Modern power system reliability assessment with cyber-intrusion on heat pump systems

Hasan Gunduz¹,² and Dilan Jayaweera¹

¹Department of Electronic, Electrical and Systems Engineering, University of Birmingham, Edgbaston, Birmingham B15 2TT, UK
²Department of Electrical & Electronic Engineering, Mus Alparslan University, Mus 49250, Turkey
E-mail: hasangunduz@ieee.org

Abstract: In smart power systems, information and communication technologies are being broadly installed and two-way communications are being established more effectively and efficiently. However, they are vulnerable to cyber-physical interactive threats and their impact depends on the system infrastructure, degree of interaction, degree of vulnerability, and the intensity and the frequency of the attack. The study addresses this problem and proposes: (i) an innovative Markov-chain based framework of the cyber-intrusion process to implement operating conditions in a smart power system; (ii) an advanced algorithm for power system reliability assessment, incorporating cyber-intrusion process and a detailed model of a heat pump system; and (iii) a new impact assessment framework for different cyber-intrusion detection-time distributions driven by Monte Carlo simulation. The cyber-detection and system recovery process with the presence of cyber-physical interactive operation models suggest that a significant level of impacts could be generated by the interactive operation of the smart power system and a quantiative assessment is needed in order to assess true impacts.

Nomenclature

| Symbol | Description |
|--------|-------------|
| A, U   | system indicators (availability/unavailability) |
| λ_system | failure/repair rate of system |
| λ_switch | failure/repair rate of switch |
| λ_HC | failure/repair rate of heating system's control panel |
| λ_HP | failure/repair rate of heat pump |
| λ_valve | failure/repair rate of expansion valve |
| λ_HAH | failure/repair rate of auxiliary heater |
| λ_Comp | failure/repair rate of compressor |
| λ_Cond | failure/repair rate of condenser |
| λ_Evalve | failure/repair rate of expansion valve |
| F_SUCCESSFUL | number of successful cyber-intrusion attempts |
| A_success | successful cyber-intrusion attempt |
| X_n | normal attack time needed during nth phase of cyber intrusion for attack agent |
| X_S | smart-attack time needed during nth phase of cyber intrusion for smart-attack agent |
| Y | detection time of the cyber intrusion during nth phase for detection agent |
| P_F, P_r | failure/repair state probability of components |

1 Introduction

Over the past decade, there has been a dramatic increase in the implementation of renewable energy resources such as solar photovoltaics (PV), wind power generation, coupled with a growing focus on strategic decarbonisation elements in the service sector, for instance, electric vehicles and heat pumps (HPs), have provoked a complexity in structure, and resulted in new challenges in power system operations [1]. Penetrating these cutting-edge technologies into the power grids shifts its topological configuration from being centralised with dispatchable conventional generation to being distributed with non-dispatchable intermittent generation [2]. To maintain reliable operations of the decentralised power systems, high-level monitoring and supervision practices are desired [3]. These desirable necessities are fulfilled by installing an advanced metering infrastructure (AMI) and additional components of Information and Communication Technologies (ICTs).

ICT is a critical infrastructure in modern power systems. AMI is a key element in the critical infrastructure and it had been deployed almost 87 million sites in the USA by 2018, representing 50% of all USA electricity customers [4]. Increasing installations of cyber-physical-based systems such as AMI, not only bring wide-ranging benefits, but also open doors for cyber-attack agents to access critical information, force the system into abnormal conditions and even leading to power outages. On account of their harmful and unexpected nature, preventing cyber-attacks have recognised as a critical issue in power systems sector.

At the end of 2015, Ukraine's power distribution system was exposed to a sophisticated cyber-attack. The pre-attack period was started several months before the attack-day and, attackers observed and determined cyber-attack pathways in the power grid. As a result, data of key assets was manipulated and almost 225,000 customers experienced a black-out for several hours [5]. In 2017, energy companies were indirectly affected by fast-spreading encrypting malware, called “NotPetya” [6, 7]. Although there were no direct effects on operations of energy companies, this ransomware caused collateral damage that was a huge financial loss, and it was linked with the previous cyber-attack on Ukrainian power grid according to [8]. Afterwards, during the year of 2019, there were a higher number of cyber incidents on critical infrastructure that was a rising concern for power sector [7]. American power companies and Russian power plants were hacked by cyber-intruders in March and June 2019, respectively [9]. Especially, parts of power networks in three states of the USA were influenced by cyber-intruders on Supervisory Control and Data Acquisition (SCADA) systems while power utilities stayed in the control of power grid operators [7, 9]. Together, these real cases show reliable operation of most of the power grids are under attack, grid resiliency is fragile, its vulnerability is rising, and preventive actions for power grids are needed for operational continuity and avoid cascading failures.
In addition, cyber-intrusion process modelling has received considerable attention. In [16], a study was conducted to quantify security failures due to cyber vulnerabilities considering conventional computer system layers. It was found that although the security failure quantification in that study was done well, the time scale identification of cyber layer's detection-attack agents was limited [16]. A recent study by Xiang et al. [17] utilised semi-Markov process in a similar way as in [16] to investigate the probability of a successful cyber-attack. The difference between cyber-intrusion methodology applied in [16, 17] is that different reconnaissance and waiting time scales were implemented in the former. When the detection-agent time interval was modified with different limits, the cyber-attack waiting time (sojourn) in each layer and pre-attack (reconnaissance) time were changed significantly. Thus, the changes in calculation of cyber-attack waiting and pre-attack times have an effect on cyber-attack impact analysis. In addition to [16, 17], the same methodology of the cyber-intrusion process was applied in [18]. Zhang et al. [18] differ from Xiang et al. [17] only in the cyber-attack types and pathways. These previous studies [17, 18] did not take into account the futuristic characteristic of system smart components, the smart capability of layers in the procedure and sophisticated attacks. This paper makes several contributions as follows:

- An innovative mathematical model for HP system configuration is proposed in order to reduce assessment process complexity of cyber-physical systems.
- A new algorithm is proposed for the reliability assessment of HP systems with cyber-physical interactive operations.
- An enhanced cyber-intrusion process model is presented for cyber-physical system reliability analysis. This model also considers stochastic attack-detection time in the cyber-intrusion process.
- Sensitivity analysis framework of attack-detection times in cyber-intrusion process for HP systems is presented.

