STRIDE-based Threat Modeling for Cyber-Physical Systems

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2018). STRIDE-based Threat Modeling for Cyber-Physical Systems. In *2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings* Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/ISGTEurope.2017.8260283

Published in:
2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

STRIDE-based Threat Modeling for Cyber-Physical Systems

Rafiullah Khan, Kieran McLaughlin, David Laverty and Sakir Sezer
Queen's University Belfast, Belfast, United Kingdom
Email: {rafiullah.khan, kieran.mclaughlin, david.laverty, s.sezer}@qub.ac.uk

***Abstract*—Critical infrastructures and industrial control systems are complex Cyber-Physical Systems (CPS). To ensure reliable operations of such systems, comprehensive threat modeling during system design and validation is of paramount significance. Previous works in literature mostly focus on safety, risks and hazards in CPS but lack effective threat modeling necessary to eliminate cyber vulnerabilities. Further, impact of cyber attacks on physical processes is not fully understood. This paper presents a comprehensive threat modeling framework for CPS using STRIDE, a systematic approach for ensuring system security at the component level. This paper first devises a feasible and effective methodology for applying STRIDE and then demonstrates it against a real synchrophasor-based synchronous islanding testbed in the laboratory. It investigates (i) what threat types could emerge in each system component based on the security properties lacking, and (ii) how a vulnerability in a system component risks the entire system security. The paper identifies that STRIDE is a light-weight and effective threat modeling methodology for CPS that simplifies the task for security analysts to identify vulnerabilities and plan appropriate component level security measures at the system design stage.**

***Index Terms*—Cyber physical systems, smart grid, synchrophasors, STRIDE, threat modeling, cyber security.**

I. Introduction

Cyber-Physical Systems (CPS) use Information and Communication Technologies (ICT) to control and monitor the physical processes. Critical infrastructures such as smart grids, industrial control systems, transportation networks, water distribution networks, etc are CPS where cyber vulnerabilities are considered very critical. The CPS are prone to cyber-attacks on their data management and network layer as occurred in the cyber attacks on Ukraine power distribution companies [1], German steel mill [2], Maroochy water breach [3] and various other industrial security incidents based on BlackEnergy and Stuxnet [4], [5]. Thus, proper threat modeling for CPS in the system design process and incorporating necessary countermeasures are of paramount significance.

Threat modeling is the identification of system vulnerabilities and their potential impact on the physical processes. The significance of threat modeling for CPS can be realized by applying against a particular system. This paper performs threat modeling against a synchrophasor application. Synchrophasor technology is used for real-time monitoring, protection and control in power systems [6]. It enables operators to track power system dynamics in real-time and promptly take actions whenever necessary. Due to the nature of synchrophasor applications, cyber attacks could result in severe consequences [4].

A. Related Work

Most synchrophasor applications are still at a laboratory validation stage [6], [7]. Proper threat modeling at the early stage is essential to establish appropriate security measures for synchrophasor applications before they are deployed in practice. IEEE C37.118 is the most commonly used synchrophasor communication framework by Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs). However, it is highly vulnerable to cyber attacks due to no built-in security mechanism [8], [9], [10], [11]. Authors in [4] investigated how vulnerabilities in synchrophasor-based systems can be exploited in the form of cyber attacks. Particularly, the authors have demonstrated attack scenarios for reconnaissance, eavesdropping, Man-In-The-Middle (MITM), replay/reflection and denial of service attacks. Most researchers focused on a specific attack type such as packet drop attacks [12], DoS attacks [13], data integrity attacks [14], GPS spoofing attacks [15], etc.

Various system safety and security modeling methodologies exist in literature e.g., STPA-sec (focuses on system safety) [16], HAZOP (focuses on hazard and system operability) [17], SAHARA (focuses on hazard, risk and security) [18], PASTA (focuses on process for attack simulation), OCTAVE (focuses on operationally critical threats and assets) [19], STRIDE (focuses on identification of potential threats in each subcomponent of the system) [20]. Although researchers have previously analyzed threats for CPS in general, few have focused on power systems. Authors in [21] presented STPA-SafeSec, an approach for security analysis that was tested against synchrophasor-based systems. However, their main focus is safety, risks and hazards analysis.

