SUnMBT4CPS: Security-related Uncertainty Model-Based Testing for Cyber-Physical Systems

Phu H. Nguyen

Simula Research Laboratory, Norway
nguyenhongphu@gmail.com

Abstract— Context: **Cyber-Physical Systems (CPS) are driving the fourth industrial revolution. The more significant impact CPS having on modern world, the more secure CPS must be. But, the complex and heterogeneous nature of CPS makes uncertainty inherent inside CPS. The uncertainty and security challenges of CPS urge for an innovative method for securing CPS. The criticality and complexity of CPS must not allow security to come as an afterthought. *Goal*: We aim to address these challenges by developing a Model-Based Security Testing approach for CPS under uncertainty. *Method*: We propose Security-related Uncertainty Model-Based Testing for CPS (SUnMBT4CPS). We build SUnMBT4CPS on a taxonomy of security-related uncertainty in CPS (SUnCPS). Based on the taxonomy, SUnMBT4CPS allows modelling SUnCPS for security testing purposes. From the test models, SUnMBT4CPS generates test cases for exploring the uncertainty boundary of CPS. *Results*: We have applied SUnMBT4CPS in a case study of smart grids. SUnMBT4CPS allows specifying SUnCPS in the Advanced Metering Infrastructure (AMI) of smart grid. Generated test cases allow discovering security-related uncertainty issues of the AMI. *Conclusion*: SUnMBT4CPS can support testing the uncertainty of CPS rooted from security issues.**

Keywords— Model-Based Testing, MBT, Security Testing, Uncertainty Testing, Cyber-Physical Systems, CPS, Taxonomy, Smart Grids, Advanced Metering Infrastructure, AMI, IoT

I. INTRODUCTION

The fourth industrial revolution has emerged with Cyber-Physical Systems at its core [16]. According to S. Shankar Sastry at UC Berkeley, "*A cyber-physical system (CPS) integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safely, securely, efficiently and in real-time*". CPS would be the game changer for a wide range of the so-called Industry 4.0. CPS is driving the smart manufacturing, smart energy, smart healthcare, and smart automotive industry. CPS is also getting more popular in infrastructures (e.g., transportation, water management, oil and gas pipelines, wind farms), facilities (e.g., airports, space stations and buildings), and military (e.g., drones and unmanned aerial vehicles). CPS technology is transforming the way people interact with engineered systems. This would be comparable with how the Internet has transformed the way people interact with information [1]. An example of CPS is modern power grid systems. In such a smart grid, information and communication technology (ICT) is increasingly integrated throughout the grid. Highly integrated ICT supports novel communication and control functions among physical resources (such as wind farm, solar farm, smart meters), and information and control systems.

The more human beings depending on CPS, the more important that these CPS must be secure. For example, a single security issue in smart grid might lead to city blackout. We should learn an important lesson from engineering information systems in the past. Security often came as an afterthought [8]. It would be impossible to engineer security into any complex system as an afterthought. CPS are often complex and making sure of their security is very challenging. Besides the cyber security challenges of CPS, the security of the physical parts of CPS is a new critical challenge. Software-defined controllers based on computational algorithms control the physical parts of CPS. These critical controllers broaden the attack surface to CPS. Besides, engineering security mechanisms into CPS must solve a tricky constraint in ensuring the confidentiality, integrity, and availability of CPS. To provide confidentiality and integrity in CPS, cryptography, authorisation, and authentication mechanisms are necessary. However, all security mechanisms implemented for a CPS must also ensure sufficient availability. This constraint often limits the utilisation of security mechanisms. If not utilised sufficiently, they may deny access to a critical function of CPS [31]. This aspect adds another dimension to the complexity of CPS, in which uncertainty is very likely to happen and must be handled [39]. From security's point of view, uncertainty in CPS could lead to serious security issues. For example, uncertainties in the functionalities of CPS might lead to security vulnerabilities. Software is the soul of CPS. Thus, software verification and validation techniques would play an essential role in engineering CPS and their security.

Model-Based Engineering (MBE) would be one of the key solutions to the handling of complex systems [4], including CPS [3]. One of the main ideas of MBE is the engineering focus at the model level, a higher level of abstraction than the code level. MBE methods also aim for engineering the security of these systems. MBE process would start very early and throughout the development life cycle as surveyed by [25, 26]. MBE would allow engineering security better together with the system. MBE could provide the foundations for (semi) automated (formal) verification or validation of systems [35] and their security [12]. A recent study [40] assesses the state of the art and the state of the practice in the verification and validation (V&V) of CPS. The authors

suggest that model-based approaches are gaining momentum. According to [40], model-based approaches will emerge as applicable to general purpose CPS. The V&V work for the security of CPS is still at an early stage. This area should get more attention from the research community [23]. This paper reports our research work for the validation of CPS security with Model-Based Testing (MBT). We have developed an MBT approach for testing the security-related uncertainty of CPS. We call this approach as Security-related Uncertainty Model-Based Testing for Cyber-Physical Systems (SUnMBT4CPS). We have developed SUnMBT4CPS on a taxonomy of security-related uncertainties in CPS (SUnCPS) [24]. The SUnCPS taxonomy allows us to specify different kinds of security-related uncertainty in the security test models of CPS. SUnMBT4CPS generates test cases from test models. The generated tests specialise in discovering the security-related uncertainties in CPS.

To stay ahead of security nightmares in the era of CPS, we need a common understanding on the security aspects and uncertainty of CPS. Learning from the security issues of information systems in the past, the security of critical CPS must not come as an afterthought while engineering such complex systems [23]. Besides, uncertainty is inherent in CPS and must be tackled, preferably together with security. We believe considering security-uncertainty as a first-class concept improves the boundary of security testing for CPS. In this direction, our research focuses on the security-related uncertainty in CPS. Based on the SUnCPS taxonomy, we define a conceptual model for capturing the security-related uncertainty of CPS. The conceptual model enables modelling CPS with their security uncertainties as test models. From SUnCPS test models, SUnMBT4CPS allows generating test cases for discovering security-related uncertainty in the CPS under test (CPSUT). The main contributions of this paper are as follows:

(1) A taxonomy of security-related uncertainty of CPS;

(2) A conceptual model and security pattern-like template for specifying security-related uncertainty of CPS, and

(3) A model-based testing approach for testing the security-related uncertainties of CPS with a proof-of-concept case study of Advanced Metering Infrastructure (AMI).

