Check for updates

Received: 22 April 2020 | Revised: 15 December 2020 | Accepted: 16 January 2021 | Published on: 20 February 2021

DOI: 10.1002/spy2.150

SURVEY PAPER

WILEY

Systematic review of features for co-simulating security incidents in Cyber-Physical Systems

Ricardo M. Czekster[1] | **Charles Morisset**[1] | **John A. Clark**[2] | **Sadegh Soudjani**[1] | **Charalampos Patsios**[3] | **Peter Davison**[3]

[1]School of Computing, Newcastle University, Newcastle upon Tyne, UK

[2]Department of Computer Science, The University of Sheffield, Sheffield, UK

[3]School of Engineering, Newcastle University, Newcastle upon Tyne, UK

Correspondence
Ricardo M. Czekster, School of Computing, Newcastle University, Newcastle upon Tyne, UK.
Email: ricardo.melo-czekster@ncl.ac.uk

Funding information
Engineering and Physical Sciences Research Council, Grant/Award Number: EP/V012053/1

Abstract

Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) plus energy are the enabling technology of modern power systems also known as the Smart Grid (SG). A SG may consist of thousands of interconnected components communicating and exchanging data across layers that stretch beyond technical capabilities, for instance, markets and customer interactions. Cyber-physical security is a major source of concern due to the high reliance of the SG on Information and Communication Technologies (ICT) and their widespread use. Addressing security requires developing modeling and simulation tools that approximate and replicate adversarial behavior in the SG. These tools have in fact two simulators, one handling continuous power flows and another for capturing the discrete behavior when communicating across CPS or IoT components. The technique of composing two models of computation in a global simulation of these coupled systems is called co-simulation. Although there are many frameworks and tools for co-simulation, the set of features for modeling cyber-physical security incidents in the SG lacks thorough understanding. We present a systematic review of features and tools for co-simulating these concerns in CPS. We also highlight and discuss research gaps with respect to the most used tools in industry and academia and comment on their relevant features.

KEYWORDS

co-simulation, Cyber-Physical Systems, energy, power grid, security, Systematic Literature Review, telecommunication networks

Abbreviations: AMI, Advanced Metering Infrastructure; BDD, Bad Data Detection; CIA, Confidentiality, Integrity, Availability; CPS, Cyber-Physical Systems; DDoS, Distributed Denial-of-Service; DoS, Denial-of-Service; DER, Distributed Energy Resources; DG, Distributed Generation; DLS, Digital Line Subscriber; DNS, Domain Name System; DR, Demand Response; DSM, Demand Side Management; DSO, Distribution System Operator; EMS, Energy Management Systems; ESCO, Energy Service Companies; ESS, Energy Storage Systems; EV, Electric Vehicles; FDI, False Data Injection; GT&D, Generation, Transmission and Distribution; HVAC, Heating, Ventilation and Air Conditioning; ICS, Industrial Control Systems; ICT, Information and Communication Technologies; IoT, Internet of Things; ITD, Integrated Transmission & Distribution; MiTM, Man-in-The-Middle; MTU, Master Terminal Unit; NIDS, Network Intrusion Detection System; PLC, Programmable Logic Controller; PMU, Phasor Measurement Unit; PSLF, Positive Sequence Load Flow; RTU, Remote Terminal Unit; SCADA, Supervisory Control And Data Acquisition; SG, Smart Grid; SLR, Systematic Literature Review; TES, Transactive Energy Systems; VAP, Vulnerability Assessment Process.

[Correction added on 1 March 2021, after first online publication: the word "exist" has been removed in the last sentence of the first paragraph of section 2.2 and reference citation was corrected from "70" to "55" in the 10th paragraph of section 3.1.]

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2021 The Authors. *Security and Privacy* published by John Wiley & Sons Ltd.

1 | INTRODUCTION

Cyber-Physical Systems (CPS) are the combined use of physical and digital counterparts to enhance decision making capabilities. It is an innovative concept applied to modern infrastructures for incorporating intelligent data gathering mechanisms, sensing, and feedback loops to support decisions. CPS are likely to be of interest to companies such as those offering services in water, energy, and transportation sectors. In the long term, CPS will assist the seamless integration of data and systems into its underlying infrastructure.

An example of CPS in the energy domain is one which focuses on efficient energy use where customers are brought into the decision making process. In this context, a Smart Grid (SG) is an example of CPS. A SG encompasses a large range of equipment, physical components and systems operating and exchanging data. At its core, pervasive Information and Communication Technologies (ICT) ensure reliable and secure pathways for end-to-end communication. Notable components of the SG are Internet of Things (IoT) devices, Building Management Systems (BMS), Heating, Ventilation, and Air Conditioning (HVAC), and Electric Vehicles (EV), to mention a few.

CPS combine physical and digital components across multiple scales whereas IoT operates on the transmission layer. Examples are power and telecommunication networks connecting smart buildings and telecommunication devices attached to the physical infrastructure. When deployed in smart contexts they are responsible for sensing the environment and monitoring its surroundings, among other features. The CPS infrastructure performs the remote management of its underlying components for energy efficiency, comfort, and reasonable use of resources.

Unfortunately, among the many challenges discouraging broad adoption of CPS across society is the lack of security, privacy, and trust. Security of the SG, when poorly addressed, cascades into more instability across systems, often leading to outages or blackouts. Critical infrastructures such as the SG expose a large attack surface for malicious interventions caused by adversaries, with potential to inflict severe financial and safety damages. Reasons of attacks are for example simplified access to ICT, poorly maintained systems, malware, or lax security measures, to mention a few. High profile security related events include the Stuxnet worm in the Iranian nuclear program facilities[1] and the attack on the Ukrainian power grid.[2]

A technique to investigate cyber-physical security in critical infrastructures such as the SG is simulation. It is often used to test designs and artificially create analysis scenarios to ease quantitative assessments. Analysts simulate the power grid, the transmission network, or the telecommunication network using different simulation engines. So, it is crucial for these simulators to accurately synchronize among each other. The approach responsible for merging two or more simulation engines into one global simulation representing the dynamics of these coupled systems is called co-simulation.[3] Present work investigates co-simulation engines with focus on security aspects, exploring situations as diverse as power theft, telecommunication delays, impact of attacks on components, and the interaction between these two core elements in SG research.

1.1 | Motivation

There is a myriad of co-simulation frameworks and tools for addressing major CPS concerns and shortcomings. However, these software suites are designed to function as general-purpose solutions. They provide a wide range of modeling possibilities but fall short on focus, making it hard to leverage other concerns altogether. For instance, to model aspects such as security, they must modify pre-existing tools and customize the models to meet their objectives, which significantly impair timely assessments.