B. Motivation and Contributions

STPA-sec, HAZOP, OCTAVE and PASTA are complex modeling methodologies with more focus on system safety and risks. This paper performs threat modeling using STRIDE which is comparatively a lightweight approach. The choice of STRIDE is motivated due to several reasons: (i) it is a systematic approach and analyzes cyber threats against each system component based on its technical knowledge, (ii) it is comprehensive and analyzes security properties such as

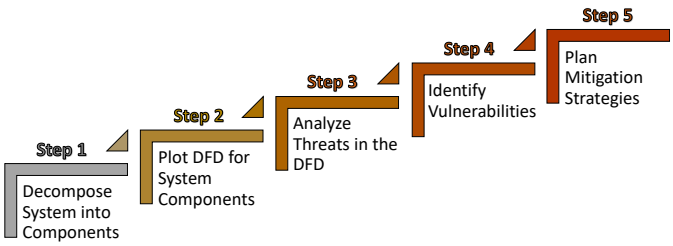

Figure 1. STRIDE-based threat modeling methodology.

Table I
SUSCEPTIBILITY OF DFD ELEMENTS TO STRIDE THREATS.

DFD Element	S	T	R	I	D	E
Entity	✓		✓			
Data Flow		✓		✓	✓	
Data Store		✓	✓	✓	✓	
Process	✓	✓	✓	✓	✓	✓

authentication, authorization, confidentiality, integrity, non-repudiation and availability against each system component, and (iii) it provides a clear understanding of the impact of a component vulnerability on the entire system and helps ensure system security as the component level.

The literature still lacks an example framework showing the application of the STRIDE approach to a CPS. Hence, the objective of this paper is to provide a walk-through demonstrating that the light-weight STRIDE approach can be applied to a CPS to produce an effective categorization of system-specific threats. Specifically, it performs STRIDE-based threat modeling against a real synchrophasor-based laboratory testbed with the objective to establish appropriate security measures to secure the environment. Most synchrophasor applications are still in laboratory testing and validation; making STRIDE the most effective cyber threats modeling approach.

II. STRIDE METHODOLOGY

The STRIDE method is proposed by Microsoft and represents a mnemonic for six different types of security threats [20]: (i) **S**poofing: Masquerading of a legitimate user, process or system element, (ii) **T**ampering: Modification/editing of legitimate information, (iii) **R**epudiation: Denying or disowning a certain action executed in the system, (iv) **I**nformation disclosure: Data breach or unauthorized access to confidential information, (v) **D**enial of Service (DoS): Disruption of service for legitimate users, and (vi) **E**levation of privilege: Getting higher privilege access to a system element by a user with restricted authority.

STRIDE analyzes vulnerabilities against each system component which could be exploited by an attacker to compromise the whole system. Due to the lack of a standard methodology, this paper proposes five high-level steps (as shown in Fig. 1) for applying STRIDE threat modeling against a system. The first step is to decompose the system into its logical or structural components. Components can be internal processes/elements communicating internally within the system or external elements communicating with the system. The next step is to plot a Data Flow Diagram (DFD) for each system component that visualizes its functionalities within or external to the system. The DFD uses four standard symbols: (i) External Entity (EE) i.e., end-points of the system, (ii) Process (P) i.e., units of functionality, (iii) Data Flow (DF) i.e., communication data and (iv) Data Store (DS) i.e., database, logs or file. The DFD may also contain trust boundaries which isolate trustworthy and untrustworthy elements. Each DFD element type is susceptible to only a few or all STRIDE threats as shown in Table I [20]. The next step is to identify STRIDE threats in the DFD of each system component. Based on each system component and its functionality, certain STRIDE threats might not be applicable to it. Once threats have been identified for each system component, the vulnerabilities causing them need to be investigated. The final step is to plan effective mitigation strategies based on the discovered vulnerabilities.

STRIDE-based threat modeling can be performed in two possible ways [22]: (i) STRIDE-per-element and (ii) STRIDE-per-interaction. STRIDE-per-element is more complex as it analyzes behavior and operations of each system component. However, it may not be sufficient to identify certain threats that are not evident from the DFD. In certain scenarios, threats show up in the interactions between system components. STRIDE-per-interaction therefore enumerates threats against system interactions by considering tuples (origin, destination, interaction). Comparatively, STRIDE-per-interaction is easier to perform and its protection strategies are normally enough to protect system (as cyber attacks normally involve malicious interactions between system components).