The remainder of this paper is structured as follows. Section II shows the background concepts used in this paper. Section III discusses a running example and the technical motivation of our work. Section IV presents the SUnCPS taxonomy of Security-related Uncertainty in CPS. In Section V, we present our MBT approach for discovering the security-related uncertainty in CPS. Section VI shows how our SUnMBT4CPS approach has been applied to a case study of AMI. We discuss the related work in Section VII. Finally, Section VIII provides our conclusions and some points for future work.

II. Background

This section provides the background concepts: CPS (Section II.A), CPS' Security (II.B), CPS' Uncertainty (II.C), and Model-Based Testing (II.D).

A. Cyber-Physical Systems

According to [28], "*CPS are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core*". Figure 1 shows an abstraction of CPS in which the physical elements are monitored and controlled via the controllers (on top) with the coordination of the computing centres (right) through communication means (left).

Fig. 1. An abstraction of CPS.

In [18], the authors surveyed the popular application domains of CPS as follows: Vehicular Systems and Transportation (e.g. smart car); Medical and Health Care Systems; Smart Homes and Buildings; Social Network and Gaming; Power and Thermal Management; Data Centres (operating like CPS to keep energy costs for computation and cooling minimal); Electric Power Grid and Energy Systems (e.g. smart grid); Networking Systems; Surveillance.

B. Cyber-Physical Systems' Security

Most (if not all) CPS are security-critical systems. The high-level security concerns (objectives) of CPS are not different from the traditional security concerns of computer security, e.g., confidentiality, integrity, availability (CIA), and accountability. Only that the details of each security concern must be interpreted in the context of CPS, e.g., as given in [7], which bring up new security challenges, e.g., in protecting (the controllers of) physical devices. We adopt some definitions of the generic security concerns from [6, 20] and CPS specific ones from [7] as follows.

"*Confidentiality is the concealment of information or resources*" [6]. In CPS, the state of the physical system must be kept confidential from unauthorized parties, i.e. sufficient security mechanisms must prevent eavesdropping on the communication channels, e.g. between a sensor and a controller, and between a controller and an actuator.

"*Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change*" [6]. Integrity in CPS can be viewed as the ability to maintain the operational goals by preventing, detecting, or surviving deception attacks in the information sent and received by sensors, controllers, and actuators.

"*Availability refers to the ability to use the information or resource desired*" [6]. Lack of availability could result in denial of service (DoS). A DoS attack is characterized by an explicit attempt to "prevent the legitimate use of a service". The goal of availability in CPS is therefore, to maintain the operational goals by preventing or surviving DoS attacks to the information collected by the sensor networks, commands given by controllers, and physical actions taken by actuators.

There could be new challenges for ensuring availability in many CPS whose real-time constraints are critical.

C. Cyber-Physical Systems' Uncertainty

Walker et al. [36] define the term uncertainty as: "*any departure from the unachievable ideal of complete determinism*." In the context of CPS, we recall a definition of uncertainty from [39]: "*Uncertainty is a state of a CPS that is unpredictable, a future outcome from the state may not be determined, or there is a possibility of more than one outcome from the state*". Uncertainty and security are two of the main essential characteristics of CPS bringing huge challenges that need to be addressed in research. Uncertainty and security of CPS could intertwine in different ways. A security incident (e.g., caused by attackers) or misconfiguration may lead to uncertainty. Vice versa, uncertainty may lead to security vulnerabilities that could be exploited by attackers. This security-related uncertainty can occur in a CPS because of 1) ambiguous or missing security requirements; false security assumption; false security goals; 2) the possible security misconfiguration, incorrect implementation, or wrong security policy that could prevent the CPS to operate certainly; and 3) the possible security vulnerabilities or misconfiguration of the CPS that could lead to successful security attacks; the unpredictable security attacks aiming at the CPS.

It is important to note that in complex systems such as CPS, uncertainty is very likely to happen and must be handled, especially regarding security. The primary goal of any cyber-physical system is to provide efficient control over some physical process. This naturally prioritizes information integrity and availability to ensure control state closely mirrors the physical system state. Security mechanisms such as cryptography, access control, and authentication are necessary to provide integrity in systems. However, all security mechanisms tailored for this environment must also provide sufficient availability. The implementation of security mechanisms needs to be tested systematically because they may cause uncertainty in CPS, e.g. denying access to a critical function. Considering the possible security issues of CPS, the security-related uncertainty of CPS could be threefold. First, some uncertainty in the functionalities of CPS (or the integration of different CPS components) might lead to vulnerabilities that could be exploited by an adversary, either attacker or malicious user. Vice versa, security attack could cause many uncertainties in the functionalities of CPS. Third, any uncertainty in the specification, implementation and evolution of security mechanisms might cause other uncertainties in the functionalities of CPS, e.g. incorrect access control can disable some physical process, especially whose real time requirement is critical. Therefore, the security-related uncertainty of CPS is a critical problem that needs to be researched and tackled systematically.

Definition of Security-Related Uncertainty for CPS: A security-related uncertainty of CPS is any violation in the security or functionality specification of CPS that caused by security-related reasons. These security-related reasons are either internal mismatches/incompatibility between the implemented security solutions of CPS or external attacks/misuses.

