Nuclear Engineering and Technology 54 (2022) 2011–2022

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Development of a method for securing the operator's situation awareness from manipulation attacks on NPP process data

Chanyoung Lee [a], Jae Gu Song [b], Cheol Kwon Lee [b], Poong Hyun Seong [a, *]

[a] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291, Gwahak-ro, Yuseong-gu, Daejeon, 34141, South Korea

[b] Korea Atomic Energy Research Institute,111, Daedeok-daero 989 Beon-gil, Yuseong-gu, Daejeon, 34057, South Korea

ARTICLE INFO

Article history:
Received 31 July 2021
Received in revised form
11 October 2021
Accepted 7 December 2021
Available online 10 December 2021

Keywords:
Cyber attack response
Manipulation attacks on process data
Control theory-based system analysis
Adaptive Kalman filter
Hardware in the loop system

ABSTRACT

According to the defense-in-depth concept, not only a preventive strategy but also an integrated cyberattack response strategy for NPPs should be established. However, there are limitations in terms of responding to penetrations, and the existing EOPs are insufficient for responding to intentional disruptions. In this study, we focus on manipulative attacks on process data. Based on an analysis of the related attack vectors and possible attack scenarios, we adopt the Kalman filter to detect process anomalies that can be caused by manipulations of process data. To compensate for these manipulations and secure MCR operators' situational awareness, we modify the Kalman filter such that it can filter out the effects of the manipulations adaptively. A case study was conducted using a hardware-in-the-loop system. The results indicated that the developed method can be used to verify whether the displayed safety-related state data are reliable and to implement the required safety response actions.

1. Introduction

Nuclear instrumentation and control (I&C) systems are designed to secure the performance and safety of nuclear power plants (NPPs) against a variety of potential physical disturbances and unexpected system failures. In recent decades, digital I&C systems have replaced analog I&C systems of NPPs. Digital I&C systems offer multiple benefits such as high reliability, high-speed calculation, easy application of useful functions through software, and large data capacity [1]. Moreover, the use of digital technologies ensures accurate and timely data flow between digital control components that are physically distributed in NPPs. In addition, it facilitates real-time and partially automatic control of nuclear I&C systems. However, the application of digital networks and heterogeneous digital components leaves NPP I&C systems vulnerable to cyberattacks. In many cases, as listed in Table 1, cyberattacks on NPPs have been possible even when they are separated from the external network. Therefore, to address the cybersecurity of NPPs, nuclear regulatory agencies and standards organizations have published cybersecurity guidelines, for instance, the US Nuclear Regulatory Commission (NRC) published RG 5.71 [2] and Korea Institute of Nuclear Nonproliferation and Control (KINAC) published RS-015 [3]. The International Atomic Energy Agency (IAEA) has published several technical guidance documents to guide the correct application of cybersecurity techniques to nuclear facilities [4–6]. These guidelines focus on the prevention of, detection of, and response to criminal or intentional unauthorized acts involving or directed at nuclear materials, other radioactive materials, associated facilities, and associated activities. In the emerging domain of nuclear cybersecurity research, the focus has been on prevention rather than detection and response. Several methods have been developed to quantitatively assess cyber risks or identify critical digital assets (CDAs) [7,8]. In addition, several methods have been developed to evaluate the effectiveness of cybersecurity controls [9,10]. However, preventive measures are not always effective against technologically evolving cyberattacks [11]. Moreover, ineffective preventive measures cannot be upgraded immediately given the operating conditions of NPPs [12]. Even robust preventive measures can be breached easily due to information leaks or malicious insiders. Therefore, preventive measures alone are insufficient to adequately secure NPPs against cyberattacks, and a systematic cyberattack detection and response strategy must be established to

* Corresponding author. Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291, Daehak-ro, Yuseong-gu, Daejeon, 34141, South Korea.

E-mail addresses: lcy5228@kaist.ac.kr (C. Lee), jgsong@kaeri.re.kr (J.G. Song), cklee1@kaeri.re.kr (C.K. Lee), phseong@kaist.ac.kr (P.H. Seong).

https://doi.org/10.1016/j.net.2021.12.011

Table 1
Cyber security incident cases in nuclear facilities.

Year	Country	Plant	Incident Description
2003	U.S.A	Davis Besse	Slammer Worm Attack
2006	U.S.A	Brown Ferry	Control Network Overload
2008	U.S.A	Hatch	Shut Down after S/W Upgrade
2010	Iran	Natanz	Stuxnet Attack
2014	Japan	Monju	Malware Attack
2016	Germany	Gundremmingen	Infection of Computer Virus
2019	India	Kudankulam	Malware Attack

supplement the prevention strategies.

After the failure of prevention measures, a cyberattack can be described as a sequential process that continuously compromises the attack conditions and gradually achieves the attack goals. This sequential cyberattack process can be divided into the penetration and disruption phases [13]. In the penetration phase, attackers try to compromise the target systems by collecting sensitive data, illegally gaining privileges, and moving laterally by following vulnerable attack paths. In the disruption phase, attackers try to affect plant operation by stopping or adversely affecting various control functions. To deter the progress of cyberattacks in NPPs, detection and response strategies must be established based on the defense-in-depth concept [14]. Defense-in-depth can be achieved in multiple ways. From a security architecture perspective, it involves setting up multiple security boundaries to protect CDAs and networks from cyberattack. In this way, multiple protection levels of mechanisms must fail for a cyberattack to progress and impact a critical system or network. Therefore, defense-in-depth is achieved not only by implementing multiple security boundaries, but also by instituting and maintaining a robust program of security controls that assess, protect, respond, prevent, detect, and mitigates an attack on a CDA and with recovery. Recently, a network intrusion detection system for NPPs has been developed [15], and statistical techniques have also been used to detect attacks that can bypass the conventional detection techniques [14]. In addition, the IAEA published a technical guideline for operators to detect and analyze cyberattacks and for supporting the establishment of appropriate response strategies [16]. With this regard, a method for estimating the security states of NPPs [17] and a cyberattack response support system [18] were developed using probabilistic graph analysis methods. Nevertheless, there remains the possibility that an advanced and persistent cyberattack can transition from the penetration phase to the disruption phase without being stopped.

Unlike industrial control systems, NPP I&C systems are designed with multiple manual backup functions for system protection. Additionally, safety-related backup functions are also designed to operate on analog platforms that cannot be affected by cyberattacks [19]. Thus, when presented with an anomaly, the main control room (MCR) operators are required to recognize only the current situation by checking plant process variables and implement necessary actions by following emergency operating procedures (EOPs). However, if information processing systems or information display systems are affected by intentional system disruptions, operators may fail to recognize the current situation and cannot implement the required actions in a timely manner. In 2003, the Davis–Besse NPP was infected with a Slammer worm that propagated through the supervisory control network [20]. This worm disrupted plant operation by generating spurious network traffic, and safety-related information remained unavailable for 5 h. In 2009, a uranium enrichment facility in Natanz was attacked by the Stuxnet virus [21]. As the attackers were destroying the centrifuges, the operators were provided with incorrect information, which prevented them from implementing manual protection actions.

To secure NPPs against cyberattacks, it is essential to establish an integrated cyberattack response strategy that includes not only security response strategies against adversary penetrations but also safety response strategies against intentional system disruptions in connection with the existing EOPs. However, the existing EOPs were developed for use in the event of I&C system function failure, and they do not address the maloperation of systems, where the root cause may be malware or compromised computers [16]. Therefore, the EOPs should be extended to allow operators to verify the integrity of safety-related process data and correct any detected manipulations. In this study, we focus on securing the operators' situational awareness in the event of a cyberattack and developing a method that MCR operators can use to identify manipulated data and estimate the current plant process status securely during a cyberattack.

The remainder of this paper is organized as follows. In Chapter 2, we analyze manipulation attacks on NPP process variables. The possible impact of cyberattack-induced operator failures and potential attack vectors for manipulations of plant process data are analyzed. In addition, some detectable symptoms of the manipulations are extracted. Chapter 3 explains the adaptive Kalman filtering algorithm, which adjusts the uncertainty of process state data based on the size of their estimation residuals. In Chapter 4, a case study is conducted to validate the developed method. Finally, Chapter 5 summarizes this study.

