 1 GHz) in Reg. Guide 1.180, Rev.01[10]. However, RS101 is not considered in this case because low frequency range of RS101 is far from the radiated frequency range (380 ~ 430 MHz) of TETRA intentional devices. Thus, exclusion zones for safety I&C equipment are determined based on the equation suggested in Reg. Guide 1.180, Rev.01 and RS103 qualification results.

Most of the non-safety I&C equipment in SKN 3 is qualified to comply with IEC 61000-4-3. To set exclusion zones, a method for applying the equation of exclusion zone in Reg. Guide 1.180, Rev.01 to the non-safety equipment is introduced by analyzing the difference of test methods between RS103 and IEC 61000-4-3. Some of non-safety equipment are not qualified for susceptibility, so a recommendation is suggested to verify their susceptibility.

In perspective of susceptibility on NSSS I&C equipment, some representative I&C system in SKN 3 are selected and tabulated in Table 2 below.

Table 2 Status of susceptibility qualification for I&C systems in SKN 3

Classification	Equipment	Compliance with
Safety Equipment	PPS Cabinet	RG 1.180, Rev.01
	CPCS Cabinet	RG 1.180, Rev.01
	QIAS-P Cabinet	RG 1.180, Rev.01
	APC-S Cabinet	RG 1.180, Rev.01
Non-Safety Equipment	FIDAS Cabinet	IEC 61000-4-3
	DIS Cabinet	IEC 61000-4-3
	PHPPCU Cabinet	None
	APC-N Cabinet	None

3.3 Application to safety I&C equipment

3.3.1 Exclusion zone for safety I&C equipment

As mentioned above in Sections 3.1 and 3.2, the minimum distance of exclusion zones depends on the allowable electric field emission levels of intentional emitters (Antennas and Portable Terminals) designated for the area in the vicinity of the installed safety I&C equipment.

Reg. Guide 1.180, Rev.01 describes how to establish the minimum distance of an exclusion zone[10]. To establish the size of an exclusion zone, an 8 dB difference between the susceptibility operating envelope and the allowed emissions level should be maintained. For the radiated electric field operating envelope of 10 V/m (140 dBμV/m), the size of the exclusion zones should be set such that the radiated electric fields emanating from the EMI/RFI emitters are limited to 4 V/m (132 dBμV/m) in the vicinity of safety I&C systems. The minimum distance of an exclusion zone (d) in meters should be calculated by the following equation (1) derived from the free space propagation model:

$$d = \sqrt{30PG/E} \qquad (1)$$

where:

- d: Distance (meter)
- P: Effective radiated power of the EMI/RFI emitter (in watts)
- G: Gain of the EMI/RFI emitter (dimensionless)
- E: Allowable radiated electric field strength of the EMI/RFI emitter (in volts/meter) at the point of installation

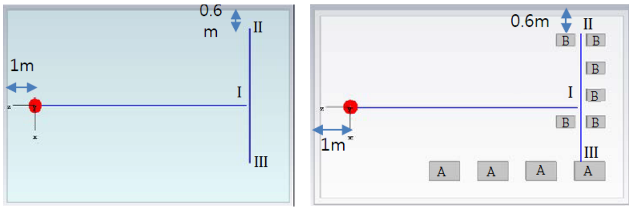
Since the safety I&C equipment is qualified according to Reg. Guide 1.180, Rev.01, allowable radiated electric field strength of the EMI/RFI emitter is set to 4 V/m. Assuming gain and power of an antenna compatible with repeater are 1.64 and 3 W respectively, the calculated distance for exclusion zone of the antenna is about 3.04 meters based on the equation (1). The distance for exclusion zone of a portable radio terminal is calculated as 1.83 meters when gain and power of the portable radio terminal are 1 and 1.78 W[9].

The minimum distances of an exclusion zone for all equipment comprising TETRA system are calculated. Antennas compatible with repeaters shall be installed for maintaining the distance from the safety I&C equipment, 3.04 m. The minimum distance of an exclusion zone for portable radio terminal is 1.83 m. The portable radio terminal carried by security personnel shall be administratively controlled considering the moving line of the security personnel. The exclusion zone for the TETRA system needs to be determined by identifying the actual location of cabinets and measuring the distances among building structures and cabinets.