The paper is outlined in the following structure. Section 2 delineates mathematical model of the research problem and cyber-physical interactive power system reliability framework for the heating system; Section 3 presents the case studies and analysis, and finally, Section 4 concludes the findings of the investigations.

2 Mathematical model

The aim of this section is to present cyber-intrusion process models combined with HP reliability assessment framework applied to a smart power grid. In order to design the framework, at first, an intrusion path model is demonstrated. Then, a new cyber-intrusion process is introduced showing calculation steps of attack-detection times that are essential parts for the calculation of cyber-physical system failures. Next, a generic component-based reliability model of an HP system is presented for cyber-physical system reliability analysis. This model also incorporates Monte Carlo simulation for composite reliability assessment.

2.1 State transition model for smart grid

As reported by the National Electric Sector Cybersecurity Organization Resource (NESCOR) in [19], power systems need a different manner to preserve critical infrastructures for present and future developments. Hence, power system studies also require distinctive approaches in order to assess the futuristic features of smart grid elements. As stated in Fig. 1, the study considers three different typical process ways to reach successful cyber intrusion for the smart grid. All three-intrusion pathways have equal probabilities to compromise a cyber-attack. This paper selected only intrusion path 1 (Fig. 1) through the DER SCADA (supervisory control and data acquisition of distributed energy resources) to show the cyber-attack process in a power grid. Path 1 is chosen due to SCADA systems is one of the most vulnerable ICT components in the energy sector. Additionally, there has been a considerable amount of real cyber-incidents are happening through SCADA systems [20, 21]. There are six distinctive phases

![Fig. 1 Generic attack tree graph for smart grid environment](image_url)
that $P_1$–$P_6$ are defined as secure and failed system states, respectively. In this cyber-intrusion process, a cyber-attack tries to get an advantageous status to pass to the next phase. Thus, $P_1$, $P_2$, $P_3$, $P_4$, and $P_5$ demonstrate the probability of each phase for cyber-intrusion to pass to the next state (Fig. 2). The cyber-intrusion process is successful only if the attack reaches the absorption state $P_6$ of the system

$$
T = \begin{bmatrix}
1 - P_1 & P_1 & 0 & 0 & 0 & 0 \\
1 - P_2 & 0 & P_2 & 0 & 0 & 0 \\
1 - P_3 & 0 & 0 & P_3 & 0 & 0 \\
1 - P_4 & 0 & 0 & 0 & P_4 & 0 \\
1 - P_5 & 0 & 0 & 0 & 0 & P_5 \\
1 - P_6 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.
$$

(1)

2.2 Calculation procedure for cyber intrusion process times

2.2.1 Definitions and assumptions for intrusion process: The mission of an attack-agent is to gain a privilege status in a particular period against the detection agent. A smart-attack agent needs to help to the attack agent for simplifying cyber-intrusion preparations in a certain amount of time. In addition, the detection agent must spend some time to detect the cyber-intrusion to isolate the attack and limit to successful-attack intrusion in each cyber-layer. By means of playing this cyber game in between agents, MTTC$_{Cyber}$ (mean time to compromise for cyber-attack) can be computed. It is defined as a statistical time-variant that is to obtain the required mean time value to go from the normal status to the abnormal status of the system. Moreover, MTTC$_{Cyber}$ (mean time to detection for cyber-attack) refers to another statistical value that is cyber-forensic with physical restoration time and this is necessary for the statistical probability evaluation of a successful cyber-attack intrusion ($P_{Cyber\text{-}\text{attack}}$). These two statistical values of threats can vary with attack type, frequency, strength and severity of layers etc. Their statistical relation is presented as follows:

$$
P_{\text{Cyber-attack}} = \frac{\text{MTTD}^{\text{Cyber}}}{\text{MTTD}^{\text{Cyber}} + \text{MTTC}^{\text{Cyber}}}.
$$

(2)

Statistical calculation of $P_{\text{Cyber-attack}}$ in (2) can be utilised in power system reliability and resiliency. The investigation aim is to present the smart attack agent role in the process of intrusion and to assess the impact on the statistical value of MTTC$_{Cyber}$. Additionally, the study has some assumptions related to the cyber-intrusion process. They are as follows:

- The investigation considered the mission of a cyber-attack is to force the system to the abnormal states. The system has a detection agent in each cyber layer that adversely affects the detection of threats and preserves the system at normal conditions.
- Available detection systems in the cyber-security sector have been designed with available cyber-attack data, which are assumed as normal attacks, in a data set [22]. Intelligent attacks or smart-attacks are accepted as unknown and unseen attacks.
- The investigation assumed component characteristics of a power system would change with smart features that would include subordinate smart firewalls and smart detection assets. As a result, the investigation includes the detection agents for cyber-attack detection. Each cyber layer has a smart detection system and different ability against threats in order to minimise their impacts on the system. Thus, the detection time is considered in a random manner.
- The attacker agent needs to spend some time to gain the trust of the cyber layer in order to get an authorisation for passing to the next stage of the smart grid. Additionally, it is assumed that the target of the attacker is to cause harm to a smart meter or control panel of HP for energy theft from end-users.
- The intruder is presumed to inject bad data into the system for the manipulation of energy reading measurements and the detector is supposed to have a capability of anomaly behaviour detection because of generic MTTD$_{Cyber}$ estimation for this study.