III. SYSTEM DESCRIPTION: SYNCHRONOUS ISLANDING USE CASE

STRIDE-based threat modeling will now be performed for a use case in the smart grid domain. Synchronous islanding deals with distributed generation sources (e.g., microgrids) and their safe integration into the main grid. A microgrid is a certain geographical area where generation (e.g., photovoltaics, wind farm, etc), load and storage are in close proximity. Microgrids can operate either independently (usually for a limited amount of time) or connected to the main grid. The synchronous islanded operation enables microgrids to be dynamically connected or disconnected from the main grid. For safe re-connection of a microgrid to main grid, it must be synchronized with the main grid (i.e., same voltage magnitude, frequency and phase angle). If a circuit breaker is closed in non-synchronized state, it could cause severe physical damage to equipment (microgrid and/or main grid), risk to human safety and loss of supply for the local consumers.

This paper performs threat modeling using a real laboratory based synchronous islanding testbed. A high level view of the testbed is shown in Fig. 2. The generator set consists of an alternator which is driven by prime mover (a DC machine in this case). The prime mover controller increases/decreases the

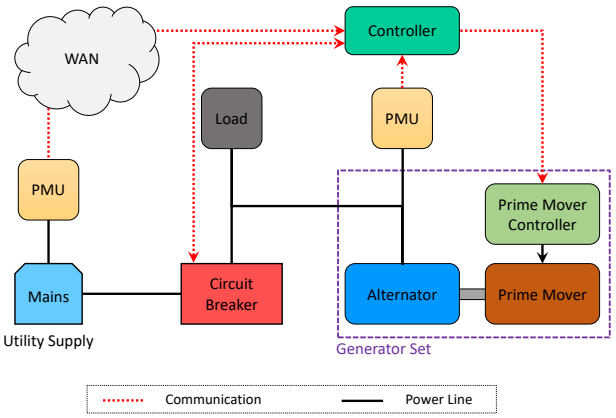

Figure 2. Synchronous islanding use case.

torque on the drive shaft to the alternator, consequently the electrical power output increases/decreases. PMUs measure electrical quantities in real-time from both main grid (i.e., utility supply) and microgrid/generator set, and communicate synchrophasor data to the controller. The controller adjusts the phase angle of the microgrid to synchronize it with the main grid. Once synchronized, the circuit breaker can be closed safely to connect the microgrid to the main grid. A detailed description of use case/testbed is available in our previous work in [7]. The rest of the section performs STRIDE-based threat modeling for the use case. Note, due to the space available, the scope of this paper is limited to only the first four steps as in Fig. 1.

A. Decompose System into Components

Step 1 (see Fig. 1) is to decompose system into its components. Based on Fig. 2, the system consists of five components: PMU for main grid, PMU for microgrid, generator set, controller and circuit breaker. Note, threat analysis does not consider physical components which are not susceptible to cyber attacks e.g., load, electrical wire connections between circuit breaker and alternator or utility supply.

B. Plot DFD for System Components

As in Fig. 1, step 2 in threat modeling is to plot a DFD for each system component. Due to paper length restriction, a single DFD is plotted for the complete system (as in Fig. 3) instead of plotting a separate DFD for each system component. Note, the PMUs in Fig. 2 are OpenPMUs [23] which consist of four functional blocks: time source receiver, data acquisition, signal processing and telecom. The time source receiver and data acquisition functionalities are provided on a BeagleBone board whereas, signal processing and telecom functionalities are provided on Raspberry Pi. Data acquisition component communicates with signal processing component using the UDP protocol. The telecom block restructures synchrophasor data into IEEE C37.118 protocol format and sends to the controller. Since PMUs time-stamp real-time measurements using a common precise time-source, the time source element is also depicted in the DFD (GPS in this case). The controller in Fig. 3 consists of two processes: PID controller (which processes received synchrophasor measurements from main grid and microgrid) and digital-to-analog converter (that provides feedback to generator set to adjust the output of the alternator).

Table II
POSSIBLE THREAT CONSEQUENCES (TC) BASED ON THE EXPERT KNOWLEDGE OF SYNCHRONOUS ISLANDING TESTBED.