3.3.2 Simulation of electric field propagation

The susceptibility qualification test of RS103 in Reg. Guide 1.180, Rev.01 is conducted in free space, but there are many installed cabinets in operating environment of TETRA system in nuclear power plants. Thus, there is a distinction of electric field propagation between in free space and in operating environment of TETRA system.

In order to compare propagation characteristics of electromagnetic wave, electric field intensity is simulated both in free space and in virtual I&C equipment room using the Computer Simulation Technology (CST) microwave studio which is a specialist tool for the three dimensional electromagnetic simulation of high frequency components. The spatial configuration of simulation is shown in Figure 2, and the condition of simulation is enumerated in Table 3.



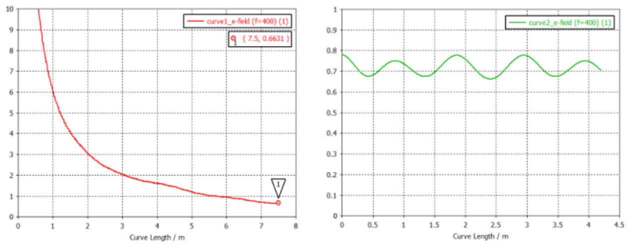
a) Free space b) I&C equipment room

Fig.2 Configuration of simulation

Table 3 Condition of simulation

Factors	Description
Frequency for analysis	400 MHz
Dipole antenna	37.5 cm, Vertically polarized wave
I&C equipment room	6 m×2.5 m ×10 m
A cabinet	1 m ×0.6 m ×1.8 m (0.6 m between cabinets)
B cabinet	0.6 m ×0.4 m ×1 m (0.4 m between cabinets)
Wall structure	20 cm (Thickness) 4.5 (Relative dielectric constant)

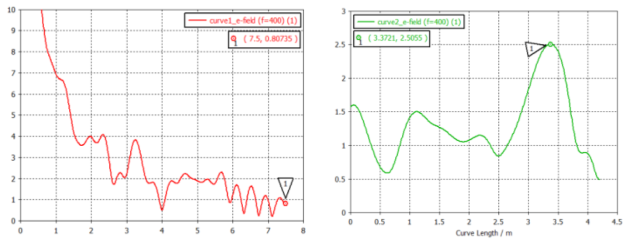
As electromagnetic wave propagates point I in Figure 2-a), the intensity of electric field is inversely proportional to square of distance in free space according to Maxwell's equations. Between point II and III, the electric field is uniformly distributed in sine form as shown in Figure 3, which demonstrates the simulation result in free space.



a) Antenna to Point I b) Point II to Point III

Fig.3 Simulation result in free space

In I&C equipment room, the intensity of electric field, like in free space, is reduced inversely proportional to square of distance as electromagnetic wave propagates point I in Figure 2-b), but electromagnetic wave exhibits diffraction, interference, and reflection. Moreover, the intensity of electric field between point II and point III is severely fluctuated. The maximum intensity of the electric field between point II and point III in I&C equipment room is about three times larger than that in free space. This phenomenon occurs because electromagnetic wave interferes, and then is diffracted, and refracted by installed cabinets and wall structure. Figure 4 shows the simulation results in I&C equipment room.



a) Antenna to Point I b) Point II to Point III

Fig.4 Simulation result in I&C equipment room

When considering the intensity of the electric field between antenna and point I, the intensity difference of electric field between in free space and in I&C equipment room is less than 8 dB which is the margin between the susceptibility operating envelope and the allowed emissions level.

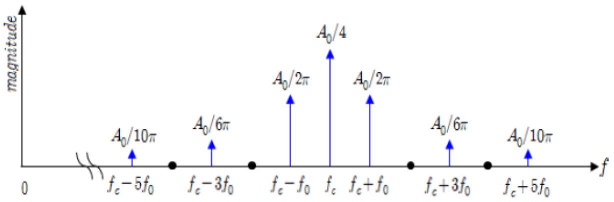
In the line between point II and point III, intensity difference of electric field between in free space and in I&C equipment room is higher than 8 dB margin. However, the region near the line is included in the exclusion zone so portable terminals of TETRA are not allowed to be used in that region.