D. Model-Based Testing

Testing is currently the most widely used technique in industry to gain some confidence in the quality of a system, normally in a cost-efficient way. MBT is a variant of testing that mainly encompasses the insight of using models, e.g. UML models that are extended for the purpose of testing of real-time embedded systems such as the OMG UML Testing Profile [2] for testing, and OMG MARTE [13] for Modelling and Analysis of Real-Time and Embedded Systems. More specifically, MBT relies on the behaviour models of a system under test (SUT) and/or its environment to (automatically) derive test cases for the system. Therefore, MBT allows the tests derivation process to be structured, reproducible, programmable, and documented. The results of a recent MBT User Survey suggest that MBT has positive effects on efficiency and effectiveness [5]. MBT approach is more systematic, and more effective in detecting issues compared to the manual testing approach in certain areas [30].

III. Motivating Example

To demonstrate for the motivation of our work on the SUnMBT4CPS, we introduce an example used throughout the paper. Smart grids would be one of the most popular instances of CPS [21]. The Advanced Metering Infrastructure (AMI) of a smart electricity grid is our focus as the CPSUT. From a cyber security perspective, the AMI seems to introduce the greatest concern due to its integration within a community, and ability to impact consumer's privacy and electricity availability [14]. AMI is an integrated CPS of smart meters, communications networks, data management systems, and head-end system(s). We synthesised the functional and security requirements of AMI from an industrial smart grid [15], from the NIST's Guidelines for Smart Grid Cyber Security [27], and from the EPRI Use Case Repository [10]. The AMI enables two-way communication between smart meters and the head-end system (Fig. 2). Smart meters periodically report meter readings (via collectors) to the AMI head-end. The head-end is the system that controls the AMI. The head-end uses the electricity consumption data for real-time pricing calculation. The head-end communicates the real-time pricing data to smart meters for consumers to customise their consumption. The two-way communication also allows remote on-demand meter reading by the head-end. Moreover, the AMI head-end can perform meter remote connect or disconnect, e.g., remote disconnect for non-payment.

Security mechanisms must be in place to protect the integrity of exchanged messages, avoid fake messages, fake senders, unintended receivers, and manipulated messages [27]. Security mechanisms must also ensure the confidentiality of sensitive data such as smart meters' status, exchanged messages. Security mechanisms must ensure the availability of key operations such as timely connectivity for connect/disconnect service, on-demand meter reading.

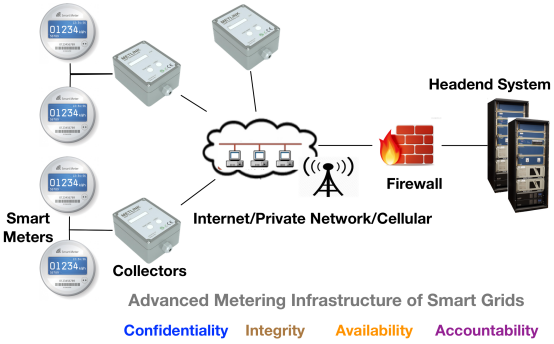

Fig. 2. An overview of Advanced Metering Infrastructure.

The AMI as a security-critical CPS faces the security and uncertainty challenges discussed in Section II. For example, it is challenging to protect smart meters from security attacks because they are deployed at consumers' side. An external attacker could tamper smart meter to inject falsified on-demand meter reading being exchanged with head-end. The intrusion detection mechanism of head-end could single out the tampered data and mark the meter as suspicious meter. This leads to the failure of on-demand meter reading operation. We call this type of uncertainty with external cause (attacker) is external SUn.

Another type of SUn is internal SUn. For example, time-consuming security mechanisms at smart meter cause the responses of meter to head-end longer than an expected threshold. If a response of smart meter, e.g., on-demand meter reading, is longer than a threshold, head-end will mark meter as suspicious. The on-demand meter reading of suspicious meter failed. This is called a false alarm of suspicious meter. We need to expand the boundary of security testing to these uncertain cases.

IV. The SUNCPS Taxonomy

To understand security together with uncertainty, we propose SUnCPS, a taxonomy of security-related uncertainty in the context of CPS. SUnCPS can provide a structured representation of security-related uncertainty in CPS as the basis for different (early) security engineering activities for CPS such as security risk analysis and management, vulnerability/attack analysis, and security testing for CPS.

This section presents our classification of the security-related uncertainties in CPS. There are two main categories of security-related uncertainties. First, internal insufficient interaction between security mechanisms and CPS's functional operations could introduce security-related uncertainties for either security mechanisms or functional operations or both. The application of extreme restrictions in systems to uphold confidentiality or integrity could cause a loss of availability. Second, external security attacks could introduce security-related uncertainties for CPS's functional operations and security properties. For CPS, safety should be considered hand in hand with security. Without security, there can be no safety for the human or environment, and/or no safety for the CPS itself.

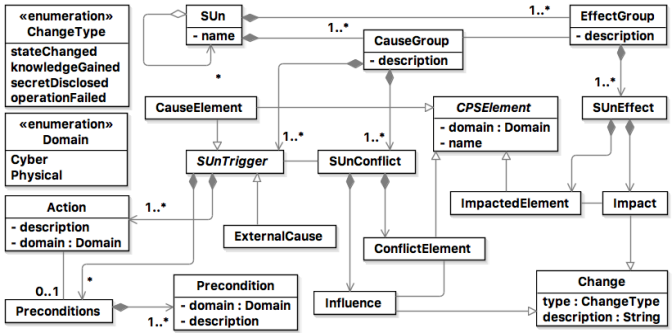

Fig. 3. A conceptual model of the SUnCPS taxonomy.

We proposed an initial version SUnCPS taxonomy in [24]. We have been developing the SUnCPS taxonomy by 1) inheriting the literature of cyber security and system theory that are applicable for CPS [37], and 2) synthesizing the possible security issues of CPS in different CPS application domains. Fig. 3 shows an overview of the SUnCPS taxonomy.