2. Analysis of manipulation attacks on NPP process variables

2.1. Analysis of operator failures caused by cyberattacks

A technical guidance published by the IAEA explained how cyberattacks can affect the control and protection functions of nuclear I&C systems [22]. Based on the guidance, cyberattacks can be classified into five types depending on how they affect nuclear I&C systems [23]. The first includes cyberattacks that cause protection failures. Cyberattacks that prevent the triggering of actuation signals from protection systems can lead to severe accidents in NPPs. These attacks aim to actively deter and prevent the expected alarms and responses corresponding to various NPP process statuses. Attackers may modify or update the system control logic or even outright prevent responses by implementing a denial-of-service attack. The second type includes cyberattacks that causes control failures. If cyberattacks target a digital controller, the related actuation components can be disabled, even if the control signals continue to be generated. Attackers disrupt the control logic and adversely affect the physical processes being controlled by the target systems. The targets of interest may include active procedures or control parameters that manipulate physical processes. Moreover, these attacks can include prevention or manipulation of reporting elements and control logic. The third includes cyberattacks that cause operator failures. As observed in the Three Mile Island accident, operator errors due to wrong information led to a severe accident [24]. Therefore, if cyberattacks target the man–machine interface system (MMIS) to indirectly cause operator errors, such as errors of omission (EOO) or errors of commission (EOC), NPP safety could be threatened in certain scenarios. The fourth includes cyberattacks that cause physical component failures. These cyberattacks aim to damage the control components by overworking them or operating them in undersigned ways. The Stuxnet accident revealed that physical components can be damaged due to cyberattacks on digitalized controllers [21]. The last type includes cyberattacks that can cause initiating events considered in nuclear risk assessments, such as a loss of coolant accident (LOCA) or station blackout (SBO). These initial events can be caused by a combination of the second and fourth cyberattack

types.

Herein, we focus on cyberattacks that cause operator failures through manipulations plant process data. Because incorrect operator actions have the same effect as the failure of NPP safety components, they have been considered as basic events in the probabilistic safety assessment models [25]. Operators cannot react properly unless appropriate information provided, as is considered for example, in the diagnosis step in the Korean standard human reliability assessment [26]. Likewise, in the event of a display failure due to a cyberattack, wrong actions may be initiated due to failure of the operator's cognitive process. Therefore, this scenario can be described as a loss of situational awareness due to a cyberattack. This is a special scenario intended by an attacker, and it differs from conventional human error analyses. In a previous study, operator failure scenarios that can be induced through manipulations of NPP process variables were analyzed with an assumption that operators have been trained to strictly follow EOPs [27]. In addition, the following types of cyberattack-induced human errors were identified, and core damage scenarios involving these types of human errors were developed.

- Failure to implement specific manual steps: If the display presents misleading information that the conditions required to implement a manual step are unsatisfied, the operator cannot implement the step and eventually commits an EOO.
- Inappropriate termination: An operator could turn off the automatically initiated safety components when the display indicates that the termination conditions pertaining to specific operations are satisfied.
- Combination of signal generation failure and operator action failure: Several safety functions are designed to be started automatically by an actuation signal originating from the safety system, and the operator is then required to confirm that the corresponding components are working as intended.
- Failure to implement specific EOP, and inappropriate termination of EOP: The first step in any target EOP is to check the entry condition, which should include plant condition and the status of the corresponding safety components.
- Failure to follow proper EOP steps: Several steps in the procedure might be overlooked simultaneously.

2.2. Analysis of attack vectors for manipulating NPP process variables

In NPPs, plant process information is provided through the I&C system, which consists of safety systems, control systems, MMIS, and other actuation and operating support systems [28]. The MCR operators typically obtain plant process information through the MMIS, which comprises operator consoles and large display panels. The MMIS is implemented on a non-safety-grade platform. Unlike non-safety systems assembled using commercial products, safety systems for NPPs are put together using special programmable logic controllers. In addition, these safety systems are developed considering the stringent cybersecurity regulatory requirements for NPPs. For these reasons, non-safety-grade systems might be more vulnerable to cyberattacks than the safety systems [27].

If an attacker infiltrates an non-safety system and compromises the MMIS, the operator can be deceived by misinformation and may take inappropriate actions. In addition, since the digital signals of process data are processed by the information processing system (IPS) before being displayed to the operators via the MMIS, damage on the IPS also enables the data manipulation attacks. The possible routes and attack vectors toward the MMIS and IPS, and related systems were investigated in a previous study [29]. The previous study suggested an NPP I&C system-specific method to obtain attack vectors, where the supervisory control network, malicious insiders, external devices, and external media were identified as attack entry points. Malware or malicious activities can be extended to CDAs through supervisory control networks. Insiders may access CDAs for operation, maintenance, and testing. External devices or systems may be used for maintenance and testing. The external devices connected to CDAs can modify or delete the programs installed in the CDAs. Moreover, external media can be connected to CDAs directly or indirectly through external devices. External media can access engineering work stations or other computing devices to transfer and execute malicious code for modifying system software or causing system malfunction.

An attacker with access to non-safety systems, such as the MMIS and IPS, and knowledge of the system specifications can discover exploitable vulnerabilities by referring to the national vulnerability database (NVD) [30]. By exploiting such vulnerabilities, they can escalate their own privileges, launch denial of service attacks, and disclose sensitive information. An attacker who can exploit such vulnerabilities can misinform operators or withhold information from them. This may interfere with the operator's situational awareness. For example, in the Maroochy attack, the attacker temporarily shut an operator out of the network, preventing them from viewing the system state [31]. In the Stuxnet attack, the attacker manipulated the view of operators replaying process input and manipulated the I/O image to evade detection and inhibit protection functions [21]. Industroyer is a sophisticated piece of malware designed to affect the working processes of the ICS used in electrical substations [32]. This malware can block serial COM channels temporarily, causing a denial of view. The OPC module of Industroyer can also brute force values and send out a status which equates to “Primary Variable Out of Limits” for the target systems, thereby misdirecting the operators from understanding the protective relay status. Industroyer was allegedly used in the attacks on the Ukrainian power grid in December 2016 [33]. Some of Norsk Hydro's production systems were infected with LockerGoga [34]. This caused a loss of view that forced the company to switch to manual operations.

2.3. Analysis of cyberattack scenarios for manipulating NPP process variables

An attack resource-based security analysis framework is adopted to analyze possible cyberattack scenarios in NPPs [35]. In this

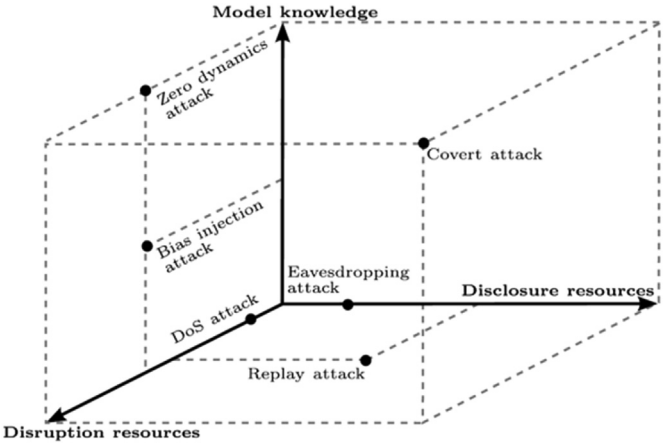


Fig. 1. The Cyber Attack Space [35].

framework, cyberattack scenarios can be captured and qualitatively classified in the attack space shown in Fig. 1. Three dimensions of the attack space were proposed: prior system model knowledge, disclosure, and disruption resources. Prior model knowledge can be used by the attacker to design more sophisticated attacks, possibly ones that are more difficult to detect and have more severe consequences. Similarly, disclosure resources enable attackers to obtain sensitive information about the system during an attack by violating data confidentiality. Note that disclosure resources alone cannot disrupt system operation. By contrast, disruption resources can be used to affect system operation, for example, through violations of data integrity or availability properties. We analyze several attack scenarios, each requiring different amounts of attack resources and system knowledge.