3.4 Application to non-safety I&C equipment

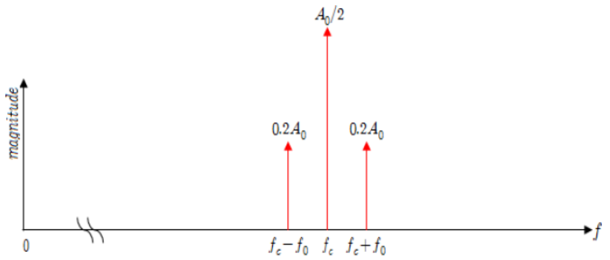
3.4.1 Comparison on interference power of test signals between RS103 and IEC 61000-4-3

As shown in Table 2, most of the non-safety I&C equipment are qualified according to IEC 61000-4-3. To apply an exclusion zone suggested in Reg. Guide 1.180, Rev.01 to non-safety I&C equipment, it is required for equipment qualified by IEC 61000-4-3 to compare a tolerance of electromagnetic field interference with equipment qualified by RS103. Thus, spectrum characteristics and interference powers of both susceptibility test signals of RS130 and IEC61000-4-3 are analyzed and compared in this section.

The test signal of RS103 has 1 kHz square wave with a duty cycle of 50%[10], and the test signal of IEC 61000-4-3 has 1 kHz sine wave with a modulation depth of 80%[11]. To perform the spectrum analysis, these modulated signals are expressed in frequency domain as shown in Figure 5.



a) RS103



b) IEC 61000-4-3

f_c : Carrier frequency

f_o : Frequency of the modulated signal

Fig.5 Susceptibility test signals in frequency domain

In comparison of spectrum characteristics, test signal of RS103 is distributed on the wide frequency range but test signal of IEC 61000-4-3 is focused on the frequency f_c and $f_c \pm f_o$. If an operating band of equipment is narrow, the interference power of IEC 61000-4-3 test signal is more intense than that of RS103 test signal.

To compare the interference power of test signals, operating bands of equipment for RS103 test signal are divided to i) $f_B < f_0$, ii) $f_0 \le f_B < 2f_0$, iii) $2f_0 \le f_B < 4f_0$, iv) $2f_0 \le f_B < 4f_0$, v) $4f_0 \le f_B < 6f_0$, and vi) $6f_0 \le f_B$. Also, operating bands of for IEC 61000-4-3 test signal are divided to i) $f_B < f_0$, ii) $f_0 \le f_B < 2f_0$, and iii) $2f_0 \le f_B$. Based on the band divisions, the interference powers of test signals are calculated using equation (2), and the calculation results are shown in Table 4.

$$P = (E_{peak}/\sqrt{2})^2 = (E_{rms})^2 \qquad (2)$$

where:

P: Interference power

E_{peak}: Intensity of maximum electric field

E_{rms}: Intensity of RMS electric field

Table 4 Comparison of interference power

Operating band of equipment	Normalized RS103 interference power [A: mag.]	Normalized IEC 61000-4-3 interference power [B: mag.]	B/A [dB]
$f_B < f_0$	0.0625	0.25	6.02
$f_0 \le f_B < 2f_0$	0.0878	0.29	5.2
$2f_0 \le f_B < 4f_0$	0.1131		4.7
$4f_0 \le f_B < 6f_0$	0.1160	0.33	4.5
$6f_0 \le f_B$	0.1188		4.4

1) $A_0 = \sqrt{2}$: RMS value of carrier amplitude are normalized to 1

2) f_0 = 1 kHz : modulation frequency

As shown in Table 4, if the carrier levels are the same, the power of the IEC 61000-4-3 test is 6.02~4.4 dB higher than that of the RS103 test. In other words, it is the testing result under more severe conditions.