Specifically, a SUn consists of at least one *CauseGroup*, and a corresponding number of *EffectGroup*(s). Each *CauseGroup* associates with its corresponding *EffectGroup* to specify the cause-effect of a SUn. Each *CauseGroup* consists of at least one *SUnTrigger*, and a corresponding number of *SUnConflict(s)*. Each *SUnConflict* specifies the CPS element (*ConflictElement*) that being conflicted with the *Action* done by the *SUnTrigger*. Each *Action* may have *Precondition*(s) before it can happen. Each *SUnConflict* also specifies the *Influence* (*Change*) caused by the conflict.

Each *EffectGroup* consists of at least one *SUnEffect* of the corresponding *CauseGroup*. *SUnEffect* indicates the *ImpactedElement* and the *Impact* made on the *ImpactedElement*. We can see that, in a simple case, a single *SUnTrigger* and a corresponding *SUnConflict* can lead to the unexpected change of a single property of the same or a different single *ImpactedElement* of *SUnEffect*. However, this scenario would not be always the case. In complex CPS, only simultaneous *SUnTrigger*(s) and *SUnConflict*(s) performed on several elements would lead to the *SUnEffect*(s) of uncertainty. In other words, there would need different *SUnTrigger*(s) and *SUnConflict*(s) together to cause a single uncertainty with *SUnEffect*(s).

SUnTrigger, *SUnConflict* and *SUnEffect* can together specify how a SUn is propagated inside the cyber parts, or physical parts, or crossing between cyber-physical parts of CPS. This crosscut nature between cyber-physical parts is because of the different domains of cause/effect's elements. In addition, each *SecurityUncertainty* is an unexpected change inside the system. Thus, each *SecurityUncertainty* might trigger follow-up *SecurityUncertainty*(ies). In other words, the *SUnEffect* of a SUn would play as the *SUnConflict* of a follow-up SUn to form a chain of effect propagations. A chain of uncertainty is possible because the cyber and physical parts of CPS are highly interconnected and dependent in complex ways. Thus, failures in one part can cross borders and cascade onto another, as happened in practice among critical infrastructures discussed by [19]. The SUnCPS supports

specifying possible chains of uncertainty to test the resilient of CPS against any significant consequences.

Unlike traditional IT systems, the respond time and availability of CPS in many cases must be ensured. For example, if an important function of a smart healthcare CPS such as pace maker were unavailable, a human life would be lost. In another example, if the response time of a smart meter were over a threshold, the meter would be marked as suspicious meter by the AMI head-end by its intrusion detection system. Availability would be more important than integrity and confidentiality for many CPS. However, the response time of a CPS's function cross-domain call may be unpredictable because it would depend on different factors such as transmission delays, hardware devices' computing power, or security controls. A cross-domain-call, e.g., from cyber part to a physical part of a CPS, will involve different parts of a CPS that often interconnect via different communication means and technologies. An analytical model quantifying the system's response time may be error-prone because of the heterogeneous nature of CPS. For example, such a model would only account for the dominant factors, such as the execution time of components, and ignore others, such as the transmission delay difference between TCP and UDP [11]. Even if the model were not wrong; an underestimation of execution environment would make the outcome of model less accurate.

We have used SUnCPS to specify different SUn instances in the smart grids system. Because of space limitation, we only show two representative instances of SUn for the AMI mentioned in Section III. First, we use the SUnCPS taxonomy to specify the "*internal*" SUn of the AMI (TABLE I.).

TABLE I. A SUNCPS EXAMPLE: FALSE ALARM OF SUSPICIOUS METER

Cause Group	**Cause**		
	Trigger	***Influence***	***Conflict Element***
Strict Security	Authen(Cyber, Authen module)	ODMR[a]	Intrusion Detection System
Effect Group	**Effect**		
	Impacted Element	***Impact***	***Description***
SUn Effect 1	ODMR	ODMR operation failed	When a meter is marked as suspicious, all its meter readings are not accepted by the HE
SUn Effect 2	PMR[b]	PMR operation failed	Same as above

[a.] On-demand meter reading.

[b.] Periodic Meter Reading

TABLE I. shows an example of internal SUnCPS, which is the False Alarm of Suspicious Meter caused by a delayed On-Demand Meter Reading. This is called an internal SUnCPS if the reason for the delay is internal security mechanisms such as heavy authentication, authorisation, and encryption. Security attacks are other main causes of uncertainty for CPS. The complexity and heterogeneous nature of CPS brings on new security challenges that have not been addressed. Cyber attack can be used to induce physical consequences [17]. Vice versa, physical attacks can affect the cyber system. Hybrid attacks crossing cyber domain and physical domain are new challenges [22]. Neither cyber security nor system theory alone is sufficient to ensure CPS security even though each area has achieved remarkable success in defending against pure cyber or pure physical attacks. In this work, we call uncertainty caused by security attacks as external SUnCPS. The Real Alarm of Suspicious Meter caused by a tampered On-Demand Meter Reading can be classified as an external SUnCPS if security attack is the reason. This means that an attacker has tampered the meter and altered the ODMR value. The ODMR returned by the tampered meter will be detected by the intrusion detection system (IDS) of AMI Headend. The IDS will mark the meter as suspicious meter, making the ODMR procedure failed. Another example of external SUnCPS is Fake Power outage notification. This is a fault replay attack attempts to emulate a valid fault by altering system measurements to mimic a Power outage, from compromised meters to send fake Power outage notifications to AMI head-end.

V. SECURITY-RELATED UNCERTAINTY TESTING FOR CPS

Our approach **S**ecurity-related **Un**certainty **M**odel-**B**ased **T**esting for **CPS** (SUnMBT4CPS) specifically supports for testing the uncertainty hand in hand with the security of CPS. We focus on testing both kinds of SUn: internal SUn, and external SUn.

First, internal SUn(s) are the (marginal) possible errors in the constraints and interactions between the security solutions and functionalities in a CPS. It is important to note that the nature of CPS (e.g., heterogeneous, limited computing power in some field physical devices) could often make attaining some sort of absolute security satisfying all three CIA principles very difficult. For example, the application of extreme restrictions in CPS to uphold confidentiality and integrity could cause a loss of availability. SUn can provide a systematic way to explore and document these kinds of internal security mismatches in CPS. Based on that, we build a threat model wrt. CPS specification.