DoS attacks prevent plant process information from reaching operators and cause loss of situational awareness. Although the absence of data packets is not stealthy, because it is trivially detectable, DoS attacks can be misdiagnosed as poor network condition. Although no disclosure resources are needed in the actual implementation of DoS attacks, the required disruption resources correspond to the data channels that the attacker can render unavailable. To implement DoS attacks, prior knowledge of the system model is not needed. In replay attacks, the attacker first performs a disclosure attack by gathering sequences of data and starts to replay the recorded data. Although replay attacks with access to all measurement data channels are stealthy, these attacks are not guaranteed to be stealthy when only a subset of the data channels is attacked [36]. In this case, the stealth constraint may require the attacker to have additional knowledge of the system model. The required disclosure resources correspond to the data channels that an attacker can eavesdrop. Specifically, the attacker can only tamper the data channels from which data has been previously recorded. A covert attack requires high levels of system knowledge and considerable disclosure and disruption resources [37]. The covert agent calculates the effect of malicious command actions on plant measurements and subtracts those effects from the measurements. Usually, a feedback structure is designed and implemented so that the objectives can be specified with respect to the plant measurements. Any plant or control action constraints that must be respected are considered when designing the covert feedback controller. It is imperative for the covert agent to remain undetected, and to this end, extensive attack resources and sophisticated plant knowledge are required.

In this study, we consider cyberattack scenarios that are designed with malicious intent to drive an NPP into an unsafe state without the attacker being detected [35]. Fastidious cyberattack scenarios designed with sophisticated plant knowledge and implemented with abundant attack resources are fatal to plant safety and difficult to detect. Even though sufficient mitigation functions are designed in NPPs, they may become unresponsive. However, we assume that the attacker's plant knowledge is not perfect, and the amounts of compromised disclosure and disruptive resources are limited. It is impossible for an attacker to have complete knowledge of the complex dynamics of the NPP physical systems. In addition, because NPP I&C systems are designed with multiple security zones and levels and are managed by means of physical measures, attackers cannot utilize attack resources indefinitely without limitations [7]. Therefore, attackers face limitations in terms of manipulating all safety-related process data simultaneously. Moreover, it is difficult to maintain physical correlations between the manipulated process data and unaffected data. These anomalies in the process data can be detected by operators with sufficient NPP system knowledge. However, the manual process for operators to identify and restore these anomalies is labor-intensive, time-consuming. and error-prone. Normally, operators do not perform a given task while verifying the integrity of plant process data. In addition, the manipulations can continue to change unpredictably over time, space, and scale, so an operator's observations may have limitations. Heavy information flow to human operators or low coincidence with their knowledge will degrade their monitoring performance [38,39]. Because NPP operators tend to barely consider the possibility of a cyberattack, this type of anomaly is highly likely to be misdiagnosed as a simple sensor failure [40]. Therefore, it is necessary to develop a support system that can secure the operators' situational awareness when some of the displayed process data are manipulated by cyberattacks.

3. Development of method for securing Operator's situational awareness

3.1. Modeling Operator's NPP system knowledge

MCR operators perceive plant process data from IPS and MMIS connected with the SCN. From the point of view of control dynamics, the received process data is classified into state variables and control variables. State variables are variables that are directly related to physical phenomena such as temperature and pressure. A control variable is a variable related to the operations of control components, such as the flow rates of feed water pumps or the heater power. For the performance and safety of NPPs, the state variables must be kept within certain acceptable ranges. The safety states of NPPs can be estimated based on how far the state variables deviate from the acceptable ranges and how close they are to the safety limit [41]. And cyberattacks that cause safety-related state variables to deviate far from the normal ranges are evaluated as more dangerous attacks for NPPs [42]. Therefore, the current EOPs are designed for the operators to check the safety-related state variables and take appropriate mitigation actions. In order to keep the safety-related state variables within the normal range even in case of physical disturbance or unexpected events, the digital controller generates field control signals and the control components operate accordingly. The operations of control components influence the process state variables following the laws of physics and system dynamics. This is a natural phenomenon that cannot be manipulated by cyberattacks. In this study, it is assumed that the operators have sufficient knowledge of the physical interactions, and a control theory-based system analysis framework is used to model the operator's plant system knowledge [43]. The physical plant system is modeled as a discrete-time state space $\boldsymbol{P}$. An operator's plant system knowledge consists of A, B, and C. They can be represented as matrix values in the context of multiple input and multiple output (MIMO) systems.

$$P : \begin{cases} x_{k+1} = Ax_k + Bu_k + w_k \\ y_k = Cx_k + v_k \end{cases}$$

where x_k is the system state variable at time k, u_k denotes the control variables of control components, and y_k denotes the process state variables. The unexpected process disturbance and measurement noise, w_k and v_k respectively, represent the discrepancies between the plant system model and the real situation due to the unmodeled dynamics of disturbances. MCR operators with sufficient knowledge of the plant systems estimate and assess the current system state using the given process data, like as described in Fig. 2. Herein, we do not consider general communication failures, such as process data loss and delay. However, the operator's situational awareness can be affected by malicious manipulations of process data, $a_k = [\Delta y_k, \Delta u_k]$. In such a case, the operators may erroneously change the control components or implement inappropriate manual actions, which may physically damage the plant.

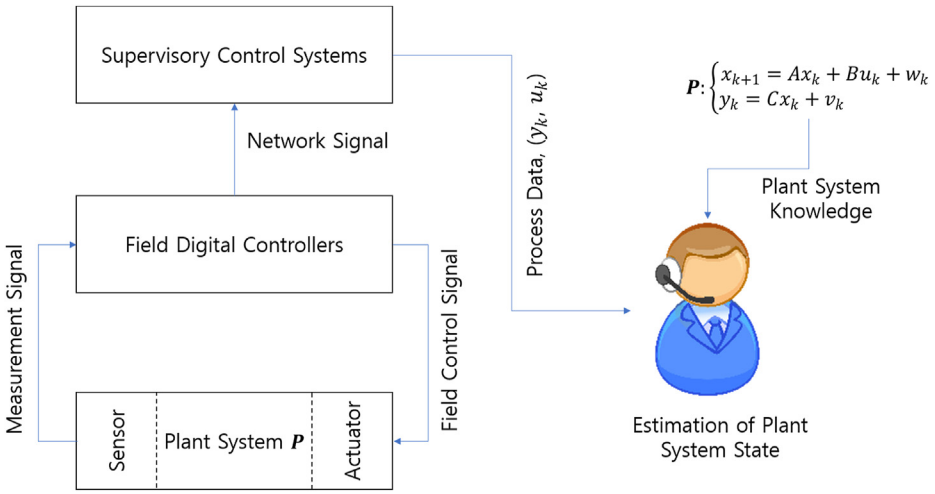


Fig. 2. Plant system state estimations by MCR operators.

The effect of manipulation attacks on the operator's observational situational awareness can be modeled as follows:

$$\tilde{y}_k = y_k + \Delta y_k$$

$$\tilde{u}_k = u_k + \Delta u_k$$

3.2. Making assumptions about the control variables

The I&C systems with hierarchical architectures measure the states of physical processes by using sensors and operate control components to maintain the performance and stability of NPPs. In this study, by referring to the Purdue enterprise reference architecture [44], we divide the network structure of I&C systems into three levels. The I/O network level includes the actual physical processes and the sensors and actuators that are directly connected to process equipment. The field control network (FCN) level includes the functions involved in sensing and manipulating physical processes. The typical devices at this level are programmable logic controllers (PLCs), distributed control systems, safety instrumentation systems, and remote terminal units. The supervisory control network (SCN) level includes the functions associated with monitoring and controlling physical processes and the general deployment of systems such as MMIS, engineering workstations, and historians. To realize distributed control process, field control signals originating from digital controllers are transmitted and processed in the field control network (FCN). The FCN and digital field controllers are classified as safety-related systems according to the standards of the Nuclear Energy Institute (NEI) [45]. Safety-related structures, systems, and components refer to the structures, systems, and components that are required to remain functional during and following design basis events to ensure the following:

(1) Integrity of the reactor coolant pressure boundary;
(2) Capability to shut down the reactor and maintain it in a safe shutdown condition;
(3) Capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures.

According to the nuclear regulation guide [46] and the IAEA technical guidance [5], the highest security level should be given to safety-related systems. Security level is an abstraction that defines the degrees of security protection required by various computer systems in a facility. Each level in a graded approach will require different sets of protective measures to satisfy the security requirements of that level. Some protective measures apply to all computer systems in all levels, while others are specific to certain level(s). Moreover, according to the nuclear cybersecurity regulatory guide [46], only one-way data flow is allowed from high security level to low security level. Initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited. Data only flows from one level to other levels through a device or devices that enforce security policy between each level.