There is a need to understand the modeling features of tools addressing key SG components and their underlying systems. It is equally crucial to model and simulate security incidents in power settings to test designs and compute the impact of cyber-physical attacks on the infrastructure. We have thoroughly assessed previous work and scientific literature and we discovered no systematic reviews pointing out modeling features focusing on security aspects when co-simulating the SG. Our work here also aims to show modelers the limitations and advantages of modeling and co-simulating the SG, exposing most used tools and features to address cyber-physical security concerns.

1.2 | Contribution

Our contribution is to conduct and present a Systematic Literature Review (SLR)[4] describing the main features of co-simulation frameworks for cyber-physical security of CPS, notably the SG. The focus here is toward power and

telecommunication issues such as harmful drops in power voltage, network latency, and problems arising in data communication shortcomings caused by malicious adversaries.

Our contribution is twofold. First, we list most used co-simulation frameworks adopted in both academia and industry, and second, we describe and discuss the key features for selected work retrieved by the SLR. We have identified the most likely targets and assets in the SG context and discussed the existing trade-offs.

1.3 | Organization

The paper is organized as follows: Section 2 discusses energy issues in the SG, simulation techniques, and related work whereas Section 3 presents the SLR's details and extracted features, discussing surveyed papers. Section 4 concludes the work with suggestions for further research.

2 | POWER GRIDS AND CO-SIMULATION

Due to sheer dependence on energy throughout society, inherent technologies have shifted from traditional centralized Generation, Transmission and Distribution (GT&D) infrastructures to decentralized smaller scale topologies strongly coupled with ICT. There is also a push toward the installation of renewable energy generation mechanisms in buildings and households, which may reduce peak demand and promote carbon neutral environments in these settings. Power disruptions have a large impact on human activity in general as they may cause serious economic or damage even for short time periods.

The SG depends on an information and communication layer responsible for reliable and secure data exchanges over a high number of components. The idea is to increase power grid efficiency through better distribution and management of energy, adjusting peak demand, and energy prices dynamically while interoperating across heterogeneous devices. However, the large scale nature of the SG makes them highly susceptible to failures caused by misuse, wrong configurations, incidents, attacks, or poor maintenance. It is worth remarking that the technological prospects and advances present in the SG effectively bring substantial benefits to customers, users, and managers.

In terms of energy generation, Distributed Energy Resources (DER) embedded in the distribution system function as scattered assets for coping with additional flexible demand or generation. A contractually increase in deployment of DER in the infrastructure will help transitioning toward low carbon operations and to offset significant decreases in centralized generation. Other SG elements encompass Distributed Generation (DG), Energy Storage Systems (ESS), and Demand Side Management (DSM). ESS are used to store energy generated by solar panels or wind turbines (to mention a few) whereas DSM employs customer-based incentives such as dynamic pricing or behavioral changes to reduce or increase power in the grid while keeping frequency within nominal boundaries.[5]

SG faces challenges affecting a wide range of stakeholders, from power operators to managers. Examples of problems are (i) intermittent behavior of renewable energy (eg, uncertainty in generation due to weather); (ii) frequency regulation and responses to variable power demands; (iii) infected software executing in CPS, IoT, or controllers that introduces vulnerabilities into other components, propagating malware (computer viruses), corrupting data, capturing wrong situational information (state estimation) or relaying spurious/inconsistent network packets; (iv) energy based controllers must cope with device heterogeneity at a large scale; and (v) uncertainties produced when dealing with dynamic energy markets and customer incentives to balance supply and demand.

Figure 1 shows an adaptation of the SG architecture proposed by the National Institute of Standards and Technology (NIST, in the US) depicting its major infrastructure, sub-systems, and participants.[6,7] Security is required across the infrastructure as disturbances and delays may cause damage or financial loss to stakeholders or wrongly switch energy prices to customers.

2.1 | Co-simulation and related work

Co-simulation is essential in power and telecommunication networks because it provides results that closely approximate the behaviors of large scale complex networks.[8] It allows the definition of multiple scenarios in the SG and attracts large interest in academia and industry.[9] It has mechanisms for artificially incorporating user or component patterns for

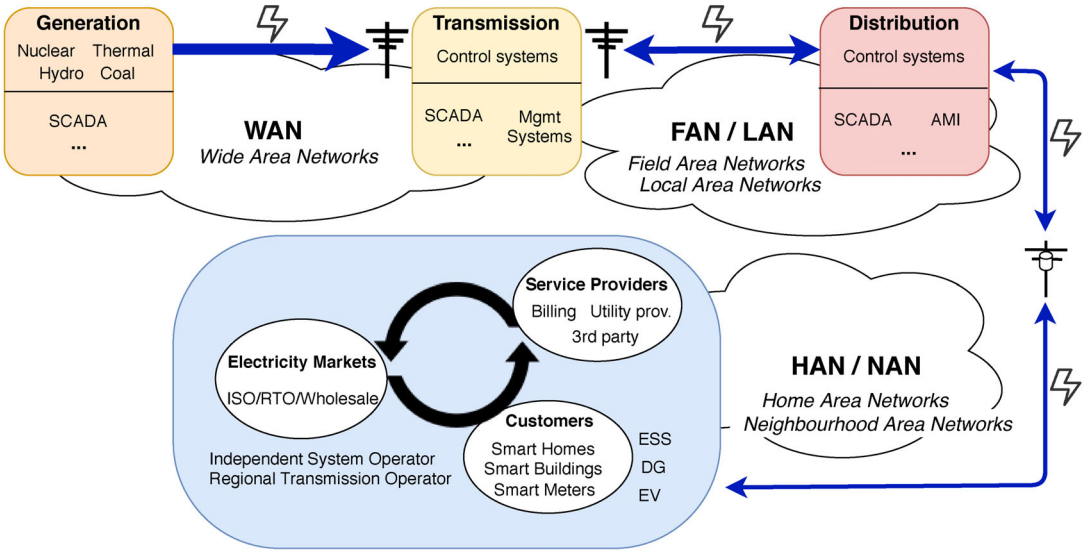


FIGURE 1 Overview of NIST's SG architecture showing power GT&D and sub-systems[6]

investigating and addressing impact on infrastructures. Depending on the tool, one could model user behaviors and appliance actions (namely scheduling), household and building properties (related to energy conservation, for example, using employing double-glazed windows), and consider different weather conditions.