Based on this, the interference level of the IEC 61000-4-3 test is converted to the interference level of the RS103 test and expressed as a calibration factor given by the equation (3).

$$Cal.fac.[dB] = E_{IEC} - E_{RS103} + B/A|_{table\ 4}\,[dB] \qquad (3)$$

where:

E_{RS103}: Signal strength of RS103 signal

E_{IEC}: Signal strength of IEC61000-4-3 signal

B/A: Converted value in Table 4

Based on Reg. Guide 1.180, Rev.01, test field is set to 10 V/m (RMS value = 7.07 V/m) and tolerance level is set to 4 V/m (RMS value = 2.83 V/m). Using the equation (3), the calibration factor for IEC 61000-4-3 tolerance test results (Electric field: 10 V/m) is calculated as shown Table 5.

Table 5 Calibration factor of IEC 61000-4-3 with respect to RS103

Operating band of equipment	E_{IEC} [dB] - E_{RS103} [dB]	B/A [dB]	Elec.field. Cal.fac. [dB]
$f_B < f_0$		6.02	9.02
$f_0 \le f_B < 2f_0$		5.2	8.2
$2f_0 \le f_B < 4f_0$	3	4.7	7.7
$4f_0 \le f_B < 6f_0$		4.5	7.5
$6f_0 \le f_B$		4.4	7.4

To set the exclusion zone of the equipment tested in accordance with IEC 61000-4-3 on the basis of Table 5, the calibration factor of exclusion zone is calculated. In order to obtain the calibration factor of exclusion zone, the electric field calibration factor in Table 5 is converted to magnitude, and the allowed radiated field strength is multiplied by the converted magnitude. Thus, the calibration factor of exclusion zone is obtained as shown in Table 6.

Table 6 Calibration factor of exclusion zone

Operating band of equipment	E_{IEC} [dB] - E_{RS103} [dB]	B/A [dB]	Elec.field. Cal.fac. [dB]
$f_B < f_0$	9.02	2.82	0.35
$f_0 \le f_B < 2f_0$	8.2	2.57	0.39
$2f_0 \le f_B < 4f_0$	7.7	2.43	0.41
$4f_0 \le f_B < 6f_0$	7.5	2.37	0.42
$6f_0 \le f_B$	7.4	2.34	0.43

Based on the result in Table 6, equipment tested at level 3 of IEC 61000-4-3 has passed the test of 2.34 to 2.82 times harsh conditions. Therefore, the immunity is considered so strong enough. That is, it is not affected by the interference even if the distance of the exclusion zone is reduced by 0.35 to 0.43.

3.4.2 Consideration of non-safety I&C equipment not EMC qualified

In order to consider interference of TETRA devices to non-safety I&C equipment not EMC qualified, it is divided into two cases.

Some of non-safety I&C equipment has sufficient immunity to electromagnetic waves. In case of PHPPCU cabinet in Table 2, it consists of relatively less sensitive devices against electromagnetic waves such as silicon controlled rectifier, relay, transformer, fan, etc. Thus, there will be no malfunction due to electromagnetic waves from TETRA devices.

In case of the other equipment which is subject to electromagnetic waves, it is considered to evaluate sensitivities for each device consisting of the equipment. For example, APC-N cabinet in Table 2 includes drawers of radiation monitoring system, reactor coolant pump shaft speed sensing system, etc. The drawers can be affected by electric field emission from TETRA devices, so the sensitivity of the drawers should be evaluated. Thus, a methodology for sensitivity evaluation is suggested herein.

For sensitivity evaluation, the malfunction resistance level of the equipment should be estimated in perspective of both the conductive interference and the radiated interference.

To establish the conductive interference, the electromagnetic waves coupled to the conductor should be analyzed. The analysis process is as follows: i) A transmission line model of the line with installation environment is constructed, ii) the electric field strength incident to the line, iii) the interference signal applied to the pin of the equipment in the line is extracted, iv) the interference voltage applied to the semiconductor device located closest to the pin is extracted, v) the interference voltage on the semiconductor device is compared with the malfunction threshold of the device, and vi) the analysis process is performed at the carrier frequency of both uplink and downlink of TETRA.