This study deals with the manipulations of process data delivered to the operators by compromising the MMIS or IPS connected to the SCN. And these attacks alone are difficult to affect the FCN and field digital controllers that have been given higher security levels. In addition, in the field of nuclear I&C systems, several soft-sensing techniques were developed that can estimate control variables using field control signals transmitted through FCN [47,48]. A method for restoring missed or damages control variables was also developed [49]. These methods make it possible for operators to monitor whether the control or protection components are operating properly when some control variables are unavailable. In this study, it is assumed that methods for estimating control variables using field control signals have already been deployed in NPPs and that the integrity of displayed control variables are continuously checked.

3.3. Adopting the Kalman filtering algorithm

In this study, the Kalman filter [50] is adopted for developing a method to secure operators' situational awareness against process data manipulation attacks. In statistics and control theory, Kalman filtering, also called linear quadratic estimation (LQE), is an algorithm that uses a series of measurements obtained over time, including statistical noise and other inaccuracies, and produces estimates of unknown variables that tend to be more accurate and secure than those based on a single measurement by estimating a joint probability distribution over the variables in each timeframe. The Kalman filter is a recursive algorithm for online system state estimation. It uses the state estimate and control variables from the previous timestep to estimate the current state $\hat{x}_k^-$. In addition, estimation covariance P_k^- is generated using the previously

estimated covariance and the covariance of the process control variables Q.

$$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1}$$

$$P_k^- = AP_{k-1}A^T + Q$$

The predicted state estimate $\hat{x}_k^-$ is called the a priori state estimate because although it represents an estimate of the state in the current timestep, it does not include current observations of the process state variables. Once the process state variables are observed, these estimates are updated using a weighted average, where a higher weight is assigned to the estimates with higher certainty. The difference between the current a priori prediction and the current observation is multiplied with the optimal Kalman gain K_k considering the estimation covariance P_k^- and covariance of the process state variables R. The difference is combined with the previous state estimate to refine the state estimate.

$$K_k = \frac{P_k^- C^T}{CP_k^- C^T + R}$$

$$\hat{x}_k = \hat{x}_k^- + K_k(y_k - c\hat{x}_k^-)$$

$$P_k = (I - K_k C)P_k^-$$

This improved estimate based on the current observation is called the posteriori state estimate $\hat{x}_k$, and it is used to produce an a priori state estimate for the next timestep.

The Kalman filter runs in real time by using only the present process data, previously estimated system state, and its uncertainty. Because the estimates obtained using the Kalman filter tend to be more accurate than those based on a single measurement and because the filter can be used to estimate unmeasurable system states, the Kalman filter has been applied to coordinate response actions [51] and to detect and isolate system faults [52]. Recently, the Kalman filter has been used to detect not only faults but also false data injection attacks [53]. The Kalman filter was used to detect multiple faults individually and to determine whether they are caused by cyberattacks or not [54]. The efficiency of the Kalman filter was assessed in both stealthy and non-stealthy attack scenarios [55]. The difference between an observed process state variable and its estimate is defined as an estimation residual. Under normal conditions, the estimation residuals are not reactive. However, the estimation residual of a state variable tends to increases when the pattern of state variable is not contextually linked to other state variables or control variables. It also tends to increase when its estimation residual patterns cannot be well explained using dynamic models. Therefore, a state variable with a high estimation residual is highly likely to be manipulated by a cyberattack. Here, an increase in the estimation residual can be used as a signal to provide warnings about cyberattacks.

This approach can help with the detection of cyberattacks that cannot be detected using intrusion detection techniques from the IT domain [56]. In addition, the detection information can be directly linked to diagnostic information, which can help NPP operators to immediately identify the affected physical processes and respond to potential damages. In addition, because the proposed approach does not warrant any system modification and does not affect system performance, it may have fewer side effects. However, zero-dynamic attacks can bypass this detection technique [57]. In zero-dynamic attacks, the attack signals are designed such that the estimation residual does not change. In other words, these attacks are decoupled from the measurements of the closed-loop linear system. In general, their design depends on sufficient knowledge of the plant, controller, and anomaly detector dynamics. However, in the previous chapter, we assumed that it is impossible for an attacker to have complete knowledge of the complex dynamics of NPP physical systems, and attackers cannot utilize disclosure and disruptive resources indefinitely without constraints.

3.4. Modifying the Kalman filtering algorithm

The existing Kalman filter uses covariance matrices R and Q to reflect the uncertainty of the process state and process control variables on the system state estimation. Fixed values are assigned to parameters of the matrices by considering the sensing process, physical properties, and data statistics. Therefore, when certain process state variables are manipulated by cyberattacks, the manipulated values cannot be filtered out, which introduces noise in the system state estimation. In particular, the lower the uncertainty of a manipulated state variable, the more severe is its effect on the system state estimation. Operators cannot determine which state variables have been manipulated based on less reliable estimations. Therefore, the Kalman filter has been used to check for the occurrence of a process data manipulation attack, but it cannot be used to identify which value has been manipulated [58]. Herein, we modify the existing Kalman filter that relies on fixed covariance matrices to be more adaptive. This modification is based on the fact that the influences of some variables on the system state estimation can be reduced by increasing the uncertainties of the variables. As mentioned earlier, state variables with high estimation residuals have a higher likelihood of being manipulated in cyberattacks. By increasing the uncertainty of the process state variables that are suspected of being manipulated, the system state estimations can be more secured. However, it cannot be concluded that all state variables with high estimation residuals have been manipulated by cyberattacks. This is because the estimation residuals of unaffected state variables can also increase indirectly when they are strongly linked with manipulated state variables. Therefore, the estimation residual-based identification approach for manipulated state variables requires one to analyze the changes in estimation residual patterns with updates to the associated uncertainty levels.

Fig. 3 shows the feedback process of the adaptive Kalman filter. The process consists of checking the estimation residuals of state variables and adjusting their uncertainty levels depending on the patterns of their estimation residuals. The two blocks on the left

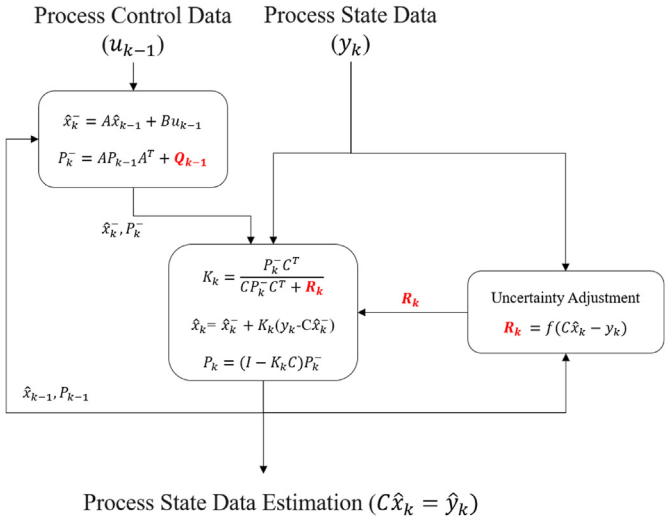


Fig. 3. The adaptive Kalman filtering algorithm.

