The Development of a Scientific Evaluation System of Force-on-Force (FOF) Exercise for Performance-based Regulation in Nuclear Security

Moonsung Koh, * Myungtak Jung
Korea Institute of Nuclear Nonproliferation and Control (KINAC, 1534 Yuseong-daero, Yuseong-gu, Daejeon 305-348, Republic of Korea)
**Corresponding author: mskoh@kinac.re.kr*

1. Introduction

Nuclear facilities contain radioactive materials, strategically important systems, as well as equipment and supplies. This situation offers an opportunity for the unauthorized removal of material or sabotage. Therefore, in order to implement physical protection measures at a nuclear facility, a licensee is required to invest in equipment, system, and security guards based on the Act on Physical Protection and Radiological Emergency (APPRE).

A terrorist attack or sabotage at a nuclear facility could lead result in a great amount of loss of life and social chaos, in addition to serious radiological damage.

As threats have been evolved more intelligent, divergent, advanced, the international societies including IAEA encourage for all member states to establish the performance-based regulation using Force-on-Force (FOF) exercise, computer simulation.

Consequently, the performance evaluation for physical protection at nuclear facilities should focus on properly reacting to threat scenarios. Physical protection should also include detecting, blocking, delaying, interrupting including the human and technical factors the adversary having malicious intention of the realistic main threat element before he accomplishes the goal based on Design Basis Threat (DBT). However, Korea's standardized training and evaluation system cannot be applied to real situations and there are limitations to propose a valid performance evaluation result about the physical protection with an objective data.

A FOF exercise is a performance-based inspection designed to assess licensee's capability to protect their facility against sabotage. Any potentially significant deficiencies identified during this inspection is to be promptly corrected by the licensee

The purpose is to evaluate the effectiveness of a licensee's security plans against a series of attack scenarios by a simulated commando-style adversary force seeking to exploit potential deficiencies in the plant's defensive strategy. During this mock exercise, an adversarial force attempts to reach and destroy enough safety equipment to set in motion an accident that would damage a reactor core or spent fuel pool, and potentially causing a release of radiation to the environment. The nuclear power plant's security force, in turn, would seek to interdict the adversary force and prevent them from reaching the safety equipment.

The main purpose of this paper is to establish performance-based regulation by developing a scientific evaluation system of FOF exercise. This paper introduces the development of engagement equipment and evaluation systems for FOF exercise at nuclear facilities.

2. Status on the implementation of FOF in NRC

The Nuclear Regulatory Commission (NRC) has carried out FOF exercises regularly at commercial operating nuclear power plants since 1991 as part of its comprehensive security program. However, they are not pass/fail inspections. They are the primary means to evaluate and improve the effectiveness of plant security programs to prevent radiological sabotage as required by NRC regulations (10 CFR Part 73).

FOF exercises assess a nuclear plant's physical protection to defend against DBT. A full FOF exercise, spanning several days, includes both table-top drills and simulated combat between a mock commando-type adversary force and the nuclear plant security force. During the attack, the adversary force attempts to reach and damage key safety systems and components that protect the reactor's core (containing radioactive fuel) or the spent nuclear fuel pool, potentially causing a radioactive release to the environment. The nuclear power plant's security force, in turn, seeks to stop the adversaries from reaching the plant's equipment and causing such a release.

2.1 Before September 11, 2001

Before the September 11, 2001 terrorist attacks in the USA, the NRC conducted security exercises at all 65 nuclear plant sites nationwide. These exercises were conducted at about eight sites per year. Immediately after the 11 attacks, nuclear plants went to their highest level of security.

FOF exercises were temporarily halted after the September 11 attacks because they would have distracted plant security forces. Instead, NRC security staff focused on strengthening and monitoring security improvements that nuclear power plants made in response to commission advisories.

2.2 Changes Since 9.11

After September 11, 2001, the NRC strengthened its security programs, while reevaluating its DBT and improving FOF exercises. In one of its key decisions, the commission decided to increase the frequency of security exercises starting in the fall of 2004, so that NRC could evaluate FOF exercises at each plant site once every three years- (with tactical security drills in the intervening years).

The NRC redesigned its FOF program after more than two years of testing at almost two-thirds of the nuclear power plants in the country. An expanded table-top exercise program was conducted during 2002; and an expanded FOF exercise program was carried out during 2003.

In February 2004, the NRC began a transitional FOF program that incorporated lessons learned from the previous two years. It also used characteristics of a supplemented DBT that had expanded adversary force capabilities. In accordance with a commission order issued in April of 2003, all nuclear power plant operators had to be able to meet the requirements of the supplemental DBT. These requirements altered the type of possible threats and attacks that the plants had to be able to deter, by October 29, 2004. All plants met this requirement.

2.3 Current FOF Program

In November 2004, the NRC began implementation of its full-scale FOF program that incorporates experience and lessons learned since September 11, 2001. The NRC increased the frequency of FOF exercises. Each nuclear power plant site will conduct an NRC evaluated exercise at least once every three years, rather than once every eight years, with tactical response security drills in the intervening years. The current FOF program reflects the supplemented DBT and significantly increases the level of realism, while ensuring the safety of both plant employees and the public.