On the other hand, CIA principles tend to focus on preventive measures, which in most cases will not be always guaranteed. Therefore, another type of security-related uncertainty that SUn can help to specify is the external causes of security-related uncertainty for CPS, called external SUn. The external causes come from the attackers or malicious users of CPS, who can leverage some sorts of uncertain behaviours of CPS or uncertain security mechanisms to attack. We need to test that the CPSUT has to behave in a secure way even if it is under attack. External SUn in terms of attack can be instantiated as malicious CPS components. Thus, we first specify external SUn in threat model wrt. CPS specification: e.g., connection means are vulnerable, and can be accessed and manipulated by an intruder.

Fig. 4 gives an overview of the main framework of our SUnMBT4CPS, which consists of two main phases (at the

bottom line): SUn modelling and SUn test generation. The SUnCPS taxonomy presented above is the basis for developing the SUnCPS UML profile that allows us to specify different kinds of security-related uncertainty in the CPS. Specifically, SunTrigger element can be assigned to a state in the state machine of a CPS element. The "trigger" state means the CPS is in a state that might cause uncertainty. For example, in case of a false alarm of ODMR, the trigger state is that "meter receiving an ODMR request". Based on the SUnCPS UML profile, the SUnMBT4CPS framework facilitates the process of modelling security-related uncertainties. We rely on the UTP V.2 to model the testing aspects of test ready models.

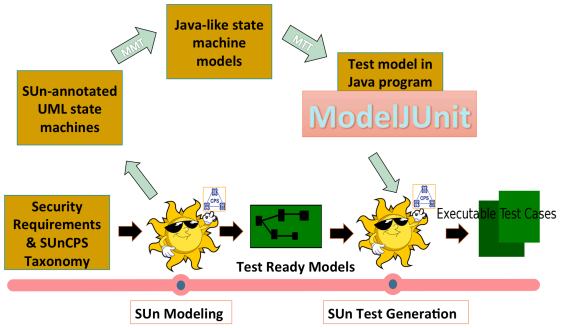

Fig. 4. An overview of SUnMBT4CPS.

The test-ready models are the input to the test generation strategies for automatically generating test cases. The top of Fig. 4 shows more details about the modelling and test generation processes. Specifically, we use the SUnCPS UML profile to annotate the test-ready models (class diagram and state machine diagrams) with SUn(s). The behaviours in state machine diagrams are extended with some uncertain behaviour. We specified and implemented a generic model-to-model transformation (MMT) to transform the SUn-annotated UML state machines to the Java-like state machine models. We then leveraged model-to-text transformation (MTT) to generate the test model in Java program of the Java-like test models [33]. Fig. 5 shows a partial Java-like test model of the AMI, which is equivalent to a Java class executable by the test engine ModelJUnit [32] to run all the tests in the test model.

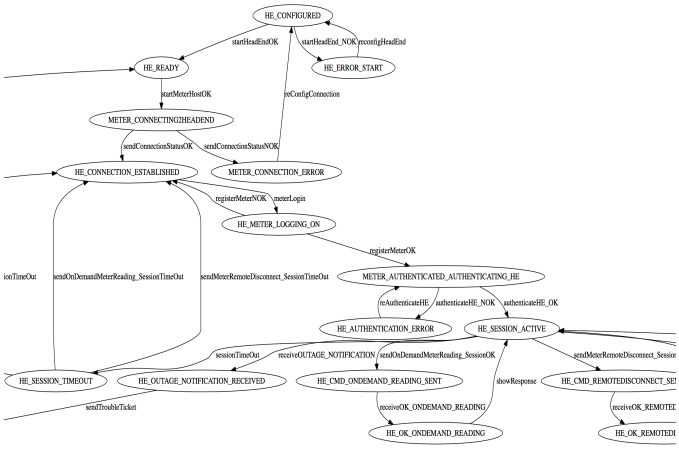

Fig. 5. Partial Test Model of the AMI.

The test engine ModelJUnit [32] mentioned in [33] can execute the test models in Java programs for testing a SUT. The test execution process of a SUT can be done via its test adaptors if needed.

Our hypothesis is that SUnMBT4CPS can support for testing the new challenges in the security of CPS; for the highly interdisciplinary nature of CPS; and for expanding the boundary of testing to reduce the uncertainty regarding security for CPS. With the SUnMBT4CPS approach, the boundary for testing the security and security-related uncertainty of CPS can be expanded and more systematic because security-related uncertainty is explicitly taken into account in an MBT approach for CPS. By taking into account the interactions among the security mechanisms and functionalities the physical and cyber elements of CPS, SUnMBT4CPS can tackle the new challenges for the security of CPS.

VI. Case Study

We are evaluating our SUnMBT4CPS approach in testing the security-related uncertainty for the Advanced Metering Infrastructure (AMI) of a Smart Grid project. Fig. 6 shows the prototype of the AMI, which consists of AMI Head-end system(s), collectors, and smart meters. Security is a must for the AMI system, but indeed is a big challenge due to possible uncertain conflicts between security mechanisms and AMI operations, and big threats of cyber attacks.

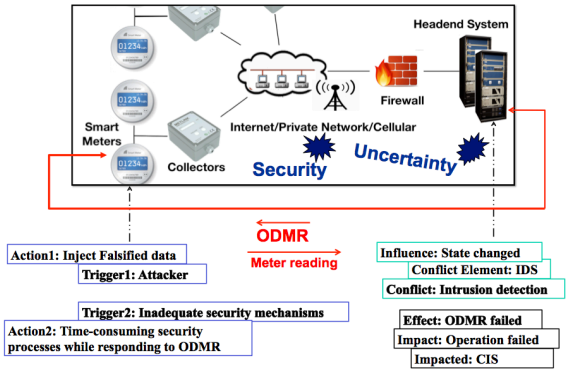

Fig. 6. (False) alarm of on-demand meter reading.