To establish the radiated interference, the radiated interference power to the target equipment should be analyzed. The analysis process is as follows: i) The strength of the electromagnetic field distributed inside the enclosure containing the equipment is obtained by electromagnetic wave simulation tool, ii) the interference voltage across the Printed Circuit Board (PCB) loop from the distributed field is extracted, iii) the interference voltage applied to the semiconductor devices constituting the loop is extracted, iv) the interference voltage on the above semiconductor device is compared with the erroneous operation threshold of the device, and v) the analysis process is performed at the carrier frequency of both uplink and downlink of TETRA.

If the threshold value of the field intensity entering the line and equipment is determined from the erroneous operation threshold of the weak semiconductor device through the above procedure, the exclusive zone can be adjusted according to the output of the antenna and the terminal so as not to exceed the threshold value.

4 Conclusion

In order to apply wireless technologies to NPPs for communication purpose, proper wireless technology must be selected and EMI with the installed I&C equipment must be considered.

Since most of wireless technologies provide high performance, such as low power, broad coverage, and good connectivity, etc., security characteristics become an important factor to select an adequate wireless technology for NPPs. TETRA provides robust security functions in perspective of authentication, encryption, confidentiality, authorization, non-repudiation, and availability compared to other wireless technologies.

When TETRA devices are used in NPPs, electromagnetic interference generated by TETRA devices to the installed I&C equipment can be prevented by setting exclusion zones. For safety I&C equipment, all equipment in SKN 3 are qualified according to Reg. Guide 1.180, Rev.01, so exclusion zones are calculated according to the equation (1). By complying with exclusion zones, safety I&C equipment can be protected from electromagnetic waves of TETRA devices. For non-safety I&C equipment, most of the equipment in SKN 3 are qualified according to IEC 61000-4-3. To utilize the equation (1) based on Reg. Guide 1.180, Rev.01, RS103 test in Reg. Guide 1.180, Rev.01 and IEC 61000-4-3 test must be compared in perspective of susceptibility. Thus, the calibration factor of exclusion zone for the equipment tested by IEC 61000-4-3 is calculated by comparing the interference power of RS103 test signal and IEC 61000-4-3 test signal. For other equipment which is not EMI-qualified, a methodology for sensitivity evaluation is suggested. If threshold value of the field intensity is determined by the methodology, the exclusion zone can be adjusted not to exceed the threshold value.

By setting exclusion zones in NPPs, TETRA can be utilized for wireless communication without any problem to I&C equipment. Moreover, managerial control, such as procedure, warning sign, training, etc., must be accompanied to prevent workers and operators from making human errors.

References

[1] IEC TR 62918, Edition 1.0, “Nuclear power plants – Instrumentations and control important to safety – use and selection of wireless devices to be integrated in systems important to safety”, July 2014.

[2] Gunther Lackner, “A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX”, International Journal of Network Security, Vol.15, No.6, pp.420-436, 2013.

[3] K. Scarfone and J. Padgette, “Guide to Bluetooth Security”, Tech. Rep., 2008.

[4] C. He and J. C. Mitchell, “Security Analysis and Improvements for IEEE 802.11i”, in Proceedings of the 12th Annual Network and Distributed System Security Symposium, pp.90-110, 2005.

[5] ETSI ETR086-3, “Trans European Trunked Radio (TETRA) System; Technical Requirements Specification – Part 3: Security Aspects”, 1994.

[6] “TETRA Security”, tandcca.com/fm_file/tetra-security-pdf, TETRA Association, 2006.

[7] “TETRA Technology Advantages & Benefits”, tandcca.com/fm_file/technology-benefits-pdf, TETRA Association, 2006.

[8] “BSF 3094 Specification”, www.cobhamwireless.com/wp-content/uploads/BSF3604_rev-A.pdf, Axell Wireless, Ltd.

[9] “Airbus TH9 Handheld Terminal Datasheet”, datasheets.globalspec.com/ps/4557/AirbusGroup/12B9E5AA-7816-4233-AADC-35091A12B934.

[10] USNRC Regulatory Guide 1.180, Rev.01, “Guidelines for Evaluating Electromagnetic and Radio-frequency Interference in Safety-related Instrumentation and Control Systems”, 2003.

[11] IEC 61000-4-3, Edition 3.1, “Electromagnetic Compatibility (EMC) – Part 4-3: Testing and Measurement Techniques – Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”, 2008.