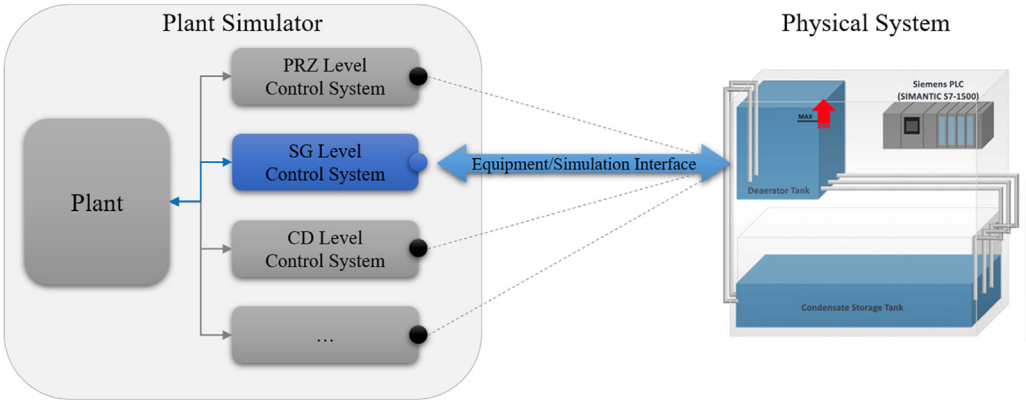


Fig. 4. Operation modes of the HIL system.

describe the existing Kalman filtering algorithm. By estimating the system state x_k with the Kalman filter, NPP operators can recognize the current plant system states more accurately. Here, the estimation residual is the difference between the estimated state variable $C\hat{x}_k$ and the measured state variable y_k. To reduce the influence of variables with large estimation residuals on the system state estimation, the matrix R is updated to increase the uncertainty of the state variables. This action can reduce the effect of variables being suspected as manipulated on the system state estimations. The level of uncertainty of a state variable that continuously generates large estimation residual is adjusted to be higher, and the level of uncertainty of a state variable that generates small estimation residual is adjusted to be lower. In this manner, the process of checking the estimation residual and updating its uncertainty is iterated several times. By repeating this process, the effects of process data manipulations on the system state estimation can be attenuated gradually. In addition, by comparing the observed process state variables with the estimated values, the manipulated variables can be identified, and MCR operators' situational awareness can be secured. However, the function $f(C\hat{x}_k - y_k)$ that determines the magnitude of uncertainty adjustment associated with suspect process state data, and it will be addressed in a future study.

The developed adaptive Kalman filter can securely estimate the state variables, even in unpredictable process data manipulation attacks. In addition, it is possible for NPP operators to implement the required safety response measures based on the securely estimated system states. However, in a situation in which the integrity of the control variables cannot be guaranteed or in a situation in which more than half of the state variables are manipulated, the reliability of the state estimation may be deteriorated. Further studies are needed to address these limitations.

4. Case study

4.1. Application of hardware-in-the-loop system

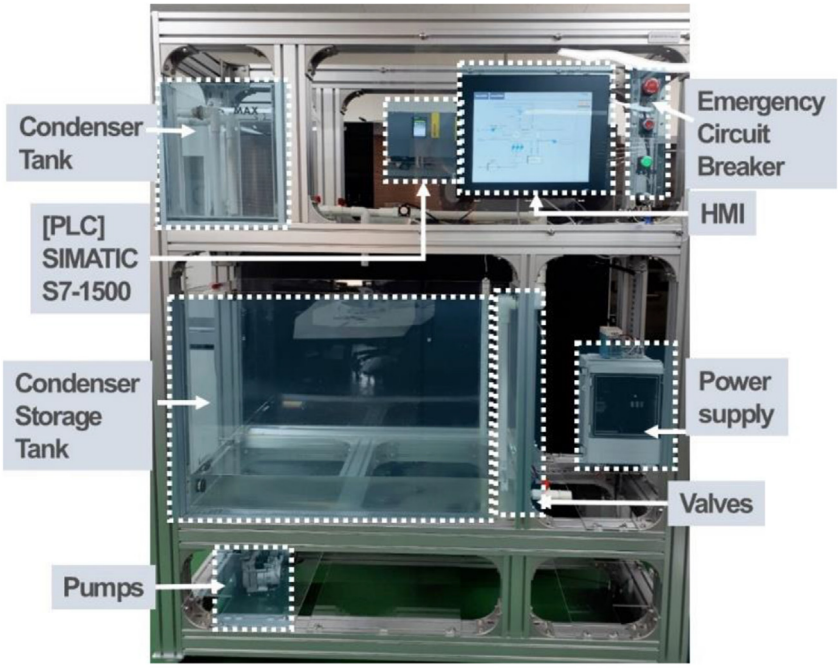
To validate the developed adaptive Kalman filter, an NPP simulator that can implement cyberattack scenarios and generate plant process data accordingly is needed. However, the existing NPP simulators cannot implement cyberattack scenarios or provide the necessary data. To address this limitation, a hardware-in-the-loop (HIL) system which had been constructed for NPP cybersecurity research [59] was used in this case study. The HIL system includes an NPP simulator based on a hypothetical NPP called *Asherah*. The *Asherah* NPP simulator was developed by coupling PARCS/RELAP5 with the high-performance language MATLAB/Simulink [60]. A supervisory system that allows MATLAB/Simulink to oversee the nuclear codes for exchanging online data was implemented. The preliminary simulation results obtained by deploying realistic cyberattack scenarios facilitated an understanding of the effects of cyberattacks, how they propagate in nuclear digital cyber-physical systems, and their consequences in terms of plant security and safety [61].

In addition to the *Asherah* NPP simulator, the constructed HIL system consists of control components, such as PLCs, digital pumps, and digital valves. The HIL system transmits the measured process state values to the simulator and controls the control variables in line with the control logic. The deployed PLC controls the physical components by using two control channels, as illustrated in Fig. 4 [62]. Control channel 1 is used to synchronize the physical systems with the operation of NPP simulator, and control channel 2 is used to operate the physically implemented control components. Owing to the use of two types of control channels, the simulator and physical components are integrated and synchronized to operate in a manner similar to a real plant. This integration provides access points for cyberattacks and allows attackers to obtain plant process data and digital signal data. Owing to the flexibility of the interface module used in the HIL system, the PLC can be assigned as any control system in the hypothetical NPP depending on the cyberattack scenario and can be used for cyber impact analysis [63]. This expands the scope of demonstrable cyberattack scenarios. The scalable communication module of the HIL system facilitates cooperation with other testbeds that have differently configurations or are in remote locations. This helps users to simultaneously implement multiple cyberattack scenarios. A human–machine interface (HMI) is mounted on the HIL system. The HMI displays the plant state and the operational states of the control components and generates manual command actions. Fig. 5 (a) shows the local HMI deployed for displaying process states related with the HIL system, and Fig. 5 (b) shows the MCR simplified for operating the Asherah NPP simulator. By using the local HMI and the simplified MCR, the behaviors of MCR operators in the event of a cyberattack can be analyzed.

4.2. Experiment design

In this case study, the HIL system was used as the pressurizer (PRZ)-level control system of the *Asherah* NPP simulator. In the *Asherah* NPP simulator, the PRZ level is controlled using the makeup and letdown valve flows, which are controlled using a control system in which the reference level was programmed as a function of the reactor coolant temperature [61]. The chemical and

(a)



(b)

Fig. 5. (a). The HIL system with local HMI (b). The simplified MCR

volume control system is used to oversee the reactor coolant system inventory, inject water when the PRZ level is low or open the letdown valve when the coolant level is high, and provide water to the pressurizer spray to control the reactor pressure. The PRZ level control logic used PI compensators. The PRZ level control logic was designed to operate automatically. An old version of EOP was also assumed that guides operators to operate the makeup or letdown valves manually when it is judged that there is an anomaly in the PRZ level control process.

To implement the developed adaptive Kalman filter algorithm, a state-space model of the PRZ-level control system is required. The state-space model can be constructed using system design specifications, but it is difficult to obtain the system design specifications of the NPP simulator. For this reason, the model was estimated using simulation data obtained under normal conditions. By using the a toolbox developed by *MathWorks* for estimating a state-space model [64], we developed a state-space model of the control system and control components and trained it using the simulation data. Fig. 6 displays the validation results of the constructed models. A new version of EOP was assumed that guides operators to check safety-related state variables when estimation residuals from the adaptive Kalman filter exceed a threshold. The PRZ level

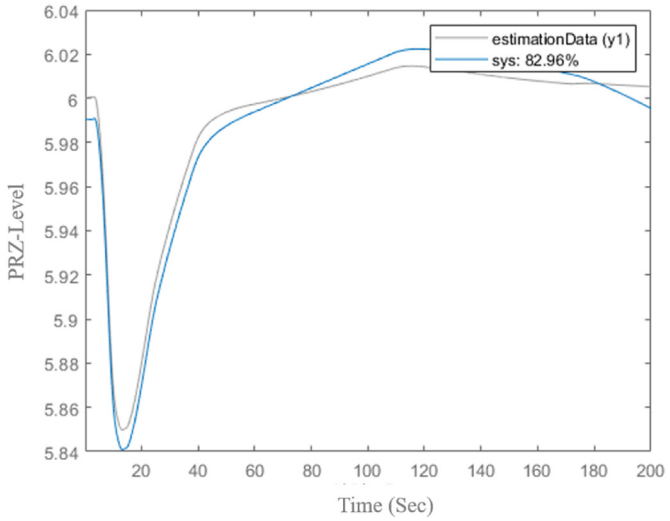


Fig. 6. Validation of the state space model.