2.2.2 Calculation of MTTC$_{Cyber}$. This sub-section aims to introduce statistical calculation of cyber-attack waiting (sojourn) times in each cyber layer and the total intrusion process time. A fundamental instrument is to develop cyber intrusion occurrence and its waiting time in each cyber-physical layer. Hence, it is vital to point out the calculation of required time for each attack phase as well as full attack process. In order to quantify security levels of cyber-physical components on the smart grid, the MTTC$_{Cyber}$ refers to requisite time to go from secure to failure status of the system that is implemented for power system reliability evaluations. As previously mentioned, normal attack $f(X^n)$, smart-attack $f(X^s)$, and detection agents $f(Y)$ are introduced. AlmasiZadeh and Azgomi [16] quantify security failures with conventional computer layers, and detection time of cyber-intrusion has a restriction in the time scaling identification of detection process. Similarly, Xiang et al. [17] utilise semi-Markov chain for cyber-attack process, except adding a clear identification on lower boundary limit of cyber-intrusion process time, though utilising a constant value for detection time in [16, 17], which is an unreal approach that it should be assigned as a variable value in each intrusion attempt. The differences between our approach and previous studies in [16, 17] on MTTC$_{Cyber}$ calculation are: (i) considered the implementation of a smart-attack agent in each layer that has different boundary limits for detection time (as noted in Fig. 3); (ii) new lower-upper boundary limits have been implemented for cyber-attack process (as in Fig. 3); and (iii) added variable detection time of cyber-intrusion established that brings novelty to the cyber-threat modelling framework. Fig. 3 shows the difference between the previous studies’ approaches on calculation of MTTA (mean time to attack) [16, 17] and the proposed approach on MTTC$_{Cyber}$. This study models attack and defense times incorporating with uniform distributions. To begin the calculation process, let $X^n_t$ and $X^s_t$ denote normal attack and smart-attack time.

![Fig. 2 Semi-Markov model for cyber-intrusion in a smart grid](image-url)
As described in (4) and (5), $[\tau_{d,i}, \tau_{a,i}, \tau_{a,i} + Z_{i}]$ and $[\tau_{a,i}, \tau_{d,i}, \tau_{d,i} - Z_{i}]$ are utilised for lower–upper boundary limits of $X^a_i$ and $X^d_i$ in each phase, respectively. Whereas $X^a_i$ and $X^d_i$ refer to the total operation of attack times of normal operation and smart operation, respectively, $Y_i$ refers to the detection time of the cyber intrusion during the $i$th phase for detection agent. To select appropriate time intervals for $Y_i$, the uniform distribution function is applied in this study. The $Y_i$ detection time interval is chosen as $[\tau_{a,i}, \tau_{d,i}]$ for each cyber layer. In each phase of the system, relation on determination of successful attack intrusion and detection probability is presented in (6):

$$P(Y_i < [X^a_i + X^d_i]) + P(Y_i > [X^a_i + X^d_i]) = 1. \quad (6)$$

As stated in (7), the probability of successful detection, where $P(Y_i < [X^a_i + X^d_i])$, is computed by using conditional probability theorem. While the probability of successful detection at each phase of the system is as in (8), waiting (sojourn) time $W_i$ at each phase of the system is referred to $Z_i = \min \{Y_i, [X^a_i + X^d_i]\}$. (see (7))

$$W_i = \int_0^{\tau_{max}} (1 - P(Z_i \leq r)) dr = \int_0^{\tau_{max}} P(\min \{Y_i, [X^a_i + X^d_i]\} > r) dr = \int_0^{\tau_{max}} \frac{(\tau_a - \tau_{d,i})(2\tau_a + \tau_{a,i} - 3\tau_{a,i}) + 6(\tau_{a,i} - \tau_{d,i})^3 - 3(\tau_{a,i} - \tau_{d,i})(2\tau_a + \tau_{a,i} - 3\tau_{a,i})}{(\tau_{a,i} - \tau_{d,i})(\tau_a - \tau_{d,i})(\tau_{d,i} - \tau_{a,i})} dr = \frac{1}{18}$$

The procedure of MTTCyber depends on the study of queuing theory, that is, predicting waiting time and queue lengths [23]. Thus, the semi-Markov model (Fig. 2) (1) is constructed with intrusion path calculation procedure steps of the MTTCyber. In addition, after identification of time boundaries of each cyber layer, waiting time ($W_i$) (8) at each phase is calculated for the transient state by the help of calculation steps of [16]. Due to different boundary limits in our approach, the final formula of waiting time ($W_i$) (8) differs than [16]. First, the final canonical form of transition matrix of $K$ is presented as similar as in [16, 24]. It ($K$) is written as:

$$K = \begin{bmatrix} T & C \\ 0 & I \end{bmatrix} \quad (9)$$

where $T$ represents state transition probabilities that [23] demonstrates state transitions of the presented model for smart grid, and sub-matrix $C$ refers to transition probabilities between the cyber-layers. Secondly, combining (1)–(8) and (9), MTTCyber is finally calculated as in (10):

$$P(Y_i < [X^a_i + X^d_i]) = \int_0^{\tau_{max}} P(Y_i < [X^a_i + X^d_i]) f_{[X^a_i + X^d_i]}(r) dr = \int_0^{\tau_{max}} \frac{3(\tau_{a,i} - \tau_a - 2(\tau_{a,i} - \tau_a - \tau_{d,i} - \tau_{a,i}) - (\tau_{a,i} - \tau_{a,i}) + (\tau_{a,i} - \tau_{a,i})^2}{2(\tau_{a,i} - \tau_a - \tau_{d,i} - \tau_{a,i})^2} + \frac{2(\tau_{a,i} - \tau_a - \tau_{d,i} - \tau_{a,i})(\tau_a - \tau_{a,i})(\tau_a - \tau_{a,i})^2 + 2(\tau_{a,i} - \tau_{a,i})(\tau_a - \tau_{a,i})}{4(\tau_{a,i} - \tau_a - \tau_{d,i} - \tau_{a,i})(\tau_a - \tau_{a,i})} + \frac{(\tau_{a,i} - \tau_a - \tau_{d,i} - \tau_{a,i})(\tau_a - \tau_{a,i})}{(\tau_{a,i} - \tau_a - \tau_{d,i} - \tau_{a,i})(\tau_a - \tau_{a,i})} dr. \quad (7)$$

1543

564 IET Smart Grid, 2020, Vol. 3 Iss. 5, pp. 561-571
This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
\[ \text{MTTC}_{\text{Cyber}} = \sum_{i=1}^{N_i} N_i W_i \]  
(10)

where \( N_i \) is expected statistical number of times in \( i \) transient state phase that the system reaches failure state finally. It is written as in (11):

\[ N_i = q_i \sum_{j} N_i W_i \]  
(11)

where \( q_i \) denotes the probability of the process starts from state \( i \). It is assumed that the initial status is the secure state.