Code	Description	Hazard
TC-1	Circuit breaker closure in non-synchronized state.	H-1 - H-3
TC-2	Power equipment operation outside safe limits.	H-1 - H-3
TC-3	Violation of power quality.	H-2
TC-4	Inability to achieve synchronization.	-
TC-5	Inability to meet micro-grid local power demand.	H-3
TC-6	Disclosure of system state or secrets.	-
TC-7	Inability to control or configure micro-grid.	H-3
TC-8	Inability to communicate with circuit breaker.	-
TC-9	Inability to communicate with controller.	-
TC-10	Disclosure of communication secrets (e.g., encryption keys, algorithms, IEEE C37.118 CFG-2, etc).	-

Hazard codes: H-1 = Human injury, H-2 = Equipment damage and H-3 = Black-out.

C. Analyze Threats in the DFD

To perform threat analysis (step 3 in Fig. 1), it is necessary to first identify possible attacker intentions (or threat consequences) based on the expert knowledge of the system. For use case in Fig. 2, Table II identifies possible threat consequences and assigns a code to each for referencing purpose. Fig. 4 graphically represents STRIDE-per-element approach for threat analysis. Its results are summarized in Table III and briefly explained in the following.

1) Spoofing: Precise timing information in the use case is critical for the controller to synchronize the microgrid to the main grid. If the time source (EE-1 or EE-2 in Fig. 3) is spoofed by an attacker, the phase angle estimation (by P-3 or P-7) will be incorrect. This could result in destructive failure if controller detects synchronization and closes the circuit breaker (TC-1). Due to incorrect timing information, the controller may fail to achieve synchronization (TC-4). If disconnected microgrid cannot meet its local power demand, it could also result in blackout (TC-5). The attackers might spoof P-1 or P-5 to prevent system from acquiring timing information. This could result in TC-4 and TC-5. Spoofing of phasor estimation process (P-3 or P-7) and telecom process (P-4 or P-8) are critical as they can trick controller to assume synchronization and close the circuit-breaker (TC-1). Spoofing of processes P-9 to P-12 could enable attacker to cause severe damage to equipment or fail the entire synchronous islanding mechanism. E.g., safe limit for prime mover is analog signal between 0V and 5V which could be violated by spoofing of P-10.

2) Tampering: Tampering in the use case is very risky as they could easily trick controller performing unsafe actions. In Fig. 3, tampering attacks could easily take place on DF elements due to unencrypted communication. Particularly, tampering on DF-3 and DF-6 could trick controller to close circuit breaker in non-synchronized state (TC-1). DF-2 and DF-5 are safe from tampering as they are not exposed to the network and connected using secondary NICs on Raspberry