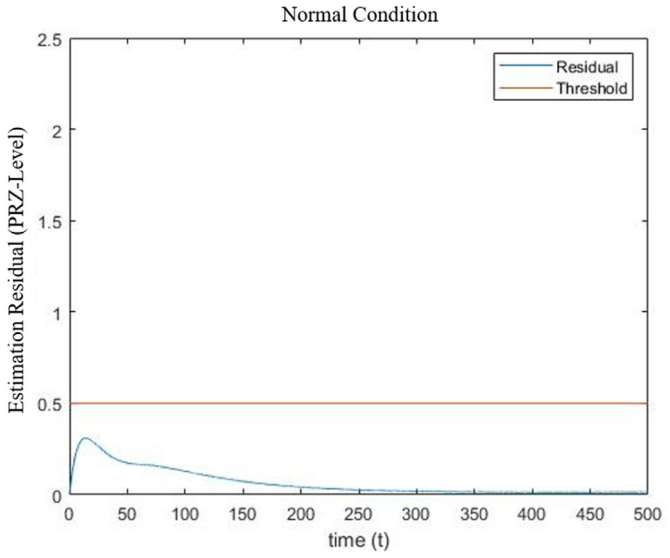


Fig. 7. Estimation residual under normal condition.

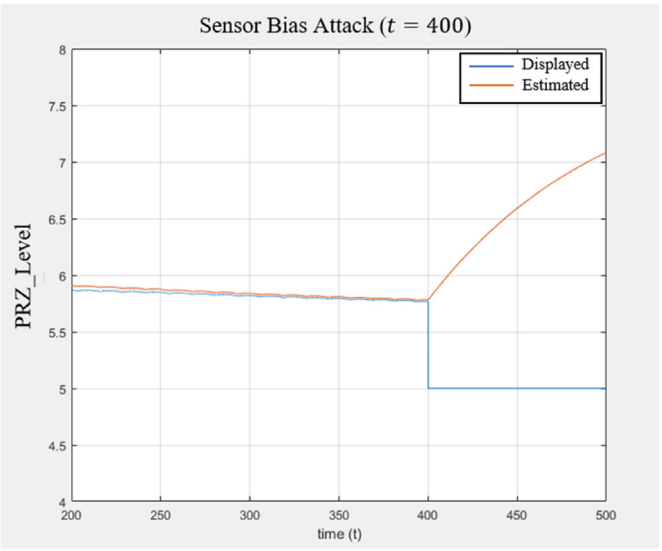


Fig. 8. PRZ level under sensor bias attack.

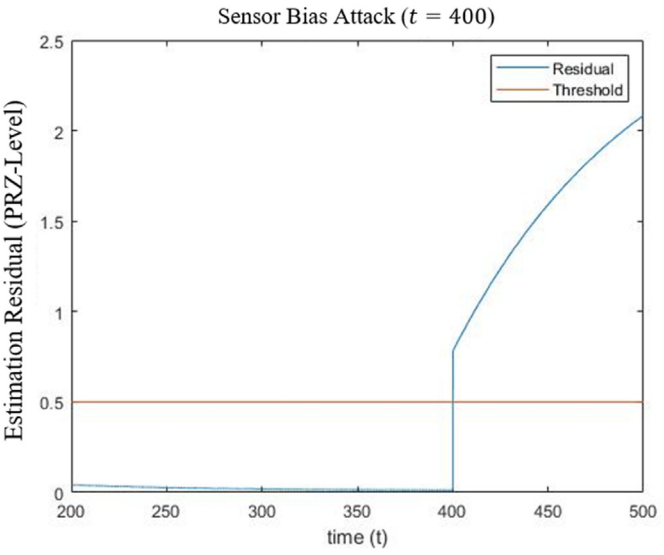


Fig. 9. Estimation residual under sensor bias attack.

estimation residual in the normal scenario is shown in Fig. 7. In this study, when the estimation residual of the PRZ-level data was within 0.5 m in a given scenario, the scenario was considered normal. When the residual exceeded 0.5 m, the PRZ-level data of the scenario was considered to be manipulated.

In this case study, we used a cyberattack scenario developed and implemented in the IAEA ITC program [65]. In the scenario, related vulnerabilities were discovered and malicious codes were exploited for manipulating several safety-related process variables such as PRZ level. By using switch credentials, an attacker enabled port mirroring (Switch Port ANalyzer - SPAN), accessed the system configuration, and reengineered the protocol of the Siemens 1500 PLC (S7comm). Bidirectional traffic (backflow of traffic into the network) was enabled on that port. By using an engineering workstation, a wrong PRZ level was maliciously and repeatedly transmitted to the HMI.

4.3. Result and discussion

A sensor bias attack was implemented on PRZ-level data, as illustrated in Fig. 8. The PRZ level was manipulated to 5 m at 400 s from the initiation of the cyberattack. As the PRZ level estimation residual increased rapidly, as depicted in Fig. 9, the operators were able to detect the cyberattack and recognize that the PRZ-level data was failed using the old version of EOP or the new version of EOP. In this study, a sensor drift attack, which is more difficult to detect, was additionally implemented, as depicted in Fig. 10. The PRZ level was manipulated to gradually decrease from 400 s. The operator monitoring the process variables through the deployed HMI misunderstood that the PRZ level was decreasing and executed a control command to increase the PRZ level, as prescribed in the old version of EOP. As the action continued to open the makeup valve, the operators kept the water level of the PRZ increasing. Such misjudgment and wrong actions could lead to LOCA accidents like the TMI accident. However, when the old version of EOP was

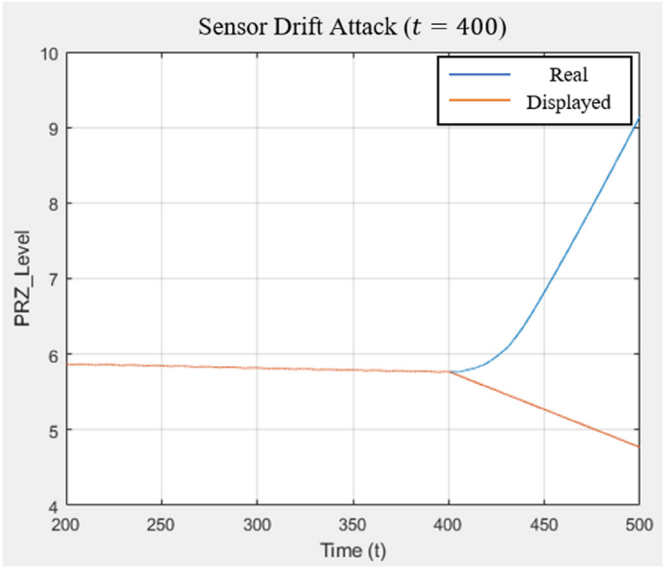


Fig. 10. PRZ level under sensor drift attack.

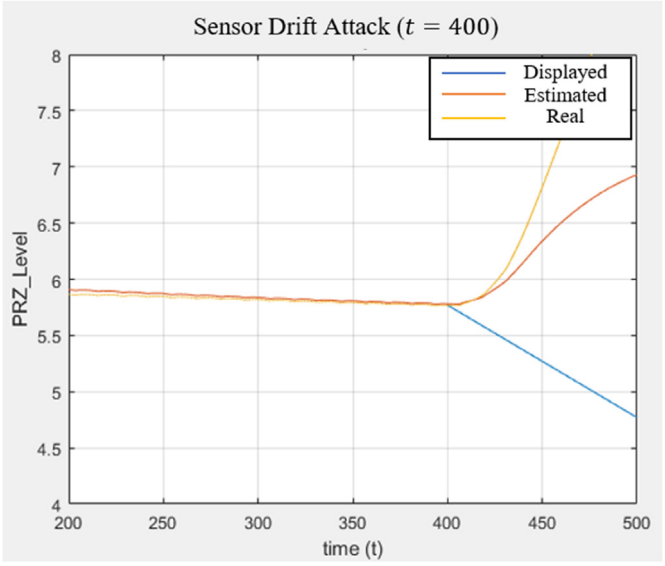


Fig. 11. Secure PRZ level estimation under sensor drift attack.

replaced by the new version of EOP, the operators were able to recognize that the cyberattack occurred at a point where the estimation residual of the PRZ level exceeded 0.5 m. And, through the adaptive Kalman filter rather than observation through the HMI, the operators were able to recognize that the actual PRZ level was increasing, as shown in Fig. 11. It was proved that the adaptive Kalman filter can secure the operator's situational awareness from process data manipulation attacks. In addition, it was possible to prevent a sharp rise in the PRZ water level, shown in Fig. 12, by enabling operators to have proper situational awareness and to take appropriate manual actions in time.