As explained previously, the calculation process of MTTC_{Cyber} needs to be carefully examined due to disparities (time intervals, severity of layers etc.) between each cyber/system layer characteristics. Taking into consideration of these disparities, security of each cyber layer could be quantified more accurately with this process. We assumed that each layer behaves differently against cyber intrusion during the process due to future characteristics of smart grids. Each layer could have a different impact on the statistical calculation of MTTC_{Cyber}. For this reason, the calculation process of cyber intrusion probability \( (P_{\text{Cyber-attack}}) \) is carefully examined with the effect of MTTC_{Cyber}.

As far as MTTC_{Cyber} is concerned, MTTC_{Cyber} plays an essential role when evaluating \( P_{\text{Cyber-attack}} \) as well as cyber-physical system reliability. It is important to highlight that the system will remain in the failure status in a certain amount of time until the detection agent catches the attacker. In this study, detection time denotes detection time plus recovery time of the system. Therefore, it is necessary that detection time \( (\text{MTTD}_{\text{Cyber}}) \) identification for \( P_{\text{Cyber-attack}} \) calculations is essential. This unique value could change according to attack type, frequency, strength and severity of layers etc. As previous studies stated in [17, 18], there is no available real data for detection time. These studies [17, 18] utilise a constant number for MTTD_{Cyber} which should be a different statistical value in each system. For this reason, the mean detection time needs to be determined according to a statistical analysis of the detection agent's capabilities. Within this target, our study investigates the fundamental behaviour of the detection process and the underlying distribution of detection time. There is a large volume of published studies describing the role of intrusion detection in the context of computer science. Intrusion detection studies are mainly classified into two types: misuse and anomaly detection [25, 26]. As the aim of the attacker could be the energy theft from consumers with false data injection, the study considers it as an anomaly detection of the detection time. In the anomaly-based detection mechanism, the intruder can only be detected if it acts in a different way compared to legitimate behaviour of the system. Thus far, several studies have indicated that the intrusion detection process could obey heavy-tail distribution characteristics [27–29]. Heavy-tail distributions are probability density functions and their tails are not limited by an exponential distribution. The results in [28] show that detection time follows the heavy-tail distribution. Sampling path of a heavy-tailed featuring system reduces slowly, and its efficacy falls over time. Therefore, heavy tail distributions have been utilised for sampling of many extreme events such as floods, tsunamis etc. Since cyber-attacks are considered as rare and extreme events and they are less extreme over time due to not being anymore as unseen threats [27, 29], the marginal distribution of intrusion detection times may follow a heavy tail pattern. On the other hand, some previous studies confirmed the effectiveness of Gaussian distribution on the intrusion detection process [30, 31]. As in [32], a system error is assumed to follow a normal distribution. Yu et al. [32] confirmed that manipulated data may pursue Gaussian distribution if the adversary has information on the detection technique. As a result of many variables and uncertainties in the relation of adversary and detection, the statistical value of MTTD_{Cyber} is considered as a random number. By using MATLAB, these random numbers are determined from a pool that has a specific range and distribution technique. MTTD_{Cyber} is carefully chosen from the following pool with pre-defined distribution:

\[
4h = \alpha_1 \leq \text{MTTD}_{\text{Cyber}} \leq \alpha_2 = 1000h \quad \text{MTTD}_{\text{Cyber}} \rightarrow \text{rand}\]  
(12)

For this study, heavy tail (General Pareto, Stable [33], Pareto distributions) and Gaussian distributions are utilised for the selection of MTTD_{Cyber} in each case. Having discussed how to calculate MTTC_{Cyber} and MTTD_{Cyber}, the following section of this paper addresses the component-based reliability model for the heating system.

2.3 Component-based reliability modelling for heating system

The study utilises a common implementation model of a heating system in a power grid to compute composite system availability with piecewise element consideration [34]. By doing so, the heating system model is divided into three sub-sections as in Fig. 4. It consists of a control panel \( (\lambda_C, \mu_C) \), HP and auxiliary heater with switch \( (\lambda_H, \mu_H) \), and storage \( (\lambda_{Str}, \mu_{Str}) \) as a series system, respectively. This system is modelled with the eight-state Markov transition matrix (14) if there is a successful cyber-intrusion. Whether there is a cyber-intrusion, availability calculation takes consideration of four-state Markov model (13) if there is a successful cyber-intrusion. Availability calculation takes consideration of four-state Markov model (13) that involves sub-sections 2 and 3. The sub-section 1 of the heating system is considered as a control panel that has a capability of two-way communication and stores consumer reading data. Its statistical value of failure-recovery against cyber-intrusion plays a key role for availability analysis of all systems. For this purpose, we introduce \( P_{\text{Cyber-attack}} \) calculation in previous parts. By means of \( P_{\text{Cyber-attack}} \) the study estimates \( \lambda_C, \mu_C \) composite availability analysis of the cyber-physical system. Following that, the sub-

---

**Fig. 4** Generic heating system configuration

**IET Smart Grid, 2020, Vol. 3 Iss. 5, pp. 561-571**

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
Fig. 5 Generic HP’s components

section 2 is composed of HP ($λ_{HP}, μ_{HP}$), switch ($λ_{Switch}, μ_{Switch}$) and auxiliary heater ($λ_{AH}, μ_{AH}$). In addition, estimated availability of HP is determined with its internal elements that includes an evaporator ($λ_{Evap}, μ_{Evap}$), compressor ($λ_{Comp}, μ_{Comp}$), condenser ($λ_{Cond}, μ_{Cond}$) and expansion valve ($λ_{Valve}, μ_{Valve}$) as a series internal system. One of the generic HP models [34] is demonstrated in Fig. 5.