In terms of open-source tools, OMNeT++,[10] and *adevs* are general purpose discrete event simulators used in academia and industry.[11] For network simulation there is wide acceptance of ns, Network Simulator (ns-2 or ns-3).[12] Another example is INET (a networking simulator used with OMNeT++) and OPNET,[13] employed for performance and network behavior (note that OPNET Modeler is proprietary). There is a wealth of relevant work in analysis studying the impact of attacks specifically in telecommunications. For example, SEA++ is a framework written in OMNeT++/INET[14] where authors have proposed a high-level Attack Specification Language to help modelers define and consider attacks in the network level.

Tackling power GT&D involves the numerical solution of linear equations thus many tools have been proposed over the years. For generation, MATPOWER[15] solves power equations with MATLAB whereas Powerflow (proprietary) computes load flows for 10 to 10 k electrical buses. Other known proprietary tools include PowerWorld, a visual approach to power simulation, and the Real Time Digital Simulator (RTDS) equipped with real-time simulation.

Specialized CPS require proper analysis methods to guarantee data consistency in the presence of combined power and telecommunication challenges in large scale systems. Palensky et al[16] discussed six dimensions to advance the understanding of SG combined with modeling and simulation: (i) realistic topologies; (ii) data flow and concurrency; (iii) simultaneously tackling multiple events happening in the infrastructure; (iv) issues related to variable structure dynamics, that is, situations where CPS enable/disable/alter parts, influencing other systems; (v) modeling language, offering initialization, incremental modeling, reuse and readability; and (vi) scalability issues.

For simulating power at the distribution level, GridLAB-D[17] employs agent based simulation for house thermal models, appliances, power distribution feeders, and scheduling configurations. OpenDSS[18] simulates distribution power systems and models multiple DER whereas EnergyPlus[19] (free) is used to address complex building power flows with different materials. It is worth mentioning that the latter is also equipped with co-simulation capabilities. The SGSim framework combines OMNeT++ and OpenDSS into one solution for distribution power networks[20] with a visual interface. A proprietary tool called Power System Simulator (PSS) addresses transmission and distribution. A similar tool is DIgSILENT PowerFactory (proprietary), a real time simulation engine for large distribution networks.[21]

An example of a general purpose co-simulation framework is Mosaik[22] (written in Python) employing PYPOWER for optimal power load computation. Another project worth noticing is the Global Event-driven Co-simulation platform (GECO).[23] It combines the Positive Sequence Load Flow (PSLF) tool with the Network Simulator version 2 (ns-2). One co-simulation tool that offers a model-based approach is the Integrated tool chain for model-based design of CPS (INTO-CPS).[24]

We also mention the Cyber physical co-simulation platform for Distributed Energy Resources in SG (CyDER),[25] developed to function as a modular co-simulation framework for multiple DER and their interaction with stakeholders. Puerto et al[26] provided a similar approach with the Zero OBvious Node Link co-simulator (ZerOBNL) employing pandapower[27] in a partitioned approach, where modeling elements are divided into more manageable parts to ease analysis efforts. More recently, Morstyn et al[28] presented a framework called the Open Platform for Energy Networks (OPEN) for modeling and simulating SG elements with examples consisting of EV and Energy Management Systems (EMS) interaction.

In terms of defending Supervisory Control and Data Acquisition (SCADA) systems, Nazir et al compiled a comprehensive list of vulnerabilities.[29] Other surveys and systematic reviews tackled CPS, IoT, power, and the SG.[30,31,32,33,34] Work on security and privacy of SG discussed location obfuscation techniques, corrupt data detection algorithms, cloud network data security, privacy preservation, and mobile user data privacy.[35] Kundur et al[36] proposed a cyber attack impact analysis using graphs for the SG. The authors discussed the importance of plausibility and severity of vulnerabilities and attacks in coupled networks.

There is also an increasing interest in developing testbeds for analyzing SG designs and addressing cyber-physical security concerns.[37] The idea is to devise realistic settings that closely maps the actual infrastructure, energy loads, and telecommunication patterns to assess problems and trade-offs on alternative scenarios. Ashok et al[38] devised a domain specific testbed for investigating design shortcomings and training stakeholders to better respond to grid situations. Another research developed the SCEPTRE toolchain,[39] a virtualized (on-line) approach considering multiple DER that focuses on telecommunication latencies.

Tesfatsion et al[40] developed the Agent based Modeling of Electricity Systems (AMES) for modeling Transactive Energy Systems (TES) that approximate the energy market to customers and wholesale/retail suppliers as well as different design options. In the same direction, researchers have devised the Transactive Energy Simulation platform (TESP)[41] and the ITD-TES Platform.[42] TESP aggregates other tools and provides a framework that integrates buildings (using EnergyPlus), households and weather (GridLAB-D), and allows the integration with so called "agents" that may be attached to the co-simulation. ITD-TES considers Integrated Transmission & Distribution (ITD) systems and an environment to test transactive designs according to sets of strategies (eg, centralized vs distributed approaches for energy bidding and committing).

2.2 | Desired co-simulation features for security

A considerable body of work exists on broad aspects of cyber-physical security tackling different dimensions,[43,44,45,46,8,6] as well as a survey of surveys about these issues.[47] Research gaps highlighted in these surveys include: (1) modeling incident responses and impact in co-simulation frameworks; (2) easy to read and interchangeable format for representing security incidents; (3) simulation of cascading attacks (or chain failures) and their effects on the infrastructure; (4) data obtained from security based testbeds (used as parameters to models) from real-world architectures addressing attacks or instabilities; (5) studying the system-wide effects of incidents over wide-areas impacting energy GT&D as well as telecommunication networks; and (6) corrupted data transmission across the ICT infrastructure (from different sources with replay or data injection attacks) and impacts on system-level decisions to balance energy supply and demand.

Governmental stakeholders must ensure reasonable service reliability by regulating energy infrastructure providers. The focus is on the use of policies and techniques to accommodate traditional threats such as weather or climate related, equipment failures, attacks, accidental damages, or human errors in representative models. The US Department of Energy (DoE) has proposed a Vulnerability Assessment Process (VAP) in the Infrastructure Assurance Outreach Program[48] consisting of nine steps: (1) evaluate threat environment; (2) information network architecture assessment (eg, SCADA and EMS); (3) penetration testing of information systems; (4) physical security assessment; (5) operations security assessment; (6) review administrative procedures and policies; (7) Physical asset analysis; (8) impact analysis; and (9) risk characterization.

With respect to the assessment proposed by the US DoE, there is a need to consider different types of threats (#1), architectures (#2), across multiple types of physical equipment (#4, #7), distinct operational aspects (#5, #6), impact analysis (#8), and risk characterization (#9). Penetration testing is out of the scope of modeling and simulation because it is usually addressed after the system is physically operational.