CPSUT is implemented as a simulation in Java, with all public methods of classes available for testing. The uncertainty occurs when there is some unexpected behaviour in the **interaction** between head-end and meter. For example, it may take too long for a meter to process a request because of its wrong/insufficient implemented security policy. The AMI head-end cannot distinguish the reason of over-time response from meter: whether due to insufficient security policy processing or malicious/tampered process. Fig. 6 shows how the (false) alarm of suspicious meter would happen. On the left side, Action 1 is a possible trigger of an external SUnCPS (attacker). Action 2 is a possible trigger of an internal SUnCPS. On the right side, it shows that both of them can lead to the similar influence and effect, i.e., SUnCPS. Fig. 7 presents the metrics after executing the test model of the AMI, which aims to cover possible SUnCPS in the taxonomy.

The test engine ModelJUnit executed the test model ensuring the transition-pair coverage. This strategy also makes sure that all the actions and states in the test model are covered.

```
********** Testing Metrics **********
Generated 1568 steps.

ActionCoverage Metric details:  {sendOnDemandMeterReading_SessionTimeOut=9, sendConnectionStatusOK=69, sendMeter
StateCoverage Metric details:  {HE_CMD_REMOTEDISCONNECT_SENT=20, HE_CMD_ONDEMAND_READING_SENT=29, HE_READY=133,
TransitionCoverage Metric details:  {(HE_SESSION_ACTIVE, sendMeterRemoteDisconnect_SessionOK, HE_CMD_REMOTEDISC(
TransitionPairCoverage Metric details:  {(HE_METER_LOGGING_ON, registerMeterOK, METER_AUTHENTICATED_AUTHENTICAT

action coverage: 27/27
state coverage: 19/19
transition coverage: 29/29
transition-pair coverage: 53/53
```

Fig. 7. Execute the Test Model with test strategy Transistion-pair coverage.

Specifically, 1568 steps are executed to make sure the transition-pair coverage. Fig. 8 shows that the test model has covered the internal SUnCPS of false alarm of ODMR. In this case, if the response time of a meter to the head-end is more than one second, the meter will be marked as a suspicious meter. However, the heavy security mechanisms at the meter lead to the response time more than one second. The effect of this false alarm is that the ODMR operation failed. In other words, the test of expected ODMR operation has failed.

```
[SmartMeter] Received an ON-DEMAND METER READING command from AMI HeadEnd. Code = CMD_ONDEMAND_READING
[HEAD-END] isSessionActive() SESSION_401f1f07-a23c-4f70-8d9f-d6f237456a9c while receiving OK_ONDEMAND_READING
[HEAD-END] OK_ONDEMAND_READING: ALERT!!!!!!!!!! Time used = 1.014 second(s). Marked Meter as SUSPICIOUS_METER
[HEAD-END] FINISHED wait4RespondFromSmartMeter
[SmartMeterSession] Renew timeout for getSessionID() = SESSION_401f1f07-a23c-4f70-8d9f-d6f237456a9c and getLastAccessedTime (seconds ago) = 1.026
[SmartMeterSession] Timeout set to 60 seconds for sessionID = SESSION_401f1f07-a23c-4f70-8d9f-d6f237456a9c
VerboseListener: done (HE_SESSION_ACTIVE, sendOnDemandMeterReading_SessionOK, HE_CMD_ONDEMAND_READING_SENT)

***Running Step 1566

***[HEAD-END] RECEIVE A RESPONSE FROM SMART METER***
 Smartmeter METER_5416ea61-1f57-48a8-8370-51e28f842fbe sent a response code: SUSPICIOUS_METER
**********


[HEAD-END] ***RECEIVE A RESPONSE FROM SMART METER***
 Smartmeter /127.0.0.1 sent a response code: SUSPICIOUS_METER
**********

[HeadEndTestSuiteAdaptor] : Test FAILED at method receiveOK_ONDEMAND_READING for meter METER_5416ea61-1f57-48a8-8370-51e28f842fbe
VerboseListener: done (HE_CMD_ONDEMAND_READING_SENT, receiveOK_ONDEMAND_READING, HE_OK_ONDEMAND_READING)
```

Fig. 8. Uncertainty in policies leads to false alarm of suspicious meter.

In another test, it covers the case if a meter is really tampered by an attacker, who could even trigger a fake power outage notification. Fig. 9 shows the test failed for this uncertainty scenario caused by attacker.

```
***Running Step 1427
[HEAD-END] waiting to receiveOUTAGE_NOTIFICATION 4 meter METER_c53e222c-0a2b-46c1-80d2-4aa021ba8c88
[HEAD-END] wait4OutagePackage...
[HEAD-END] isSessionActive() SESSION_4daa0dfd-c44e-47e2-b8fb-b680eedca24f while receiving OUTAGE_NOTIFICATION
[HEAD-END] Responded OUTAGE_NOTIFICATION = PACKAGE_3b3ea51c-761a-45d2-a66f-37a2edc285dd
cancelWaiting4OutagePackage!!!
[HEAD-END] FINISHED wait4OutagePackage
[SmartMeterSession] Renew timeout for getSessionID() = SESSION_4daa0dfd-c44e-47e2-b8fb-b680eedca24f and getLastAccessedTime (seconds ago) = 0.012
[SmartMeterSession] Timeout set to 60 seconds for sessionID = SESSION_4daa0dfd-c44e-47e2-b8fb-b680eedca24f

[HEAD-END] ***RECEIVE A RESPONSE FROM SMART METER***
 Smartmeter /127.0.0.1 sent a response code: OUTAGE_NOTIFICATION
**********

VerboseListener: done (HE_SESSION_ACTIVE, receiveOUTAGE_NOTIFICATION, HE_OUTAGE_NOTIFICATION_RECEIVED)

***Running Step 1428
VerboseListener: done (HE_OUTAGE_NOTIFICATION_RECEIVED, sendTroubleTicket, HE_TROUBLE_TICKET_SENT)

***Running Step 1429
[HeadEndTestSuiteAdaptor] : Test FAILED at method removeOutagedMeter for meter METER_c53e222c-0a2b-46c1-80d2-4aa021ba8c88
```

Fig. 9. Tampered meter leads to the power outage notification failed.