Defining series or parallel arrangement of any system has significant importance on reliability calculations [35]. Thus, formulas (15)–(18) are adopted into fundamental part of reliability calculation of HP ($λ_H, μ_H$):

$$M_v = \begin{bmatrix} -λ_H - λ_{Str} & λ_H & λ_{Str} & 0 \\ μ_H & -μ_H - λ_{Str} & 0 & λ_{Str} \\ μ_S & 0 & -μ_S - λ_H & λ_H \\ 0 & μ_S & μ_H & -μ_H - μ_{Str} \end{bmatrix}$$

(see (14))

$$\dfrac{P_f}{P_f} = \frac{λ_{System}}{μ_{System}} \Rightarrow λ_{System} = μ_{System} \times P_f \times P_f^{-1}$$

(see (16))

$$λ_{HP} = λ_{Comp} + λ_{Cond} + λ_{Evap} + λ_{Valve}.$$  

$$μ_{HP} = μ_{Comp} \times μ_{Cond} \times P_{Evap} \times P_{Valve}^{-1}.$$  

(17)

(18)

Once the reliability of internal components of HP is computed, a series arranged auxiliary heater with switch must be involved in reliability calculations by (19)–(21):

$$P_{f_H} = \frac{μ_{AH}}{λ_{AH} + μ_{AH}} \times \frac{μ_{Switch}}{λ_{Switch} + μ_{Switch}} \Rightarrow P_{f_H} = 1 - P_{f_H}$$

(19)

$$λ_{AH,tot} = λ_{AH} + λ_{Switch}.$$  

(20)

$$μ_{AH,tot} = λ_{AH,tot} \times P_{f_H} \times P_{f_H}^{-1}.$$  

(21)

After completion of reliability calculation of series arranged components ($λ_{HP}, μ_{HP}$), the parallel arrangement of estimated failure–repair rates is used to reach the final calculation of ($λ_H, μ_H$) via (22)–(24):

$$P_{f_H} = \frac{λ_{AH,tot}}{λ_{AH,tot} + μ_{AH,tot}} \times \frac{λ_{HP}}{λ_{HP} + μ_{HP}} \Rightarrow P_{f_H} = 1 - P_{f_H}$$

(22)

$$μ_{H} = μ_{AH,tot} + μ_{HP}.$$  

(23)

$$λ_H = μ_H \times P_{f_H} \times P_{f_H}^{-1}.$$  

(24)

The final sub-section is assumed as heat storage of which the failure and repair rates are denoted by $λ_{Str}, μ_{Str}$ respectively. Taken together all, piecewise reliability calculation will incorporate the Markov model of heating system to compute the system availability at a top down level.

2.4 Composite system availability analysis for heating system with cyber-physical component

In this study, a framework is presented to calculate overall system availability, and it is an indicator of system reliability. Four-state ($M_r$) and eight-state ($M_v$) stochastic transition matrices represent system state probabilities. To determine and simplify these system probability vectors [36] and Markov transition matrices are modelled in (25):

$$\overline{P(v)} = \sum_{\bar{v}} \bar{s} \bar{v} e^{\bar{v}}$$

(25)

where $v$ represents the eigenvalues of the transpose matrix $M$, $\bar{v}$ is the eigenvectors of the transpose matrix $M$ and $S$ denotes a constant that is calculated according to the initial system state.

In general, the system availability is evaluated as one of the factors for reliability determinant. It can be defined with all the probability states. Availability and unavailability of the system can be represented by operational and non-operational system states of probabilities, respectively. They are written as in (26):

$$\overline{P(v)} = P_r(t) + \cdots + P_n(t) = A(t) + U(t).$$

(26)
In this study, composite-system availability as a factor in power system reliability analysis with cyber-intrusion effects. Power grids generally examine the operational reliability even if there is not a cyber-intrusion through a heating system. On the other hand, regular assessment can help to avoid system losses and large system disturbances. Composite system availability analysis and its reliability calculation procedure are described in Fig. 6 and its steps are given as follows:

i. Select the relevant reliability data for each component of the heating system, generators, transformers, lines and power system components and then determine the HP pool profile and time intervals for each cyber-layer transitions.

ii. Randomly select a day and an HP user for initiating an HP load profile.

iii. Extract HP load for time t from the selected profile and initialise the number of intrusion attempts.

iv. Model MTTC_{Cyber} and MTTD_{Cyber} with given time intervals for each cyber-layer transitions.

v. Check the number of successful cyber-intrusions within 100 attempts (assumed number) in time t. This process is described as in (29):

\[
F_{Cyber} = \begin{cases} 0, & r \leq P_{Cyber - attack} \\ 1, & r > P_{Cyber - attack} \end{cases}
\]

where \( F_{Cyber} \) denotes number of successful cyber-intrusion attempts within 100 attempts and \( r \) is a random number. \( F_{Cyber} \) is a function that helps to estimate failures of the cyber-physical system. Initial condition of successful cyber-intrusion attempt \( A_{successful} \) is set to zero. If a success of an attempt is larger than \( r \), \( A_{successful} \) is increased. Failure rate of the control panel is expressed as \( \lambda_c = 1/A_{successful} \) for time \( t \).

vi. By constraining as \( r < P_{Cyber - attack} \), the relevant stochastic transition matrix is determined.

vii. According to the identified transition matrix, calculate updated failure-repair rates of heating sub-systems as described in Section 2.3.

viii. Then, compute the eigenvectors and the eigenvalues of the system as in Section 2.4.

ix. Build relevant composite system availability function at time \( t \).

x. Quantify availability function according to the system state.

xi. Extract HP load value and re-produce it for time \( t \). Next, extract re-generated HP load profiles.

xii. Select the physical system state randomly.

i. Perform power flow considering power balance with voltage limits as a constraint.

xv. If the solution is not converged, go to the step xi.

xvi. Compute load curtailment of the whole system.

xvii. Estimate the expected energy not supplied (EENS).