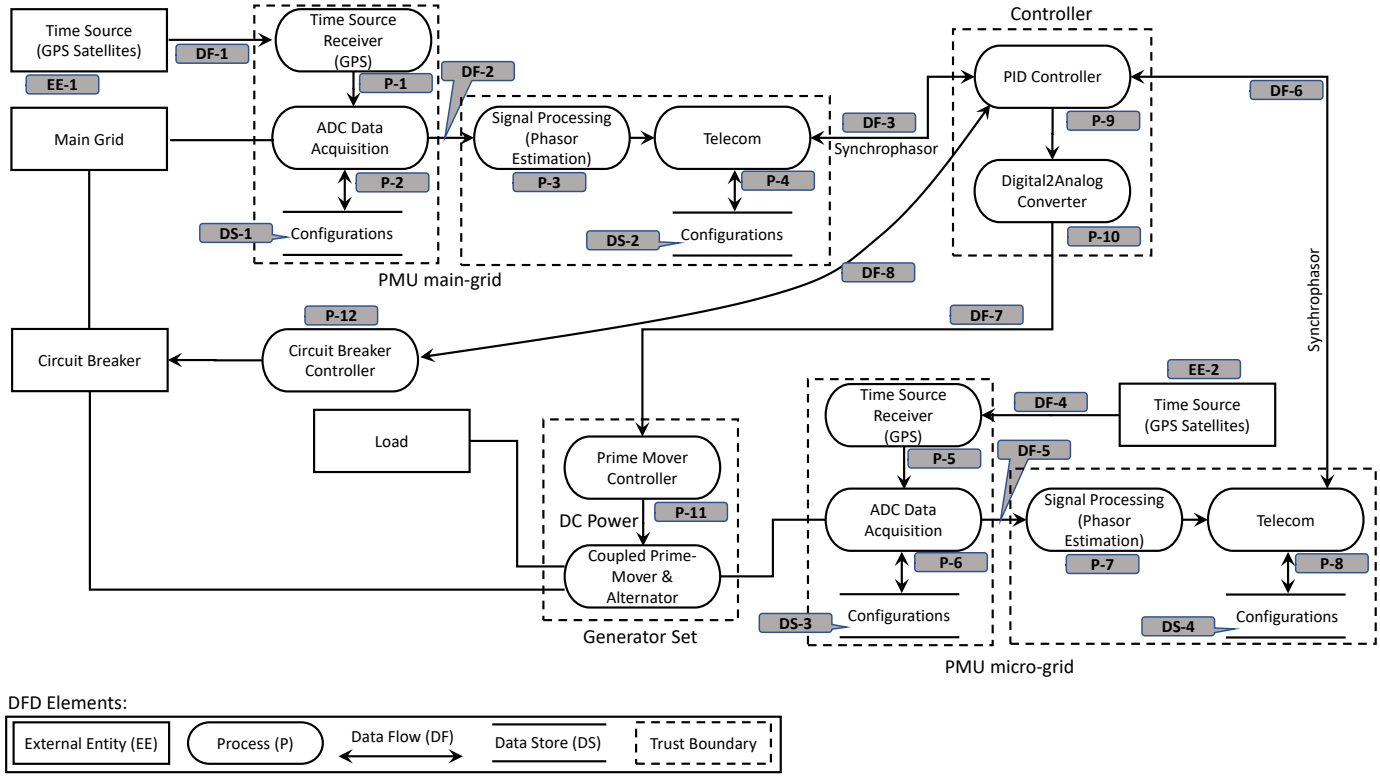

Figure 3. Data flow diagram for synchronous islanding testbed. Grey tags are used for referencing purpose and are not part of the DFD. Solid lines with no arrow sign on both sides are electrical wired connections which are safe from cyber attacks.

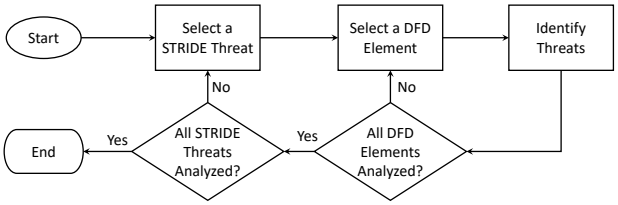

Figure 4. Threat analysis using STRIDE-per-element approach.

Pi and BeagleBone. Tampering on DF-7 could provide unsafe input to prime mover (TC-2) and damage the generator set. Tampering on DF-8 could also result in TC-1. Tampering on DS-2 and DS-4 (which contain necessary configuration information related to IEEE C37.118 communication framework) could prevent PMUs from communicating with controller or send incorrectly formated packets to controller (TC-9). Not only DF and DS elements, tampering could also take place on processes (P) if they are compromised by an attacker and are equally risky as DF elements.

3) Repudiation: Non-repudiation cannot be guaranteed for each DFD element in Fig. 3 due to very high synchrophasor data transmission rate (i.e., 100 packets/second). This will require huge amount of storage at each DFD element for logging activities or recording events. Instead, non-repudiation should be ensured for command and system critical messages (which might be injected by attackers). E.g., P-4 and P-8 are susceptible to repudiation attacks because there is no logging of IEEE C37.118 command and configuration messages. Further, P-9, P-10 and P-12 are also susceptible to repudiation attacks.

4) Information disclosure: Information disclosure attacks in the use case are not risky themselves but could reveal system critical information to attackers which could be used in more complex attacks. DF-1 to DF-6 in Fig. 3 may not be the target elements for attacker as information disclosure here will be of no much use. E.g., GPS timing is globally available and attacker does not need to execute information disclosure attack for it. The most obvious targets for attacker will be DF-7 and DF-8 which will provide attacker the information on generator set and status of circuit breaker, respectively. Information disclosure attacks of DS-2 and DS-4 could reveal attacker the configurations of IEEE C37.118 communication framework. Processes are especially susceptible to information disclosure attacks e.g., P-4 and P-8 (how synchrophasor data is encoded in IEEE C37.118 packets), P-9 (when microgrid is synchronized or non-synchronized with main grid), P-10 (what adjustment is made to generator set), etc.