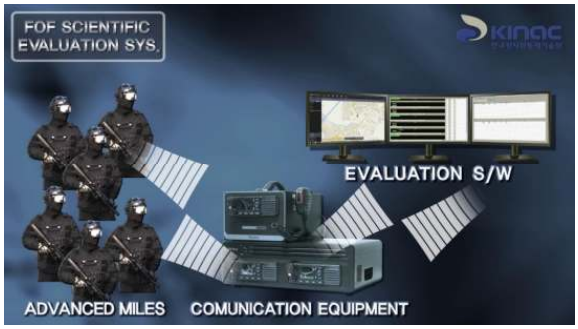
With regard to the conduct of the exercises, the NRC notifies plant operators in advance of FOF exercises. This is done for safety and logistical purposes and to provide adequate time for planning the coordination of efforts between the two of security officers--one for maintaining actual security and the other for participating in the exercise.

In preparation for a FOF exercise, information from table-top drills, inspections, and security plan reviews are used to design a number of commando-style attacks seeking to probe for potential deficiencies in the defensive strategy. The aim of the site's defenders is to keep the attackers from destroying or damaging key equipment. Any potentially significant deficiencies in the protective strategy identified during the FOF exercises are promptly reviewed and fixed.

3. Engagement and Telecommunication System

As mentioned above, a FOF exercise is all-encompassing performance evaluation system for an entire physical protection system (Detection, Delay, and Response) for a nuclear facility. In order to introduce FOF exercises, KINAC got started the project to develop the FOF system.

The system is composed of a variety of sophisticated communication and computer devices. These include, first, the advanced MILES (Multiple Integrated Laser Engagement System) can be used for simulating attacks and protection. Second, a DMR-based telecommunication control system enables the transmission of real-time drill situations and voice communication between the players and the control room. Third, software that can be used for saving, analyzing, and evaluating all data sent to the central communication control system.



3.1 Development of Engagement System (MILES)

The advanced MILES is composed of a SAT (Small Arms Transmitter) player unit, detector set, and effects simulator.

Among these, a SAT for a rifle offers convenience and economic efficiency when using electronic blank fire--which is simulated ammunition. Next, a player unit was manufactured in the form of a combat vest, which incorporates a detector set, effects simulator, and communication equipment. The detector sends real-time voice and location information within a radius of 2 km in combination with the DMR.

3.2 Telecommunication system (DMR)

Central communication control equipment is Data Mobile Radio, that is, DMR equipment, and is composed of 3 parts: Mobile DMR, MD equipment in charge of monitoring the voices of virtual attackers and nuclear power plant protection personnel, and the location tracking of all players, and various drill data signals.

3.3 Scientific Evaluation S/W (DMR)

Basically, the FOF will be conducted with over 50 response forces at night. In order to evaluate the FOF exercise, the scientific tool should be need to gather all kinds of data such as time, detection signals, communication signals, engagement results, moving paths, etc. Also, the evaluation tools should be needed to analyze the data and identify the vulnerable factors. So, we developed three types of software that are used to evaluate FOF exercisers.

First, an intrusion and response monitoring software is used to display intrusion and response situations, such as detection, delay, and response from the start of the FOF to its end on screen. It also creates a database.

Second, location tracking software displays the real-time location of players at certain intervals and tracks their routes using GPS.

Lastly, combat situation information management software remotely controls each player and records the condition of participants in the drill (e.g., death, wounds, and physical condition).

It carries out a function that can compare and analyze information in connection with GPS information, combat situation information software, and event monitoring after a drill is finished through the scientific evaluation software. As a result of evaluation, the KINAC will figure out the findings and recommendations which will be measured by the licensees.

Currently, a FOF scientific evaluation system is at a stage where a product trial of combat equipment and evaluation software has been developed. Also, KINAC plans to establish an applicable system in 2015.

In the future, we intend to quantitatively evaluate FOF exercises by using the DB of three kinds of software through the development of evaluation programs. Moreover, the institute intends to develop a system that can deduce and improve weaknesses in a physical protection system

4. Summary

Force-on-Force (FOF) training is an essential part of a nuclear facility's security program. With this development, we can construct a FOF system that can imitate a real situation by using a simulated adversary team. It can also be used to construct a system that can objectively and quantitatively evaluate an entire physical protection system.

After the completion of the FOF evaluation system, KINAC will evaluate, and later strengthen its overall security program in response to changes in the threat environment, technological advancements, and lessons learned. As a result, substantial improvements to a nuclear facility's security can be predicted. These improvements will focus on a plant's security force, physical barriers, intrusion detection systems, surveillance systems, and access controls.

Through the building a Force-on-Force scientific evaluation system, KINAC will establish an efficient physical protection implementation system for nuclear energy facilities. This system will also earn the trust of people, both here and abroad, who are concerned about the use and misuse of nuclear energy.

REFERENCES

[1] 2012 Report to congress on the security inspection program for commercial power reactors and category I fuel cycle facilities: Results and Status Update, NUREG-1885, Rev.6, NRC, 2012.
[2] NRC Oversight of security at NPP needs to be strengthened, GAO, 2003.
[3] Nuclear Power Plant Security and Vulnerabilities, CRS, 2010.
[4] Nuclear Security Recommendation Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.5, IAEA, 2011.