### 3 Case studies and analysis

The aim of the case studies is to investigate how cyber-intrusion on HP systems affect power system reliability considering different attack-detection time distributions. To investigate its effects on power system reliability, two ‘what if’ scenarios are implemented. Scenario 1 reflects how cyber manipulation on the electricity usage of each HP user can affect system reliability with different drivers which could be a control panel of heating system, then traditional power system reliability analysis should evolve to assess the impact of these cyber-physical components of the control panel. It is considered that the control panel of the heating system is linked to smart meters. System designers and decision-makers of power grids generally examine the operational reliability even if there is not a cyber-intrusion through a heating system. On the other hand, regular assessment can help to avoid system losses and large system disturbances. Composite system availability analysis and its reliability calculation procedure are described in Fig. 6 and its steps are given as follows:

i. Select the relevant reliability data for each component of the heating system, generators, transformers, lines and power system components and then determine the HP pool profile and time intervals for each cyber-layer transitions.

ii. Randomly select a day and an HP user for initiating an HP load profile.

iii. Extract HP load for time t from the selected profile and initialise the number of intrusion attempts.

iv. Model MTTC_{Cyber} and MTTD_{Cyber} with given time intervals for each cyber-layer transitions.

v. Check the number of successful cyber-intrusions within 100 attempts (assumed number) in time t. This process is described as in (29):

\[
F_{Cyber} = \begin{cases} 0, & r \leq P_{Cyber - attack} \\ 1, & r > P_{Cyber - attack} \end{cases}
\]

where \( F_{Cyber} \) denotes number of successful cyber-intrusion attempts within 100 attempts and \( r \) is a random number. \( F_{Cyber} \) is a function that helps to estimate failures of the cyber-physical system. Initial condition of successful cyber-intrusion attempt \( A_{successful} \) is set to zero. If a success of an attempt is larger than \( r \), \( A_{successful} \) is increased. Failure rate of the control panel is expressed as \( \lambda_c = 1/A_{successful} \) for time \( t \).

vi. By constraining as \( r < P_{Cyber - attack} \), the relevant stochastic transition matrix is determined.

vii. According to the identified transition matrix, calculate updated failure-repair rates of heating sub-systems as described in Section 2.3.

viii. Then, compute the eigenvectors and the eigenvalues of the system as in Section 2.4.

ix. Build relevant composite system availability function at time \( t \).

x. Quantify availability function according to the system state.

xi. Extract HP load value and re-produce it for time \( t \). Next, extract re-generated HP load profiles.

xii. Select the physical system state randomly.

i. Perform power flow considering power balance with voltage limits as a constraint.

xv. If the solution is not converged, go to the step xi.

xvi. Compute load curtailment of the whole system.

xvii. Estimate the expected energy not supplied (EENS).

### 3 Case studies and analysis

The aim of the case studies is to investigate how cyber-intrusion on HP systems affect power system reliability considering different attack-detection time distributions. To investigate its effects on power system reliability, two ‘what if’ scenarios are implemented. Scenario 1 reflects how cyber manipulation on the electricity usage of each HP user can affect system reliability with different drivers which could be a control panel of heating system, then traditional power system reliability analysis should evolve to assess the impact of these cyber-physical components of the control panel. It is considered that the control panel of the heating system is linked to smart meters. System designers and decision-makers of power grids generally examine the operational reliability even if there is not a cyber-intrusion through a heating system. On the other hand, regular assessment can help to avoid system losses and large system disturbances. Composite system availability analysis and its reliability calculation procedure are described in Fig. 6 and its steps are given as follows:

i. Select the relevant reliability data for each component of the heating system, generators, transformers, lines and power system components and then determine the HP pool profile and time intervals for each cyber-layer transitions.

ii. Randomly select a day and an HP user for initiating an HP load profile.

iii. Extract HP load for time t from the selected profile and initialise the number of intrusion attempts.

iv. Model MTTC_{Cyber} and MTTD_{Cyber} with given time intervals for each cyber-layer transitions.

v. Check the number of successful cyber-intrusions within 100 attempts (assumed number) in time t. This process is described as in (29):

\[
F_{Cyber} = \begin{cases} 0, & r \leq P_{Cyber - attack} \\ 1, & r > P_{Cyber - attack} \end{cases}
\]

where \( F_{Cyber} \) denotes number of successful cyber-intrusion attempts within 100 attempts and \( r \) is a random number. \( F_{Cyber} \) is a function that helps to estimate failures of the cyber-physical system. Initial condition of successful cyber-intrusion attempt \( A_{successful} \) is set to zero. If a success of an attempt is larger than \( r \), \( A_{successful} \) is increased. Failure rate of the control panel is expressed as \( \lambda_c = 1/A_{successful} \) for time \( t \).

vi. By constraining as \( r < P_{Cyber - attack} \), the relevant stochastic transition matrix is determined.

vii. According to the identified transition matrix, calculate updated failure-repair rates of heating sub-systems as described in Section 2.3.

viii. Then, compute the eigenvectors and the eigenvalues of the system as in Section 2.4.

ix. Build relevant composite system availability function at time \( t \).

x. Quantify availability function according to the system state.

xi. Extract HP load value and re-produce it for time \( t \). Next, extract re-generated HP load profiles.

xii. Select the physical system state randomly.

i. Perform power flow considering power balance with voltage limits as a constraint.

xv. If the solution is not converged, go to the step xi.

xvi. Compute load curtailment of the whole system.

xvii. Estimate the expected energy not supplied (EENS).
3.1 Input data for cyber-intrusion process in smart grid

This part describes the data utilised for reliability assessment. The reliability assessment framework of a heating system in Section 2 incorporated the data are given in Table 1 and the data is sourced from [38]. Time intervals for calculating MTTC\text{Cyber} are randomly selected from Table 2 for each phase. The study assumed that each cyber layer has its own time characteristic and the capability of an attacker will have a different approach on waiting (sojourn) time. HP load profile data is sourced from the open-source in [39]. This data consists of HP load profiles of 19 customers over a month during the heating season in 2014. The study only uses HP load data of ten customers for re-generating HP load profile. Utilised HP data has been randomly selected from 350 HP load profile samples of the data pool.