The VAP (from #1 to #9) is mapped as follows:

- Types of threats (#1): (a) Agent: terrorism, financial, criminal, nonmalicious user; (b) Market: exposure of the transactive energy market; (c) Asset: elements belonging to the infrastructure, systems, devices, sensors, DER, ESS, servers;
- Different architectures (#2): Handle scalability (different magnitudes, geographically dispersed entities), continuity (of services, power provision), complexity, flexibility, heterogeneity (vendors, suppliers, equipment, devices, components);
- Physical equipment (#4, #7): (a) Quantitatively show the harmful effects of cascading failures as disruptions in key components that may influence the service level in the grid; (b) Uncertainty and variability in energy load (intermittent behavior); (c) Representing different granularity for devices, appliances, and components;
- Operational aspects (#5, #6): (a) Deal with the needs and expectations of stakeholders in the short/long term planning; (b) Involve stakeholders in communications and power networks; (c) Define energy test feeders to address possible configurations and loads; (d) Adjust the level of monitoring and control; (e) Capture social/behavioral aspects of so called *prosumers* and dynamic energy pricing; (f) Model mitigation strategies and coordination of responses in the event of incidents or service interruptions; (g) Adjust maintenance options through modeling;
- Undertaking impact analysis (#8): (a) Impact on market and system operations affected by attacks; (b) System impacts on reliability and costs;
- Risk assessment (#9): (a) Characterization of the value and importance of assets; (b) Comparison and evaluations;

The target audience for these integrated systems are network and power managers (working together in a joint control operations room), ICT administrators, infrastructure owners, aggregators, suppliers/vendors, and solution developers working on applications to assist SG management. Timescale is another important aspect as operators may be interested in planning energy demands in the long term whereas building managers may be concerned with daily needs, adjusting supply/demand accordingly.

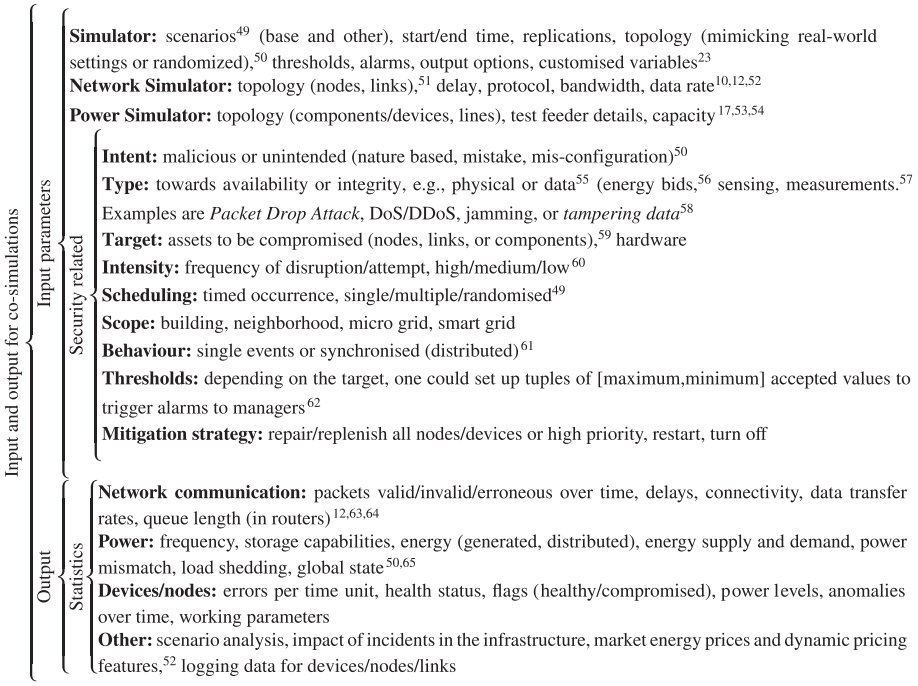
We highlight crucial characteristics with respect to the security spectrum of *desired functions* to embed into co-simulators:

- Integration of continuous and discrete simulations capturing interaction between power and telecommunication;
- Simple to use interface for designing scenarios and assigning parameters to define multiple heterogeneous targets;
- Reasonable modeling abstraction of the reality in terms of topological features, offering different level-of-detail (for various audiences);
- Helpful to stakeholders working across planning, maintenance or decision making in different time scales and objectives (short or long term);
- Work with different energy profiles across buildings, houses, commerce, and industry;

One could better exemplify co-simulation modeling characteristics by aligning desired features with security requirements:

- Tackling *incidents* in general, that is, attacks, accidents, malicious behaviors;
- Definition of *events*: incidents (what?), locations (where?), list of affected equipment (who?), service dependencies, with a timestamp or scheduling of events happening (when?). Modelers may instantiate *types* of events, for example, single, multiple, or synchronized events across the infrastructure;
- Assigning *thresholds* and addressing the consequences of incidents, for example, which device or stakeholder is affected;
- Use of alarms and triggers that are activated when reaching predefined threshold values;
- Interoperability among co-simulators: (i) seamless transformation across co-simulators with similar characteristics; (ii) modelers may select target platform to match incidents described in the model;

We list below a summary of desired features of simulators for security.[49-65]



3 | CO-SIMULATION FEATURES FOR MODELING CYBER-PHYSICAL SECURITY

Researchers use SLRs to select key work and evaluate research gaps and venues for pursuing neglected investigation paths.[4] We present next our literature review identifying tools for co-simulating security incidents and extracting features from the frameworks. Our research question was "What features are needed in a tool in order to simulate security incidents in Cyber-Physical Systems?" The review protocol focused on the following scientific resources: (1) Google Scholar; (2) ACM Digital Library; (3) IEEE Xplore; and (4) Scopus between January/2009 and December/2019.

As exclusion criteria we disregarded papers: (i) failing to address the physical part of CPS in conjunction with network communications; (ii) having simulation tools described only as related work, not as the main paper's objective; and (iii) with research not tackling security incidents or physical/integrity concerns, for example, where adversaries are only using telecommunication networks. The search string used to retrieve documents was:

(("simulation" OR "co-simulation") AND
("tools" OR "framework" OR "software") AND
("security" OR "incident"OR "attack" OR "vulnerability") AND
("cyber-physical system" OR "CPS" OR "smart" OR "infrastructure"))

The inclusion criteria selected work that has used simulation or co-simulation with focus on cyber-physical security, safety, and incidents in CPS (it may be related to Advanced Metering Infrastructure—AMI—or similar technologies) using power and network telecommunication in a coupled mechanism. We excluded work that: (i) it concerned low level domain application (eg, work on hardware aspects and internals of Phasor Measurement Unit [PMU], smart meters or smart cards); (ii) addressed only physical security issues in power systems (eg, transient voltages) instead of cyber concerns; (iii) employed other technologies for communication; iv) did not detail communication network parameters; v) used game based, Monte Carlo Simulation, Dynamic Systems, Linear Programming, or optimization techniques; (vi) published a poster or short paper (up to four pages); were (vii) patents; (viii) theoretical frameworks; or (ix) proofs of concept. The data extraction and reporting phase will list bibliographical details, toolchains, or auxiliary tools, offered features for modeling and simulating security incidents, and tool integration details for coupled power and telecommunication networks, and scalability.