5) Denial Of Service: DoS attacks could interrupt power supply for microgrid consumers. If the microgrid is in disconnected state and cannot meet local demand, a DoS attack could prevent it from synchronizing and connecting to the main grid. Thus, blackout could result for microgrid local consumers. Most DFD elements in Fig. 3 are susceptible to DoS attack;

Table III
THREAT MODELING USING STRIDE-PER-ELEMENT METHODOLOGY.

STRIDE	DFD Elements	TC
S	P-1, P-5	TC-4, TC-5
	P-3, P-4	TC-1, TC-4, TC-5, TC-9
	P-7, P-8	TC-1, TC-4, TC-5, TC-7, TC-9
	P-9	TC-1, TC-4, TC-5, TC-7, TC-8
	P-10	TC-2
	P-11	TC-2 - TC-5, TC-7
	P-12	TC-1, TC-8
	EE-1, EE-2	TC-1, TC-4, TC-5
T	DF-1, DF-3	TC-1, TC-4, TC-5
	DF-4, DF-6	TC-1, TC-3 - TC-5
	DF-7	TC-2
	DF-8	TC-1
	DS-1, DS-3	TC-4, TC-5
	DS-2, DS-4	TC-9
	P-1 - P-8	TC-1, TC-4, TC-5
	P-9	TC-1, TC-4, TC-7
	P-10	TC-2
	P-11	TC-2 - TC-5, TC-7
	P-12	TC-1, TC-8
R	P-4, P-8	TC-6, TC-9
	P-9, P-12	TC-1
	P-10	TC-2
I	DF-7 - DF-8	TC-6
	DS-1 - DS-4	TC-6
	P-3, P-7, P-9, P-10	TC-6
	P-4, P-8	TC-10
D	DF-1, DF-3, DF-4, DF-6	TC-4 - TC-5
	DF-7	TC-7
	DF-8	TC-8
	DS-1, DS-3	TC-4, TC-5
	DS-2, DS-4	TC-9
	P-1 - P-8	TC-4, TC-5
	P-9	TC-7, TC-8
	P-10	TC-7
	P-12	TC-8
E	P-3, P-7	TC-1, TC-4 - TC-6
	P-4, P-8	TC-1, TC-4, TC-5, TC-10
	P-9	TC-1, TC-4, TC-5, TC-7
	P-10	TC-2
	P-11	TC-2 - TC-5, TC-7
	P-12	TC-1

however, the most likely and easy targets could be DF-3, DF-6 to DF-8, P-9 and P-12. To execute DoS attack against a process, attacker would normally flood the process with superfluous traffic to consume its processing resources and prevent it from processing legitimate requests. If an attacker has compromised the physical device, he may stop the process. Comparatively, DoS attacks could be easily executed against DF elements by simply dropping the packets.

6) Elevation of privilege: Elevation of privilege means a high privilege activity performed by a less privileged user. In the use case, no authorization or privilege levels are defined for processes. Thus, a process will perform the task requested by a legitimate user/element or the attacker. E.g., P-4 and P-8 cannot verify if IEEE C37.118 command messages received from a legitimate user and may provide configurations to an attacker. Due to no authorization, P-9 processes received synchrophasor data from any device. P-12 cannot verify authenticity of received commands and may close circuit breaker in non-synchronized state (TC-1).

Table IV presents threat analysis using STRIDE-per-interaction methodology that takes into account all interactions taking place in the testbed. It can be observed in Table IV that two elements (e.g., P-4 and P-9) could have different types of interactions where each interaction type could be susceptible to different STRIDE threats. E.g., IEEE C37.118 command messages are susceptible to all STRIDE threats whereas data messages could be susceptible to tampering, information disclosure and DoS attacks.

Table IV
THREAT MODELING USING STRIDE-PER-INTERACTION METHODOLOGY.