VII. Related Work

Uncertainty in software and systems has emerged as an important topic because of the highly interactive nature with unpredictable environment in modern systems such as adaptive systems [11] [29], cyber-physical systems [39], [38]. In [11], the sources of uncertainty in adaptive systems drive the classification of uncertainty's characteristics and impacts to adaptive systems. In [29], the different causes at different stages in the lifecycle of adaptive systems form the taxonomy of uncertainty for adaptive systems. The authors of both [11] and [29] looked into uncertainty from the point of view for engineering adaptive systems. Our approach has the point of view for security-related uncertainty testing of CPS.

Related work in [39], [38] could be the first to explicitly tackle the uncertainty for CPS but not yet to specifically consider the security issues for CPS. In [39], the authors propose an uncertainty taxonomy to support MBT of CPS. Based on the taxonomy, the authors of [38] propose evolution algorithms to evolve the test models for discovering more unknown uncertainty. The taxonomy presented in [39] is generic for supporting uncertainty testing of CPS in general. Our work is inspired from this work but focuses on the uncertainty aspects regarding the security of CPS.

The authors of [9] propose an MBT approach for testing real-time systems under uncertainty. There is no formal definition of uncertainty in [9]. Their testing focus is the "*timing uncertainty of uncontrollable actions*". This approach is neither for security testing, nor for testing CPS with its physical nature. It shares the nature of an MBT approach with test case generation. While they use timed automata for test case generation, our approach uses standard UML state machines annotated with SUn UML profile. Our work focuses on testing security-related uncertainty.

The authors of [34] surveyed the recent Model-Based Security Testing approaches. But the surveyed approaches neither explicitly deal with CPS nor the uncertainty problem of CPS. In summary, SUnMBT4CPS is the first approach that deals with the uncertainty aspect regarding security of CPS. This security uncertainty-wise approach is unique also in combination with MBT methodology. On the other hand, the application domain of CPS introduces new challenges for security testing of CPS compared to the traditional security testing, e.g., regarding the impact of cyber attacks to physical elements in CPS, or the effects of security uncertainty to the controlling and monitoring systems in CPS.

VIII. Conclusions

SUnMBT4CPS is proposed to address the following main reasons. First, CPS is going to be dominant in the modern life with Industry 4.0 that is transforming our modern world. Second, the security of many critical CPS cannot come as a second thought like IT systems in the past. Third, the uncertainty and security in CPS are intertwined, that should be taken into account together. Fourth, MBT can provide the basis for systematically manipulating different scenarios and reasoning about the interactions between security and uncertainty.

In this paper, we have showed why the security for CPS is of paramount importance. Because security must not come as an after thought while developing CPS, the notion of security by design should be promoted. In this direction, we have developed an approach of Security-related Uncertainty Model-Based Testing for Cyber-Physical Systems (SUnMBT4CPS). We have showed the research hypothesis of SUnMBT4CPS that could provide an innovative way of dealing with the uncertainty for ensuring the security of CPS. Finally, we have discussed the importance of our approach as well as the uniqueness of SUnMBT4CPS. Future work includes completing the SUnMBT4CPS framework with customizable test generation strategies and a more complete evaluation based on a case study of Advanced Metering Infrastructure.

ACKNOWLEDGMENT

The Research Council of Norway (RCN) supports this work under the MBT4CPS project.

REFERENCES

[1] (NSF), N.S.F. *Cyber-Physical Systems (CPS) PROGRAM SOLICITATION NSF 16-549*. 2016 [cited 2016 May 2016]; Available from: http://www.nsf.gov/pubs/2016/nsf16549/nsf16549.htm.

[2] Bagnato, A., A. Sadovykh, E. Brosse, and T.E.J. Vos. *The OMG UML Testing Profile in Use--An Industrial Case Study for the Future Internet Testing*. 2013. IEEE.

[3] Balaji, B., A. Faruque, M. Abdullah, N. Dutt, R. Gupta, and Y. Agarwal. *Models, abstractions, and architectures: the missing links in cyber-physical systems*. in *Proceedings of the 52nd Annual Design Automation Conference*. 2015. ACM.

[4] Bézivin, J., *Model driven engineering: An emerging technical space*, in *Generative and transformational techniques in software engineering*. 2006, Springer. p. 36-64.

[5] Binder, R.V., B. Legeard, and A. Kramer, *Model-based testing: where does it stand?* Communications of the ACM, 2015. **58**(2).

[6] Bishop, M., *Computer security: art and science*. Vol. 200. 2012: Addison-Wesley.

[7] Cardenas, A.A., S. Amin, and S. Sastry. *Secure control: Towards survivable cyber-physical systems*. in *The 28th International Conference on Distributed Computing Systems Workshops*. 2008. IEEE.

[8] Cysneiros, L.M. and J.C. Sampaio do Prado Leite, *Non-functional requirements: from elicitation to modelling languages*, in *Proceedings of the 24th International Conference on Software Engineering, 2002. ICSE 2002*. 2002. p. 699-700.

[9] David, A., K.G. Larsen, S. Li, M. Mikucionis, and B. Nielsen. *Testing real-time systems under uncertainty*. in *Formal Methods for Components and Objects*. 2012. Springer.

[10] EPRI, E.P.R.I., *The EPRI Use Case Repository* http://smartgrid.epri.com/Repository/Repository.aspx. 2012. Available from: http://smartgrid.epri.com/Repository/Repository.aspx.

[11] Esfahani, N. and S. Malek, *Uncertainty in self-adaptive software systems*, in *Software Engineering for Self-Adaptive Systems II*. 2013, Springer. p. 214-238.