3.1 | Extracted features from selected literature

We queried the list of scientific libraries using our search string. Then, we applied the inclusion and exclusion criteria in the yielded results, which resulted in selecting 15 papers for deeper inspection (identified next by the # symbol). For these results we extracted their main features and tools for simulating cyber-physical security incidents in CPS.

[#01]: Chinnow et al[50] extended an auxiliary tool called NeSSi[66] for their simulation needs. They used a multi-platform solution combining Java with InterPSS[67] to model and simulate the power network. They presented a simple case study and an evaluation of data corruption attacks for AMI. They considered data issues for a case study that represented two attack scenarios: (1) Falsely Reporting Low Consumption; and (2) Falsely Reporting Low Prices. Both attacks influenced the energy market prices with wrong information simulated via the auxiliary tools where they measure the impact of data alterations over the infrastructure. They modeled attacks by different adversary types, for example, outsiders, homeowners, and by an energy provider employee. It employed a supporting tool called NeSSi[2], implemented as a security-oriented framework.

[#02]: The Attack Simulation TOolset for Smart GRid InfrAstructures (ASTORIA) by Wermann et al[60] used co-simulation to evaluate and analyze the impact of malicious attacks in SG components. It described a framework where modelers can specify customized topologies to build realistic simulation scenarios. ASTORIA used three auxiliary tools: PYPOWER, ns-3, and Mosaik. It offered the capability of modeling security attacks and incidents in the SG.

[#03]: Gupta and Akhtar[34] made a survey on frameworks, tools and security issues of smart power grids. It cited power and networking simulators, discussing strengths and weaknesses. The authors described simulation models and address how one may combine tools in a co-simulation.

[#04]: The paper by Sgouras et al[68] addressed attacks on AMI using realistic grid topologies. The authors analyzed the impact of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) on power distribution's reliability. A power simulator was not used, however, this work is relevant to discussions about AMI related security shortcomings. As a result, the authors state that DDoS attacks over critical peak hours increase interruption probability due to unavailability of Demand Response (DR) controlled loads. The authors used an auxiliary tool called realistic simulation environments (ReaSE)[69] to generate realistic data traffic patterns of common communication protocols. Other auxiliary tools were OMNeT++ and INET.

[#05]: Queiroz et al. (2011)[65] described a framework for SCADA based simulations, helping modelers test the effects of malicious attacks and evaluate security. It used OMNeT++ and INET and an auxiliary tool for designing network topologies called NED. For power simulation it connected to a MATLAB/Simulink model using SimPowerSystems for representation of a wind farm of six wind turbines connected to a 25 kV distribution system.

[#06]: The Cyber-Physical Security Assessment (CPSA) by Saxena et al[62] used co-simulation to identify vulnerable states allowing control center operators to devise countermeasures to mitigate disruption in the physical layer. For co-simulation, the tool employed auxiliary tools such as GridSim, MATLAB, Matlabcontrol (Java to MATLAB), PowerWorld, and JADE (Java to PowerWorld). It presented a graphical interface for modelers detailing the communication among different smart components, logging, and contingency analysis. The tool major stakeholders were control center operators, where they may create responses in security assessments yielded back by their simulator. The authors have discussed and implemented interesting features, however, the network communication missed significant details (eg, they have used GridSim for a limited topology). They ended the work by discussing how the tool may be used for training operators to react to potential cyber-attacks in power systems.

[#07]: Tundis et al[49] focused on attack scenario modeling in critical infrastructures. The objective was to identify unexpected behavior, anomalies, and vulnerabilities. The authors implemented a Smart Grid Simulator for experimentation and validation of the approach in a realistic case study. Attack simulation complemented testing and validation phases of the SG defining attacks, scenarios, and targets with a reasonable amount of detail. The drawbacks are that it is proprietary and no power or network auxiliary tool was employed for the analysis.

[#08]: Babu et al[70] characterized attack data in high fidelity datasets with close interactions among physical and cyber communications in SG using PowerWorld. The authors produced a case study using a Network Intrusion Detection System (NIDS), focused on monitors that could identify attacks from previous signatures and differentiate them from regular traffic. They have presented a six-step attack plan to shut down two generators in the grid, mapping the network topology with the power topology to inspect which components were being affected.

[#09]: Pan et al[55] have combined DIgSILENT PowerFactory, OMNeT++, and MATLAB in a co-simulation. The focus of the work was on data attacks targeted at EMS and a vulnerability assessment framework. It discussed attackers gaining access to measurement data such as: (i) on Remote Terminal Unit (RTU; containing power flow measurements that are

sent to SCADA servers); (ii) on the communication network; and (iii) on the master server. Such large scale systems are usually equipped with alarms that are triggered through a scheme known as Bad Data Detection (BDD), activated when measurements exceed a threshold (eg, inaccurate data or failing RTU). The work focused on specific components such as RTU, communication network, and SCADA controllers. It discussed how attackers may deflect detection by inserting measurement data to influence the BDD scheme. As drawbacks, the co-simulation did not detail the impact attacks in the SG nor the used parameters and topologies.

[#10]: Genge and Siaterlis[61] described an experimental framework for modeling and simulation of the SG, allowing scenario exploration for understanding the impact of cyber attacks in the infrastructure. The authors have used MatDyn (integrated with Simulink) for the power simulator and Emulab[71] (an emulation testbed with arbitrary topology generation and other features suitable for realistic network flows) for simulating the communication network. It discussed the harmful effects of voltage oscillations due to synchronized attacks showing results per power bus in the grid topology.

[#11]: The paper describes the Transactive Energy Security Simulation Testbed (TESST) by Zhang et al,[72] a testbed for simulating cyber attacks in energy pricing. The authors have used PYPOWER, GridLAB-D, ns-3, and EnergyPlus for modeling transmission, distribution, telecommunication, and buildings, respectively. Transactive energy markets are decentralized models where end-users play active roles in managing energy consumption and generation that influences electricity pricing. The authors have extended the TESP where they have incorporated security concerns. The paper discussed how DoS attacks may influence pricing due to information unavailability or delays between end-points.