By using the developed adaptive Kalman filter to securely estimate safety-related process state variables, such as the PRZ level, MCR operators can not only detect and identify the process data manipulation attack but also recognize the current situation correctly. Moreover, the developed filter could help NPP operators to prevent the plant status from entering a dangerous state.

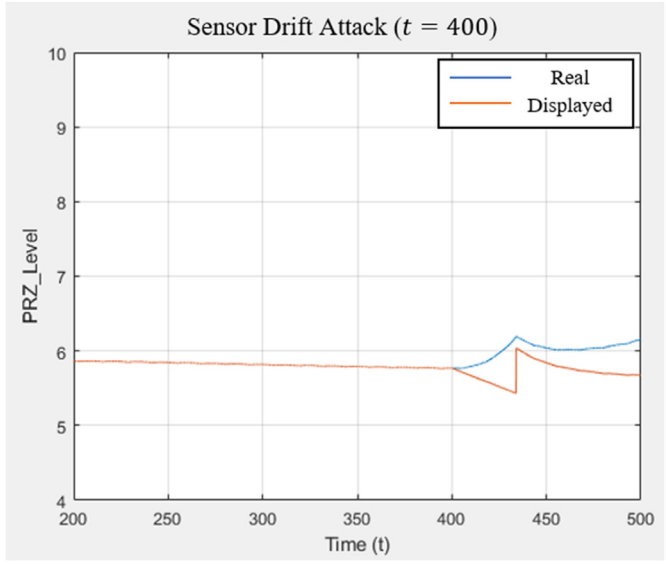


Fig. 12. Response to sensor drift attack.

However, in order to prove the effectiveness of the developed method more thoroughly, it should be confirmed that the estimation performance of the developed adaptive Kalman filter can be maintained within an appropriate range even in various attack scenarios. In addition, sensitivity analysis studies for the assumed conditions should be sufficiently performed. Although there were limitations in developing various cyberattack scenarios in this study, it is expected that sufficient sensitivity analysis studies can be conducted in the future when a method is developed for developing and implementing more diverse cyberattack scenarios. In addition, the developed adaptive Kalman filter has limitations in estimating the current system state securely and accurately. In a situation in which the integrity of the control variables cannot be guaranteed or in a situation in which more than half of the state variables are manipulated, the reliability of the state estimation may be deteriorated. In addition, estimation errors can occur because complex plant models are simplified into the form of a state space model. Further studies are needed to address these limitations.

5. Summary and conclusion

To secure NPPs against cyberattacks, it is essential to establish an integrated cyberattack response strategy that includes not only security response strategies against adversary penetrations but also safety response strategies against intentional system disruptions in connection with the existing EOPs. However, the existing EOPs were developed for use in the event of I&C system function failure, and they do not address the maloperation of systems, where the root cause may be malware or compromised computers [16]. Therefore, the EOPs should be extended to allow operators to verify the integrity of safety-related process data and correct any detected manipulations. In this study, we focus on securing the operators' situational awareness in the event of a cyberattack and developing a method that MCR operators can use to identify manipulated data and estimate the current plant process status securely during a cyberattack.

In this study, the detectable symptoms of malicious events are analyzed by using a control theory-based system analysis framework and an attack resource-based security analysis framework. Fastidious cyberattacks implemented with abundant attack

resources and sophisticated attack policies are critical to plant safety and difficult to detect by means of process monitoring. Such attacks cause NPPs to become unresponsive, even if the plants are equipped with adequate mitigation functions. However, it is more realistic to consider a cyberattack with imperfect plant knowledge and limited disclosure and disruption resources. Attackers may face limitations in terms of manipulating process data in a sophisticated manner to conceal their malicious control actions. Moreover, it may be difficult for them to maintain correlations between the manipulated process data and the unaffected process data. As a result, a few suspicious symptoms are generated that cannot be explained using NPP knowledge. However, although operators have sufficient NPP knowledge, detection and restoration of the manipulated process data is a labor-intensive, time consuming, and error-prone task for the operators.

In this study, the Kalman filter is adopted to detect plant process data manipulations. If some state variables cannot be explained by the control variables or dynamic models, the estimation residual tends to react and increases. This increase in the estimation residual can be used as an indicator of a cyberattack. However, the state estimates generated using the conventional Kalman filter can be affected by the manipulated data and cannot be used to identify the manipulated variables and correct them. For this reason, the Kalman filtering algorithm was modified to adjust the uncertainty of process data adaptively according to the size of the estimation residual.

The developed adaptive Kalman filter was validated by conducting a case study. An HIL system that was constructed for NPP cybersecurity research was used in this case study. By using the developed adaptive Kalman filter, it was possible to not only support situational awareness but also implement safety response, which helped to avert dangerous situations in advance. However, the developed adaptive Kalman filter has limitations in estimating the current system state securely and accurately. In a situation in which the integrity of the control variables cannot be guaranteed or in a situation in which more than half of the state variables are manipulated, the reliability of the state estimation may be deteriorated. In addition, estimation errors can occur because complex plant models are simplified into the form of a state space model. Further studies are needed to address these limitations.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was supported by the National R&D Program through the National Research Foundation of Korea (NRF) funded by the Korean Government. (MSIP: Ministry of Science, ICT and Future Planning) (No. NRF-2016R1A5A1013919)