[12] Felderer, M., P. Zech, R. Breu, M. Büchler, and A. Pretschner, *Model-based security testing: a taxonomy and systematic classification*. Software Testing, Verification and Reliability, 2015.

[13] Gérard, S. and B. Selic, *The UML–MARTE Standardized Profile*. IFAC Proceedings Volumes, 2008. **41**(2): p. 6909-6913.

[14] Hahn, A. and M. Govindarasu, *Cyber attack exposure evaluation framework for the smart grid*. Smart Grid, IEEE Transactions on, 2011. **2**(4): p. 835-843.

[15] Hartmann, T., F. Fouquet, J. Klein, G. Nain, and Y. Le Traon, *Reactive security for smart grids using models@ run. time-based simulation and reasoning*, in *Smart Grid Security*. 2014, Springer. p. 139-153.

[16] Jazdi, N. *Cyber physical systems in the context of Industry 4.0*. 2014. IEEE.

[17] Karnouskos, S. *Stuxnet worm impact on industrial cyber-physical system security*. in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*. 2011. IEEE.

[18] Khaitan, S.K. and J.D. McCalley, *Design techniques and applications of cyberphysical systems: A survey*. Systems Journal, IEEE, 2015. **9**(2): p. 350-365.

[19] Kröger, W. and E. Zio, *Vulnerable systems*. 2011: Springer Science & Business Media.

[20] McGraw, G., *Software security: building security in*. Vol. 1. 2006: Addison-Wesley Professional.

[21] Mitchell, R. and I.-R. Chen, *A survey of intrusion detection techniques for cyber-physical systems*. ACM Computing Surveys (CSUR), 2014. **46**(4): p. 55.

[22] Mo, Y., T.H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, *Cyber–physical security of a smart grid infrastructure*. Proceedings of the IEEE, 2012. **100**(1): p. 195-209 %@ 0018-9219.

[23] Nguyen, P.H., S. Ali, and T. Yue, *Model-based security engineering for cyber-physical systems: A systematic mapping study*. Information and Software Technology, 2017. **83**: p. 116-135. Available from: http://www.sciencedirect.com/science/article/pii/S0950584916303214.

[24] Nguyen, P.H., S. Ali, and T. Yue, *SUnCPS: A Taxonomy of Security-related Uncertainty in Cyber-Physical Systems*, in *ESSoS (Poster)*. 2017: Bonn.

[25] Nguyen, P.H., J. Klein, Y. Le Traon, and M.E. Kramer, *A Systematic Review of Model-Driven Security*, in *Software Engineering Conference (APSEC, 2013) 20th Asia-Pacific*. 2013. p. 432-441.

[26] Nguyen, P.H., M.E. Kramer, J. Klein, and Y. Le Traon, *An Extensive Systematic Review on the Model-Driven Development of Secure Systems*. Information & Software Technology, 2015. **68**: p. 62-81.

[27] NIST, *NISTIR 7628-Guidelines for Smart Grid Cyber Security vol. 1-3*. 2010.

[28] Rajkumar, R.R., I. Lee, L. Sha, and J. Stankovic. *Cyber-physical systems: the next computing revolution*. in *Proceedings of the 47th Design Automation Conference*. 2010. ACM.

[29] Ramirez, A.J., A.C. Jensen, and B.H. Cheng. *A taxonomy of uncertainty for dynamically adaptive systems*. in *Software Engineering for Adaptive and Self-Managing Systems (SEAMS), 2012 ICSE Workshop on*. 2012. IEEE.

[30] Schulze, C., D. Ganesan, M. Lindvall, R. Cleaveland, and D. Goldman, *Assessing model-based testing: an empirical study conducted in industry*, in *Companion Proceedings of the 36th International Conference on Software Engineering*. 2014, ACM: Hyderabad, India. p. 135-144.

[31] Sridhar, S., A. Hahn, and M. Govindarasu, *Cyber–physical system security for the electric power grid*. Proceedings of the IEEE, 2012. **100**(1): p. 210-224.

[32] Utting, M. *ModelJUnit*. 2016 [cited 2017; Available from: https://sourceforge.net/projects/modeljunit/.

[33] Utting, M. and B. Legeard, *Practical model-based testing: a tools approach*. 2010: Morgan Kaufmann.

[34] Utting, M., B. Legeard, F. Bouquet, E. Fourneret, F. Peureux, and A. Vernotte, *Chapter Two-Recent Advances in Model-Based Testing*. Advances in Computers, 2016. **101**: p. 53-120.

[35] Utting, M., A. Pretschner, and B. Legeard, *A taxonomy of model-based testing approaches*. Software Testing, Verification and Reliability, 2012. **22**(5): p. 297-312.

[36] Walker, W.E., P. Harremoës, J. Rotmans, J.P. van der Sluijs, M.B. van Asselt, P. Janssen, and M.P. Krayer von Krauss, *Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support*. Integrated assessment, 2003. **4**(1): p. 5-17.

[37] Yampolskiy, M., P. Horvath, X.D. Koutsoukos, Y. Xue, and J. Sztipanovits. *Taxonomy for description of cross-domain attacks on CPS*. 2013. ACM.

[38] Zhang, M., S. Ali, T. Yue, and R. Norgren, *Uncertainty-Wise Evolution of Test Ready Models*. Information and Software Technology, 2017.

[39] Zhang, M.a.S., Bran and Ali, Shaukat and Yue, Tao and Okariz, Oscar and Norgren, Roland, *Understanding uncertainty in cyber-physical systems: A conceptual model*, in *European Conference on Modelling Foundations and Applications*. 2016, Springer.

[40] Zheng, X., C. Julien, M. Kim, and S. Khurshid, *On the state of the art in verification and validation in cyber physical systems.* The University of Texas at Austin, The Center for Advanced Research in Software Engineering, Tech. Rep. TR-ARiSE-2014-001, 2014.