[#12]: Moulema et al[52] used the Framework for Network Co-Simulation (FNCS),[73] a co-simulator integrating GridLAB-D, MATPOWER, and ns-3. The idea was to create several co-simulation scenarios and study the impact of attacks. The results offered different ways of analyzing smart meters tackling network, data, and market concerns. It demonstrated how to build scenarios and how to change network performance and attack parameters and their effects on power and market.

[#13]: Sridhar and Govindarasu[57] were concerned with security applied to the Automatic Generation Control, a frequency control application encompassing a large area responsible for handling power flow and frequency measurements from remote sensors. The authors have developed a resilient control framework and described mitigation techniques to maintain system stability. The target for the study was on data integrity attacks, where they have implemented their own simulator. It focused on modeling adversaries, showing the impact of attacks on frequency.

[#14]: Mohsenian-Rad and Leon-Garcia[74] have modeled an IEEE 24-bus for Load Altering Attacks. The model did not consider the networking infrastructure, however, it presented interesting discussions on the effect of attacks in power grids. Energy managers could choose to protect vulnerable loads or implement a partial load protection scheme. Also, the paper discussed the cost of protection, a crucial metric for managers when deciding how to defend from attacks.

[#15]: Çetinkaya et al[51] addressed research challenges behind security incidents with ns-3. They discussed the main challenges in large scale networks and major events that impact normal operations. The authors commented on challenges such as: (i) natural component failures; (ii) misconfigurations; (iii) cable cuts; (iv) jammers; (v) interference; (vi) weather precipitation; (vii) attack against infrastructure component; (viii) natural disaster; (ix) pandemic; (x) nationwide Internet outage; (xi) power failure; (xii) electromagnetic pulse attack; and (xiii) coronal mass ejection (eg, solar flares). They classify *intent* (nonmalicious or malicious), *scope* (nodes, links, or area), and *domain* (wired or wireless).

3.2 | Feature analysis

Our SLR focused on co-simulation and modeling features of cyber-physical security incidents. It is worth mentioning that when tackling data attacks, one could abstract the telecommunication network and emulate data corruption directly at the component level, for example, by altering measurements. However, for availability attacks, it makes sense to model the communication infrastructure among participants as delays or malicious injection of packets impacting other portions of the SG.

Some papers were preselected and then discarded to follow the exclusion criteria. Nevertheless, they offered valuable features to incorporate into our discussion. For example, Baetens et al[75] have modeled a set of electricity feeders according to the size of their aluminium cables (for IEEE radial distribution 34 Node Test Feeder), categorizing them into strong, moderate, and weak feeder designs. For realistic simulations one must address electric feeder characteristics because they influence the power and the incidents that may occur. Table 1 shows an overview of extracted features per paper (from 01 to 15, market with a # symbol).

TABLE 1 Overview of features of selected related work from the SLR

#	Co-Simulation engine	Security incident	Target	Output
01	Nessi2, InterPSS	Falsely report low consumption Falsely report low prices	Smart Meter	voltage Power mismatch
02	PYPOWER, ns-3, Mosaik	Malicious software infection DoS buffer overflow, IP spoofing	SCADA	Power consumption
03	*Survey of tools*	Message dropping, time delays	–	–
04	OMNeT++, INET	DoS/DDoS	Smart Meter	Packet statistics
05	OMNeT++, INET, MATLAB/Simulink	MiTM, eavesdropping, spoofing	Smart Meters PLC	Service level Power generation
06	GridSim, MATLAB, PowerWorld, JADE	MiTM, DoS, delay	Disabled RTU Comm. delay	Voltage, active or reactive power
07	Smart Grid Simulator (own implementation)	Energy theft, pushing, link disc., component status, I/O manip., packet dropping/cloning	Power gener.	Attacks over time and voltage
08	PowerWorld	Multi-stage attack	Power gener.	Latency, data rate
09	DIgSILENT PowerFactory, MATLAB, OMNeT++	False Data Injection, DoS jamming, combined attacks	SCADA, RTU	Packet loss Network delay
10	MatDyn, Emulab	Physical attack	PLC	Voltage, load
11	GridLAB-D, ns-3, EnergyPlus, PYPOWER	Bid price/quantity manipulation	Energy market	Energy price
12	FNCS (GridLAB-D, ns-3), MATPOWER	False data injection, DoS	Energy market	Energy demand and response
13	*Model-based approach*	Data integrity attack Load altering attack	—	System frequency
14	*Numerical analysis*	Load altering attack	SCADA	Cost of load protection, flows
15	ns-3, NetAnim, KU-LoCGen (topology)	Modeling of various *challenges* Wide area disasters	ICT network	Packet delivery ratio

Attacks aimed at security are directed toward one or more dimensions of the CIA triad: Confidentiality, Integrity, or Availability ("Non-Repudiation" is out of the scope of this work, that is, the association of actions to unique individuals). We comment below on the issues addressed in the triad as discussed by Gunduz et al[76]:

- *Confidentiality*: papers #05 and #06 tackled Man-in-The-Middle (MiTM). Other attacks were not investigated such as: traffic analysis, phishing, wiretapping, hijacking (session), social engineering, Domain Name System (DNS) poisoning, unauthorized access, sniffing, replay/playback, tunneling, scanning, key/certificate replication;
- *Integrity*: work has considered Physical, Data Integrity/Corruption/Tampering, False Reporting (consumption/prices), False Data Injection, Bid Price or Quantity manipulation, Buffer overflow and Time delay/synchronization. Masquerading was not mentioned. However, it has been used indirectly in market bidding;
- *Availability*: interest were directed toward DoS/DDoS, Load Altering, Load Drop, Coordinated Load Changing, Malicious software infection (malware), Jamming (channel), Packet/Message drop/Blackhole. On the other hand, Spamming, Routing, Wormhole, Teardrop, Smurf, Flooding, and Zero-day attacks were not modeled in the body of selected work;

We have conducted an analysis in the feature set to identify similar characteristics and to categorizing it according to attack type, objective, and targeted infrastructure. The features were divided into seven groups (A–G), where G was sub-divided in eight parts.