Interaction	S	T	R	I	D	E
P-9 to P-4: IEEE C37.118 command message	x	x	x	x	x	x
P-9 to P-8: IEEE C37.118 command message	x	x	x	x	x	x
P-4 to P-9: IEEE C37.118 CFG-2, header or data messages.		x		x	x	
P-8 to P-9: IEEE C37.118 CFG-2, header or data messages.		x		x	x	
P-9 to P-12: Close or open circuit breaker.	x	x	x	x	x	x
P-10 to P-11: Control input to generator set within or beyond safe limits.	x	x	x	x	x	x
EE-1 to P-1: Timing signal.	x	x			x	
EE-2 to P-5: Timing signal.	x	x			x	
P-2 to P-3: Sampled data.	x	x		x	x	
P-6 to P-7: Sampled data.	x	x		x	x	
DS-1 to P-2: Configurations related to data acquisition process.		x		x	x	
DS-2 to P-4: Configurations related to communication protocols.		x		x	x	
DS-3 to P-6: Configurations related to data acquisition process.		x		x	x	
DS-4 to P-8: Configurations related to communication protocols.		x		x	x	

D. Identify Vulnerabilities

Identification of vulnerabilities (step 4 in Fig. 1) is essential for planning effective security measures. Spoofing of processes (P-1 - P-12) could take place due to lack of authentication between communicating processes. E.g., P-10 sends simple UDP packets to P-11. Due to lack of authentication, P-11 cannot verify if it has received packets from legitimate P-10. Similarly, communication between P-4 and P-9 is based on IEEE C37.118 protocol which also lacks authentication. Further, processing of IEEE C37.118 commands by P-4 and P-8 is not based on sender; they can process commands received from any device (not only P-9). Depending on time source, EE-1 and EE-2 can also be spoofed due to lack of authentication.

Tampering on all DF elements (except DF-3 and DF-6) is due to lack of integrity verification mechanism. Even though, DF-3 and DF-6 have checksum to verify integrity, they are still susceptible to tampering threats. It is due to the fact that IEEE C37.118 checksum is non-cryptographic and is based on predefined algorithm. Thus, attackers can easily modify packets, calculate new checksum and include in the packets which will go undetected by P-9. Also processes (P-1 - P-12) are susceptible to tampering due to lack access control mechanism.

There is no event logging and recording mechanism in the use case. Thus, the processes are susceptible to repudiation threats and cannot deny or track past events. The information disclosure threats to DF elements is due to lack of encryption. Unencrypted messages can be easily decoded and interpreted by attackers. Further, P and DS elements are susceptible to information disclosure threats due to lack of appropriate access control mechanism. The use case lacks redundancy of elements as well as authentication and authorization between elements, they are susceptible to DoS threats. If processes have authentication and process packets received only from authenticated senders, they could significantly save their processing resources. Also elevation of privilege threats are linked with authorization. The testbed processes are susceptible to elevation of privilege threats due to lack of access control based on authorization.

IV. DISCUSSION

There is no standard methodology defined in literature for applying STRIDE. Thus, this paper proposed five steps (see Fig. 1) which were identified as a basis to effectively

perform STRIDE-based threat modeling. It was observed that certain STRIDE threats impact a group of DFD elements. Spoofing and tampering are especially critical and they impact the operations of other elements (particularly in the physical domain) resulting in more severe consequences for the system. Further, STRIDE helped to identify that the attacker can achieve a specific malicious objective in various ways. E.g., attacker can achieve TC-1 through spoofing of P-4, P-8, EE-1, EE-2 etc or through tampering on DF-3, DF-6, etc (see Table III). This helps analysts to developed more appropriate security solutions.

STRIDE-per-element analysis in Section III-C highlighted the significance of securing the system at the component level. It was observed that entire system security can only be ensured if all of its components are secure. However, it was identified that STRIDE-per-element approach may not be sufficient to identify certain threats due to inadequate technical knowledge of system components or if threats appear only in interactions (e.g., P-4 and P-9 in Table IV). Thus, STRIDE-per-interaction should also be considered to complement threat analysis and plan more effective security measures.

It was revealed in Section III-D that each STRIDE threat in the use case is due to lack of certain security properties. For analysts to plan mitigation strategies, the six essential security properties (authorization, authentication, confidentiality, integrity, availability and non-repudiation) should be ensured for each system component.

V. Conclusions

Security of cyber physical systems is of paramount significance as they are ubiquitous in critical infrastructures. Previous works in literature mostly focused on safety, risk and hazard aspects in cyber physical systems [16], [17], [18], [21]. Few researchers have analyzed threats for cyber physical systems [24] but lack a comprehensive mechanism for ensuring system security at the component level.