References

[1] Kee-choon Kwon, Myeong-Soo Lee, Technical review on the localized digital instrumentation and control systems, Nuclear engineering and technology 41 (i) (2009) 447–454.
[2] U.S, Nuclear Regulatory Commission, “REGULATORY GUIDE 5.71 Cyber Security Programs for Nuclear Facilities, 2010, pp. 1–105. January.
[3] Korea Institute of Nuclear Nonproliferation and Control (KINAC), “Regulatory Standard on Cyber Security for Computer and Information System of Nuclear Facilities” RS-015, 2014.
[4] International Atomic Energy Agency, (IAEA), Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna, 2021.
[5] International Atomic Energy Agency (IAEA), Computer security at nuclear facilities, in: IAEA Nuclear Security Series No., vol. 17, IAEA, Vienna, 2011.
[6] International Atomic Energy Agency (IAEA), Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna, 2013.
[7] Jae-Gu Song, et al., A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nuclear engineering and technology 44 (8) (2012) 919–928.
[8] Jinsoo Shin, Hanseong Son, Gyunyoung Heo, Cyber security risk evaluation of a nuclear I&C using BN and ET, Nuclear Engineering and Technology 49 (3) (2017) 517–524.
[9] Chanyoung Lee, Yim Ho Bin, Seong Poong Hyun, Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept, Ann. Nucl. Energy 112 (2018) 646–654.
[10] Chanyoung Lee, Sang Min Han, Poong Hyun Seong, Development of a quantitative method for identifying fault-prone cyber security controls in NPP digital I&C systems, Ann. Nucl. Energy 142 (2020) 107398.
[11] Yunfei Zhao, et al., Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants, Reliab. Eng. Syst. Saf. 201 (2020) 106878.
[12] Caroline Baylon, Roger Brunt, David Livingstone, Cyber Security at Civil Nuclear Facilities: Understanding the Risks: Chatham House Report, Chatham House for the Royal Institute of International Affairs, 2015.
[13] Hamed Orojloo, Mohammad Abdollahi Azgomi, A game-theoretic approach to model and quantify the security of cyber-physical systems, Comput. Ind. 88 (2017) 44–57.
[14] Fan Zhang, J. Wesley Hines, Jamie B. Coble, A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities, Nucl. Technol. 206 (7) (2020) 939–950.
[15] Jae-hee Roh, et al., Cyber security system with FPGA-based network intrusion detector for nuclear power plant, in: IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2020.
[16] International Atomic Energy Agency (IAEA), Computer Security Incident Response Planning at Nuclear Facilities, IAEA-TDL-005, IAEA, Vienna, 2016.
[17] Chanyoung Lee, Young Ho Chae, Poong Hyun Seong, Development of a method for estimating security state: supporting integrated response to cyber-attacks in NPPs, Ann. Nucl. Energy 158 (2021) 108287.
[18] Lee, Chanyoung, et al. "Development of a cyberattack response planning method for nuclear power plants by using the Markov decision process model." Ann. Nucl. Energy 166 (2022): 108725.
[19] Hyun Gook Kang, Seung-Cheol Jang, A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant, J. Nucl. Sci. Technol. 45 (8) (2008) 850–858.
[20] Elias Levy, Crossover: online pests plaguing the off line world, IEEE Security & Privacy 1 (6) (2003) 71–73.
[21] Thomas M. Chen, Saeed Abu-Nimeh, Lessons from stuxnet, Computer 44 (4) (2011) 91–93.
[22] International Atomic Energy Agency (IAEA), Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna, 2018.
[23] Jong Woo Park, Seung Jun Lee, A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence, Ann. Nucl. Energy 142 (2020) 107432.
[24] Pierre Le Bot, Human reliability data, human error and accident models—illustration through the Three Mile Island accident analysis, Reliab. Eng. Syst. Saf. 83 (2) (2004) 153–167.
[25] Yanhua Zou, et al., Human reliability analysis for digitized nuclear power plants: case study on the LingAo II nuclear power plant, Nuclear Engineering and Technology 49 (2) (2017) 335–341.
[26] Won Dea Jung, Dae Il Kang, Jae Whan Kim, Development of a Standard Method for Human Reliability Analysis of Nuclear Power Plants, 2005. KAERI/TR-2961/2005.
[27] Hee Eun Kim, et al., Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants, Reliab. Eng. Syst. Saf. 167 (2017) 290–301.
[28] Myeong-Soo Lee, et al., Integrated Performance Validation Facility for KNICS MMIS, the Korean Nuclear Society Spring Meeting, 2007.
[29] Jae-Gu Song, et al., An analysis of technical security control requirements for digital I&C systems in nuclear power plants, Nuclear Engineering and Technology 45 (5) (2013) 637–652.
[30] Harold Booth, Doug Rike, Gregory A. Witte, The National Vulnerability Database (Nvd): Overview, 2013.
[31] Marshall Abrams, Joe Weiss, Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, MITRE CORP MCLEAN VA MCLEAN, Australia, 2008.
[32] Anton Cherepanov, WIN32/INDUSTROYER: a new threat for industrial control systems, White paper, ESET (June 2017) (2017).
[33] Robert M. Lee, M.J. Assante, T. Conway, Crashoverride: Analysis of the Threat to Electric Grid Operations, Dragos Inc., March, 2017.
[34] Suvi Leppänen, Shohel Ahmed, Robin Granqvist, Cyber security incident report—Norsk Hydro, Procedia Economics and Finance (2019).
[35] André Teixeira, et al., A secure control framework for resource-limited adversaries, Automatica 51 (2015) 135–148.
[36] Yilin Mo, Sinopoli Bruno, Secure Control against Replay attacks." 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), IEEE, 2009.

[37] Roy S. Smith, Covert misappropriation of networked control systems: presenting a feedback structure, IEEE Control Syst. Mag. 35 (1) (2015) 82–92.
[38] Hyun Gook Kang, Poong Hyun Seong, Information theoretic approach to man-machine interface complexity evaluation, IEEE Trans. Syst. Man Cybern. Syst. Hum. 31 (3) (2001) 163–171.
[39] Jong Hyun Kim, Poong Hyun Seong, A quantitative approach to modeling the information flow of diagnosis tasks in nuclear power plants, Reliab. Eng. Syst. Saf. 80 (1) (2003) 81–94.
[40] Chanyoung Lee, Poong-Hyun Seong, Development of a framework for NPP process-aware cyber attack detection and diagnosis methodology, in: Transactions of the American Nuclear Society, American Nuclear Society, 2020.
[41] Francesco Di Maio, Ajit Rai, Enrico Zio, A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis, Reliab. Eng. Syst. Saf. 145 (2016) 9–18.
[42] Wei Wang, et al., A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants, Reliab. Eng. Syst. Saf. 175 (2018) 24–37.
[43] Derui Ding, et al., A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275 (2018) 1674–1683.
[44] Theodore J. Williams, The Purdue enterprise reference architecture, Comput. Ind. 24 (2–3) (1994) 141–158.
[45] Nuclear Energy Institute (NEI), Identifying Systems and Assets Subject to the Cyber Security Rule, Jul. 2012. NEI 10-04 Rev.2.
[46] U.S., Nuclear Regulatory Commission, "The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors, " NUREG/CR-7141 November, 2014, pp. 1–77.
[47] Dong Hyuk Lim, Lee Sung Han, Na Man Gyun, Smart soft-sensing for the feedwater flowrate at PWRs using a GMDH algorithm, IEEE Trans. Nucl. Sci. 57 (1) (2010) 340–347.
[48] Young Gyu No, Poong Hyun Seong, Monitoring the performance of Aux. Feedwater pump using smart sensing model, KNS Autumn Meeting (2015) 29–30.
[49] Seung Geun Kim, Young Ho Chae, Poong Hyun Seong, Development of a generative-adversarial-network-based signal reconstruction method for nuclear power plants, Ann. Nucl. Energy 142 (2020) 107410.
[50] François Auger, et al., Industrial applications of the Kalman filter: a review, IEEE Trans. Ind. Electron. 60 (12) (2013) 5458–5471.
[51] Samira Roshany-Yamchi, et al., Kalman filter-based distributed predictive control of large-scale multi-rate systems: application to power networks, IEEE Trans. Control Syst. Technol. 21 (1) (2011) 27–39.
[52] Xinan Zhang, et al., Sensor fault detection, isolation and system reconfiguration based on extended Kalman filter for induction motor drives, IET Electr. Power Appl. 7 (7) (2013) 607–617.
[53] Kebina Manandhar, et al., Detection of faults and attacks including false data injection attack in smart grid using Kalman filter, IEEE transactions on control of network systems 1 (4) (2014) 370–379.
[54] Venkata Reddy Palleti, Yu Chong Tan, Lakshminarayanan Samavedham, A mechanistic fault detection and isolation approach using Kalman filter to improve the security of cyber physical systems, J. Process Control 68 (2018) 160–170.
[55] Takashi Irita, Toru Namerikawa, Decentralized fault detection of multiple cyber attacks in power network via Kalman filter, in: 2015 European Control Conference (ECC), IEEE, 2015.
[56] Jairo Giraldo, et al., A survey of physics-based attack detection in cyber-physical systems, ACM Comput. Surv. 51 (4) (2018) 1–36.
[57] Jean-Yves Keller, Dominique Sauter, Monitoring of stealthy attack in networked control systems, in: 2013 Conference on Control and Fault-Tolerant Systems (SysTol), IEEE, 2013.
[58] Chuadhry Mujeeb Ahmed, Adepu Sridhar, Aditya Mathur, Limitations of state estimation based cyber attack detection schemes in industrial control systems, in: 2016 Smart City Security and Privacy Workshop, SCSP-W). IEEE, 2016.
[59] Jae-gu Song, et al., Development of hardware in the loop system for cyber security training in nuclear power plants, Journal of The Korea Institute of Information Security & Cryptology 29 (4) (2019) 867–875.
[60] S.I.L.V.A. e, R.A. Busquim, et al., Advanced method for neutronics and system code coupling RELAP, PARCS, and MATLAB for instrumentation and control assessment, Ann. Nucl. Energy 140 (2020) 107098.
[61] e Silva, RA Busquim, et al. "Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants." International Journal of Critical Infrastructure Protection 34 (2021): 100453.
[62] Chanyoung Lee, et al., Development of a demonstrable nuclear cyber security test-bed and application plans, in: In Transactions of the, vol. 2019, KNS Spring Meeting, 2019, pp. 23–25.
[63] Jinsoo Shin, et al., Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed, Nucl. Eng. Technol. 53 (10) (2021) 3319–3326.
[64] MathWorks, System Identification Toolbox User's Guide, MathWorks, 2016.
[65] Jae-gu Song, et al., Preparation for cyber security incident response training in nuclear power plants, in: In Transactions of the 2020, KNS Spring Meeting, 2020, pp. 9–11.