- *A. Topology (network/power)*: modeling power and network topology for entire portions (parameter N households) of the grid, with a mapping from one to another. Automatic generation of ns-3 code according to topology parameters. Definition of critical elements within the infrastructure and use of auxiliary tools for topology generation. Modeling parameters such as number of nodes/edges, degree, clustering, diameter, hop count, and link (bandwidth) configurations.
- *B. Data related*: change data or measurements in smart components/devices, corrupting it or changing to maximize profits or reduce energy costs. Modeling data attacks: Energy Theft or Pushing, component status change, link disconnection, input/output manipulation, packet dropping/cloning.
- *C. Network communication and power related parameters*: parameters for telecommunication networks such as topology, packet size, delay, propagation delay, dropped messages per time unit, number of connected devices, protocol, and data rate. It was important to identify network traffic parameters and power measurements as well as control commands. Ability to save data (logging) to serve as evidence of attacks in the infrastructure, so it could be later replayed for more thorough investigations. Modelers may select the most appropriated test feeder to use in their design as it directly impacts power behavior among electrical buses in residential, commercial, and industrial areas.
- *D. Realistic settings*: the system must have the ability to work with realistic network communication flows in normal and in under attack situations. Also, it should allow to replay traffic and work with real world traces obtained from logs from utilities or other external datasets. Some authors discussed inserting random (traffic) noise for realistic analysis.
- *E. Attacks*: attacks were modeled by different aspects of coupled systems. It is worth commenting that some models considered attacks following timed incursions (schedules), adding control to the analysis, or a randomized approach happening in any point in simulation time. *Types*: DoS/DDoS (flooding, buffer overflow), packet spoofing and MiTM, eavesdropping, malicious software infection (modification of measured data), energy theft, Data Integrity (False Data Injection attack), Data Availability (jamming), combined attacks (eg, false data with network overflow, simultaneously), synchronized attacks, load attack, manipulation of bid price and bid quantity, Disabled RTU and communication delay at a substation, and timed attacks (according to a schedule) *Targets*: Smart meter, utility server, substations, hardware, or SCADA components.
- *F. Output*: investigation of the telecommunication network coupled with power related statistics. For instance, outputs showing plots with frequencies, power mismatch, energy consumption/generation, oro bidding prices. For communication, research investigated packet quantities, queue length in routers, and errors. In terms of general output, we mention number of attacks over time (if attacks are randomized, unscheduled, or uncontrolled).
- *G. Modeling features*: a reasonable number of extracted features was related to modeling aspects where we have categorized them as follows:

  - *G1. Modeling attackers and scenarios*: some authors discussed the need to devise attacker profiles to guide their actions, modeling the attainable attack surface and specific targets. Another interesting feature was to devise

attack scenarios to ease analysis. Other work focused on defining acceptable thresholds to increase detection because they could act as alarms for improper use. Authors also discussed how attackers may circumvent detection by choosing specific transmission patterns for susceptible targets. There were considerable concerns directed at attack locations and which components were affected.

- *G2. Modeling attacker behaviors and defenses*: some papers discussed not only attackers, but also defenses to improve security. They have directed their attention to the set of actions adversaries perform after gaining access to specific networks, increasing their privileges, protecting data, guaranteeing consistent energy bid prices and quantities, and on learning and predicting energy demand according to truthful measurements.
- *G3. Tackling synchronization*: authors have studied the hazardous effects of synchronized incidents to imbalance frequency regulation. It is caused by installing malicious software into inexpensive CPS or IoT systems that controls high-wattage devices. The idea is to toggle power on or off to cause damage in frequency destabilization attempts.
- *G4. Targets*: foci targeted physical attacks in equipment (hardware) or substations and impact on availability. When modeling adversaries, simulations must incorporate overloading the network infrastructure (excess packets) as well as altering meter measurements. Some authors were also concerned on attacks directed at data servers since they have specific power requirements and may disrupt grid operation in more harmful ways than common operations.
- *G5. Impact analysis*: one interesting feature when simulating the SG was the ability to study the impact of incidents in energy levels, device statistics, and packet traffic. The idea is to evaluate different dimensions in coupled systems and investigate variations as synchronized attacks may take place.
- *G6. Features*: one work has addressed the need to devise an extensible library of attacks, which modelers may extend it to compose more sophisticated incursions. Other interesting features included the computation of global state estimators, logging data from components, generating forecasts based on historical data, modeling different challenges of networks as well as incorporating disruption of large parts of telecommunication networks.
- *G7. Interfacing with other components*: the idea was to combine internal components' behaviors and the ability to generate useful output when communicating with the co-simulation engine. For example, one work developed ways of providing an interface to connect with SCADA components.
- *G8. Baselining*: in simulation, it is usual to create a model to base all subsequent comparisons and analysis. By devising baseline results, modelers may understand and better evaluate the impact of attacks and assess countermeasures to contain or mitigate attacks in CPS.

3.3 | Summary and insights

Three major themes emerged during the SLR for tackling security. Work has focused on (i) physical attacks (directed at one or multiple targets); (ii) data altering attacks (corrupting monitoring/sensing data or market pricing exchanges); and (iii) flooding the network with spurious packets (DoS/DDoS). The interplay and coordination effort to deploy effective operations in CPS involve different stakeholders with distinct objectives. Table 2 relates our features groups across papers retrieved by the SLR.

We discovered a total of 16 stakeholders across the selected documents. Table 3 shows how each feature group is related. It is noticeable that the *Feature C*. (eg, Power/Network parameters) was addressed by all stakeholders.

For security purposes, adversaries aim to disrupt operations, gain access, avoid detection, or tamper data. A wealth of research has stressed the need to use realistic topologies in networks close to real-world traces as well as incorporating random traffic noise while communicating. The idea is to have a framework for analyzing future attack patterns where the infrastructure may counteract or adapt to incidents. Logging plays an instrumental role in simulation because one may replay the incident and or diminish their harmful effects. It may also be used in validation and accreditation to convince audiences on the benefits of using co-simulation in complex settings of critical infrastructures.

The set of data-related attacks surveyed here focused on meter data and energy bidding in dynamic markets. Another common aspect to study when incorporating networking into co-simulations is modeling DoS/DDoS. We observed the use of toolchains and auxiliary tools to drive simulations as several results have used third-party software. Finally, some studies have tackled synchronized interventions (both unintended and malicious), and the effects on electricity prices and on energy related decisions by managers.