3.2 Scenario: 1 cyber-attack on HP during the peak times

The aim of an attacker is to manipulate an HP user data and manipulate electricity usage of each HP user. This scenario does not only help compare different detection time distributions but also demonstrates the attacker's behaviour on the manipulation of HP load and its disparity compared to the peak time of electricity consumption. It is essential that 'same original HP load profile' is necessary to be incorporated in all figures to show readers a clearer distinction in load difference in each time interval during the cyber-intrusion, attack timing effects on load manipulation and calculation of EENS. Attacked HP site includes 100 users in total. Due to not being caught by the system operator, hacker affects the operation of HP during the peak times with 20-min intervals. The objective of the scenario is to investigate what happens on the system reliability if a cyber-attack can intrude a heating system in a small discrete-time range during the peak hours. According to original HP load profiles, the peak hours are divided into two parts: morning (03.00–09.00) and night-time (18.00–22.30). The detection-recovery time calculations are developed with four different distribution techniques for this study. The availability calculation of heating system relies on random number generation of detection time by means of following distributions: A-General Pareto, B-Gaussian, C-Pareto, and D-Stable. Fig. 8 shows a comparison of aggregated original HP load profile and HP load profile with cyber-intrusion in consideration of different distributions of MTTC\text{Cyber}. As can be seen from Fig. 8, the main character of the threat's impact is to increase the load demand of HP during morning and night peak times. Increment on utilised electricity in each aggregated profile follows a slight change. There is a clear and discrete increasing trend of electricity utilisation roughly 0.1–0.3 kW during peak hours. This is because of the unavailability ratio of the heating system as a result of an attack. Figs. 8a and c follow a similar pattern and the peak load demand reaches around 2.5 kW. On the other side, aggregated HP load profiles with Gaussian (Fig. 8b) and Stable (Fig. 8d) distribution random numbers have a higher peak (2.9 kW) than Pareto distributions related HP load profiles. It appears that the impact of intrusion on electricity consumption remains in a low-level of increase for all the experiments. Fig. 8 illustrates some of the main impacts of the discrete-time cyber-intrusion on power system reliability. What stands out in Table 3 the is that increment on EENS is in a slight change for all the experiments. In all cases, disparity range of EENS between affected and original HP load profiles changes between 6.459 and 35.407 MWh/year.

Fig. 7 illustrates a comparison of aggregated original HP load profile and HP load profile with cyber-intrusion in consideration of different distributions of MTTC\text{Cyber}. As can be seen from Fig. 8, the main character of the threat's impact is to increase the load demand of HP during morning and night peak times. Increment on utilised electricity in each aggregated profile follows a slight change. There is a clear and discrete increasing trend of electricity utilisation roughly 0.1–0.3 kW during peak hours. This is because of the unavailability ratio of the heating system as a result of an attack. Figs. 8a and c follow a similar pattern and the peak load demand reaches around 2.5 kW. On the other side, aggregated HP load profiles with Gaussian (Fig. 8b) and Stable (Fig. 8d) distribution random numbers have a higher peak (2.9 kW) than Pareto distributions related HP load profiles. It appears that the impact of intrusion on electricity consumption remains in a low-level of increase for all the experiments. Fig. 8 illustrates some of the main impacts of the discrete-time cyber-intrusion on power system reliability. What stands out in Table 3 the is that increment on EENS is in a slight change for all the experiments. In all cases, disparity range of EENS between affected and original HP load

### Table 1 Reliability data for heating system

| Components      | A (failure rate/year) | µ (repair rate/year) |
|-----------------|-----------------------|----------------------|
| compressor      | 0.01354               | 0.1153               |
| condenser       | 0.0268                | 0.1394               |
| evaporator      | 0.00404               | 0.068                |
| expansion valve | 0.00027               | 0.3333               |
| storage         | 0.00404               | 0.0551               |
| switch          | 0.00628               | 0.2381               |
| auxiliary Heater| 0.0536                | 0.3862               |

### Table 2 Utilised time intervals for a smart distribution system

| Cyber-layer transitions | \( r_{\text{in}} \), h | \( r_{\text{pu}} \), h | \( r_{\text{max}} \), h | \( r_{\text{min}} \), h |
|-------------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| secure to \( L_1 \)     | [1–4]                 | —                     | [50–60]               |
| \( L_1 \) to \( L_2 \)  | [1–4] [14–18]         | [35–45]               | [50–60]               |
| \( L_2 \) to \( L_3 \)  | [1–4]                 | [50–60]               | [60–70]               |
| \( L_3 \) to \( L_4 \)  | [1–4]                 | [50–60]               | [60–70]               |
| \( L_4 \) to \( F \)    | [1–4] [14–18]         | [50–60]               | [60–70]               |
| \( F \) to \( S \)      | [1–4]                 | —                     | [50–60]               |
profiles changes between 6.459 and 35.407 MWh/year. Results suggest that Bus 3 is more impacted than Bus 2 in the context of reliability performance. General Pareto and Pareto distributions follow very similar patterns too. However, unavailability rate of the heating system with these distributions is higher than Stable and Gaussian methods of both buses. It is apparent from results that unavailability rate of heating system with stable distribution-detection time technique is less than other techniques for both buses. It means that the performance adaptation of stable detection time on this cyber intrusion process is slightly better than Gaussian detection-time method and others.