This paper presented a comprehensive STRIDE-based threat modeling for cyber physical systems. The primary contribution of the paper is to formalize a systematic methodology that can be used for effective characterization of system-specific threat using the STRIDE approach. This is demonstrated by performing threat modeling against a real laboratory based synchronous islanding testbed. The paper presented necessary mapping of STRIDE threats to the system components using the DFD. Due to inter-dependencies between system components, the entire system security can only be ensured by addressing vulnerabilities of each system component. Thus, this paper identified STRIDE as an effective approach towards ensuring system security at the component level.

The paper demonstrated that an attacker can achieve a specific malicious objective by exploiting threats at different locations in the system. By identifying component level vulnerabilities and their potential physical consequences, STRIDE can also effectively cope with such challenges. The results of STRIDE approach are more meaningful, easily understandable and comprehensive enough for system designers in order to develop appropriate security solutions. The output of STRIDE can feed into risk analysis processes to establish the most critical threats and furthermore the development of the most appropriate mitigation measures that should be applied.

Acknowledgment

This work was funded by the EPSRC CAPRICA project (EP/M002837/1).

References

[1] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case," in *Technical Report, SANS ICS*, March 2016.

[2] R. M. Lee, M. J. Assante, and T. Conway, "ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper - German Steel Mill Cyber Attack," in *Technical Report, SANS ICS*, 2014.

[3] J. Slay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in *Critical Infrastructure Protection*, 2008.

[4] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid," in *ICS-CSR conference*, 2016.

[5] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," in *Survival, vol. 53, no. 1, pp. 2340*, 2011.

[6] I. M. Dragomir and S. S. Iliescu, "Synchrophasors Applications in Power System Monitoring, Protection and Control," in *CSCS conference*, 2015.

[7] I. Friedberg, D. Laverty, K. McLaughlin, and P. Smith, "A cyber-physical security analysis of synchronous-islanded microgrid operation," in *ICS-CSR conference*, 2015.

[8] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "IEEE C37.118-2 Synchrophasor Communication Framework - Overview, Cyber Vulnerabilities Analysis and Performance Evaluation," in *2nd International Conference on Information Systems Security and Privacy*, 2016.

[9] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Transactions on Smart Grid*, 2016.

[10] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 Synchrophasor Communication Frameworks," in *IEEE Power and Energy Society - General Meeting (IEEE PES-GM 2016)*, July 2016.

[11] L. Coppolino, S. DAntonio, and L. Romano, "Exposing Vulnerabilities in Electric Power Grids: An Experimental Approach," in *International Journal of Critical Infrastructure Protection vol:7(1), pp:51-60*, 2014.

[12] S. Pal, B. Sikdar, and J. Chow, "Real-time detection of packet drop attacks on synchrophasor data," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, 2014.

[13] T. Morris *et al.*, "Cybersecurity Testing of Substation Phasor Measurement Units and Phasor Data Concentrators," in *ACM CSIIRW*, 2011.

[14] S. Paudel, P. Smith, and T. Zseby, "Data Integrity Attacks in Smart Grid Wide Area Monitoring," in *ICS-CSR conference*, 2016.

[15] D. Shepard, T. Humphreys, and A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks," in *International Journal of Critical Infrastructure Protection*, 2012.

[16] W. Young and N. G. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," in *Commun. ACM*, 2014.

[17] T. A. Kletz, "HAZOP and HAZAN: identifying and assessing process industry hazards," in *IChemE*, 1999.

[18] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: A security-aware hazard and risk analysis method," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, 2015.

[19] M. Abomhara, M. Gerdes, and G. M. Koien, "A STRIDE-Based Threat Model for Telehealth Systems," in *NISK*, 2015.

[20] M. Howard and S. Lipner, *The Security Development Lifecycle*. Redmond, WA, USA: Microsoft Press, 2006.

[21] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems," in *Journal of Information Security and Applications*, 2016.

[22] A. Shostack, "Threat Modeling - Designing for Security," in *Wiley*, 2014.

[23] D. M. Laverty *et al.*, "The OpenPMU Project: Challenges and Perspectives," in *IEEE PES-GM*, 2013.

[24] E. B. Fernandez, "Threat Modeling in Cyber-Physical Systems," in *Dependable, Autonomic and Secure Computing conference*, 2016.