3.3 Scenario 2: cyber-attack on heat pump all day along

In this scenario, the target of the intruder is to disturb HP consumers continuously and re-shape the data by making unavailability of the HP system. The number of HP users and detection-recovery time methods are the same as in scenario 1. Fig. 9 presents an overview of the aggregated original HP load profile and HP load profile with continues effect of cyber-intrusions. Compared to scenario 1, it can be clearly seen in Fig. 9 that there is some amount of electricity rise on HP load demand with each detection time method. This increase trend varies between 0.15 and 0.4 kW for each aggregated HP load profile. After the cyber-intrusion on HP user site, the peak HP load reaches almost 3 kW in all cases, except in Gaussian detection-time method. As shown in Fig. 9b, the peak load hits on 3.1 kW in the afternoon. The most striking result to emerge from both Figs. 8 and 9 is that there is another peak time for this HP site, which is at around 13:00–14:00. It is because of the size of the data pool and the increment can be decreased. Table 4 gives EENS changes in between aggregated original HP load profile and HP load profile with cyber-intrusion. Table 4 also gives different detection-time distribution effects on system reliability. EENS disparity ranges are in between 76.366 and 161.703 MWh/year. It is apparent that EENS disparity range is much higher than scenario 1 for both buses. Nevertheless, Bus 2 is more impacted than Bus 3 in the context of the impacts on reliability performance. The reaction of both General Pareto and Pareto distribution-related detection time method on EENS changes is similar as in scenario 1. However, General Pareto and Pareto distributions have a better EENS performance on detection time compared to others. These depict that unavailability of the heating system with Pareto distribution is less than other methods. The results also suggest that General Pareto detection time technique on cyber intrusion process provides better performance in calculating the reliability of the system. These results suggest several outcomes. At first, performance efficacy of detection time technique can rely on the discrete or continuous impact of cyber-intrusions due to the number of iterations of detection time in the analysis. A higher number of iterations increases the performance of Pareto distribution on reliability assessment framework and reflects less
impact on EENS. Secondly, different HP site connections might bring the different impact of cyber-intrusion into power system reliability.

4 Future works
This study is set out to investigate reliability levels of cyber-physical interactive operation of power systems with HPs. Further investigations, using a broader range of detection modelling, could shed more lights on the security of cyber-physical power systems. A greater focus on cyber-security of energy-sucking components of power systems such as temperature sensors of heating, ventilation, and air conditioning and communication sensors of vehicle-to-grid could help to understand interactions with power system operational security. Additionally, future research could also investigate closer links between vulnerability-reliability and resiliency of smart power grids with extensive cyber-attacks which cascade effects through multiple appliances connected at active customers.

5 Conclusion
A composite approach for cyber-physical interactive operation with HP systems is proposed with detailed features of cyber-intrusions. The studies justified the effectiveness of the approach for quantifying the cyber-intrusion impacts on power systems. Sensitivity analysis framework of cyber-intrusion detection-time distributions on a cyber-physical interactive power system is also proposed as an extension to the approach to justify the effectiveness models to estimate mean time to detection for cyber-attack (MTTD_Cyber). Heavy tail distribution applied in the detection-time calculation validated the effectiveness of the models. Investigations further suggest that cyber-intrusion effects on heating systems could bring a considerable impact on the operational reliability of a smart power system.

The proposed approach could serve modern power system engineers to plan and operate their systems considering cyber-physical interactive operating conditions and to plan remedial actions based on prevailing impacts.

6 References
[1] Yu, X., Xue, Y.: ‘Smart grids: a cyberphysical systems perspective’, Proc. IEEE, 2016, 104, (5), pp. 1058–1070
[2] Farhangi, H.: ‘The path of the smart grid’, IEEE Power Energy Mag., 2010, 8, (1), pp. 18–28
[3] Gunduz, H., Khan, Z.A., Altamimi, A., et al.: ‘An innovative methodology for load and generation modelling in a reliability assessment with PV and smart meter readings’. 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, 2018, pp. 1–5, doi: 10.1109/PESGM.2018.8585829
[4] EIA: ‘How many smart meters are installed in the United States, and who has them?’, 2018. Available at https://www.eia.gov/tools/faqs/faq.php?id=108&t=3, accessed 01 July 2020
[5] Lee, R.M., Assante, M.J., Conway, T.: ‘Analysis of the cyber attack on the Ukrainian power grid’, E-ISAC, USA, 2016. Available at https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accessed 01 July 2020
[6] Hemsley, K.E., Fisher, R.E.: ‘History of industrial control system cyber incidents’, Idaho National Lab. (INL), Idaho Falls, ID (United States), 2018.

Table 4 EENS changes for scenario 2

| Detection time technique | General Pareto | Gaussian | Pareto | Stable |
|--------------------------|----------------|---------|--------|--------|
| RBTS Bus 2               |                |         |        |        |
| original HP profiles, MWh/year | 9610.035 | 9344.22 | 9246.872 | 9267.607 |
| affected HP profiles, MWh/year | 9706.609 | 9489.473 | 9349.74 | 9429.31 |
| EENS disparity, MWh/year | 96.574 | 145.253 | 102.868 | 161.703 |
| RBTS Bus 3               |                |         |        |        |
| original HP profiles, MWh/year | 9155.525 | 9094.714 | 9109.013 | 9047.479 |
| affected HP profiles, MWh/year | 9231.891 | 9194.847 | 9186.262 | 9178.57 |
| EENS disparity, MWh/year | 76.366 | 100.133 | 77.249 | 131.091 |

Fig. 9 Scenario 2: comparison of aggregated original HP load profile and HP load profile with cyber-intrusion (according to different distributions of MTTD_Cyber). x-axis represents a day with 10 min resolutions (a) General Pareto distribution, (b) Gaussian distribution, (c) Pareto distribution, (d) Stable distribution

Table 4 EENS changes for scenario 2

| Detection time technique | General Pareto | Gaussian | Pareto | Stable |
|--------------------------|----------------|---------|--------|--------|
| RBTS Bus 2               |                |         |        |        |
| original HP profiles, MWh/year | 9610.035 | 9344.22 | 9246.872 | 9267.607 |
| affected HP profiles, MWh/year | 9706.609 | 9489.473 | 9349.74 | 9429.31 |
| EENS disparity, MWh/year | 96.574 | 145.253 | 102.868 | 161.703 |
| RBTS Bus 3               |                |         |        |        |
| original HP profiles, MWh/year | 9155.525 | 9094.714 | 9109.013 | 9047.479 |
| affected HP profiles, MWh/year | 9231.891 | 9194.847 | 9186.262 | 9178.57 |
| EENS disparity, MWh/year | 76.366 | 100.133 | 77.249 | 131.091 |

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