TABLE 2 List of features in retrieved work according to group

	Papers retrieved in the SLR (#)														
Feature group (out of 113 feat.)	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**
A. Power/Network topology (7)	✓							✓				✓			✓
B. Data related (5)					✓	✓	✓								
C. Power/Network parameters (12)		✓	✓			✓	✓	✓	✓		✓	✓			✓
D. Realistic settings (7)				✓				✓			✓		✓		✓
E. Modeling attacks (15)		✓		✓	✓	✓	✓		✓	✓	✓	✓	✓		
F. Output features (11)	✓	✓		✓	✓	✓	✓			✓	✓	✓	✓		✓
G1. *Attackers* (14)	✓	✓				✓	✓					✓	✓	✓	
G2. *Behaviors and defenses* (5)			✓					✓					✓	✓	
G3. *Tackling synchronization* (4)										✓			✓	✓	
G4. *Targets* (9)			✓	✓	✓	✓	✓							✓	✓
G5. *Impact analysis* (4)	✓		✓			✓									
G6. *Features* (13)		✓				✓									✓
G7. *Interfacing w/components* (3)		✓			✓										
G8. *Baselining* (4)				✓		✓						✓			

TABLE 3 Major stakeholders according to feature group

Group	S01	S02	S03	S04	S05	S06	S07	S08	S09	S10	S11	S12	S13	S14	S15	S16
A.	✓			✓	✓	✓		✓							✓	
B.	✓	✓								✓		✓	✓			
C.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
D.				✓	✓	✓	✓			✓				✓		
E.	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
F.	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
G1.	✓	✓	✓				✓	✓	✓	✓		✓	✓			
G2.				✓	✓				✓	✓						✓
G3.	✓			✓					✓	✓						
G4.		✓				✓	✓		✓	✓		✓	✓			✓
G5.	✓												✓			✓
G6.	✓		✓			✓	✓		✓	✓			✓			
G7.	✓		✓				✓		✓	✓						
G8.							✓	✓					✓			

Stakeholders:

S01—Researchers	S09—SG operators
S02—Engineers	S10—SCADA operators
S03—System administrators	S11—SCADA operators (focus: EMS)
S04—NIDS researchers	S12—Domain experts (SG related)
S05—Network administrators	S13—Control Centre Operator
S06—Network administrators (focus: topology)	S14—DSO
S07—Utility companies (and ESCO)	S15—DSO (focus: market and pricing)
S08—Utility companies (focus: DR)	S16—Multiple (eg, survey)

Figure 2 shows modeling choices in SG and open-source frameworks. It is noticeable that many tools are required in conjunction for a comprehensive analysis depending on the modeling objective. It also shows where security officers may direct their attention for integrity and availability analysis (they correspond to boxes in red in the figure).

Cyber-physical security may address uncertainty and adverse conditions in weather affecting power generation, storage (batteries), physical attacks and delays in CPS and IoT as well as synchronizing incursions in appliances working at the same schedule (through malware). The figure shows dependencies among modeling possibilities, for example, to model embedded generation, or "behind the meter generation," one should consider the weather aspects that may influence renewable power provision.

Figure 3 presents a summary of findings in the SLR. There is significant use of free and open-source as well as proprietary frameworks and a preference for using open-source networking solutions (eg, ns-2, ns-3, and INET). It shows the major topics found in the SLR for co-simulation of CPS where targets were SCADA components, power generators, market, and ICT. Few results have tackled confidentiality due to difficulties in modeling these aspects in a realistic manner (one models the consequence of breaching systems, that is, what happens after these occurrences).

4 | CONCLUSION

Over time, interaction, design, implementation, evaluation, monitoring, and maintenance of CPS will only increase their relevance. As these systems are physically deployed, customers and managers must ensure their trustworthiness (security, privacy, safety, reliability, and resilience). It is thus essential to conduct thorough and timely cyber-physical security analysis when addressing critical infrastructures.

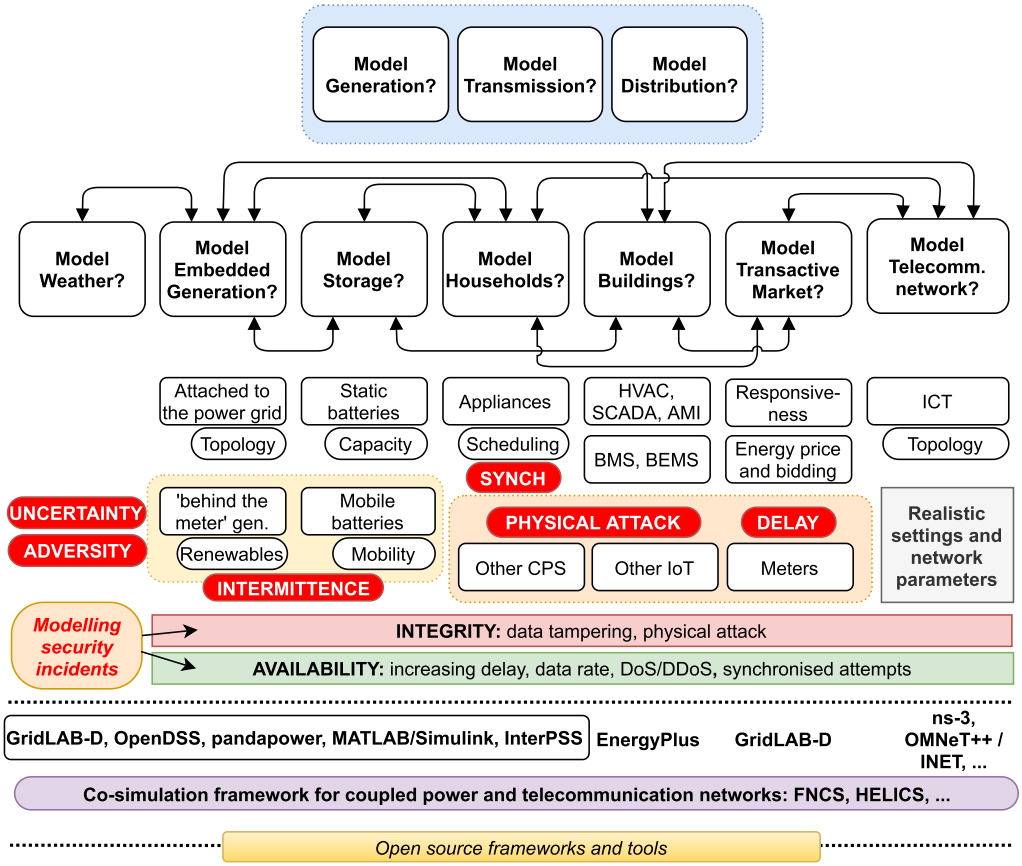


FIGURE 2 Modeling possibilities in SG contexts with respect to security and open-source frameworks

The state space size needed to model a set of interacting CPS makes formal approaches impractical. That is the main reason why co-simulation approaches emerge as mechanisms to tackle difficulties in CPS settings. These techniques could be used before physical deployment where modelers and analysts can test configurations and make decisions involving cost-benefit trade-offs. Simulation allows multiple scenario creation by altering parameters and evaluating the impact of each one on selected metrics of interest.

Many existing co-simulation frameworks and solutions are built for modeling general-purpose behaviors. Modelers may employ the tools to consider a number of concerns, not specifically security. That is one of the reasons as to why we selected 15 papers and extracted a total of 113 features closely related to cyber-physical security, grouping by their characteristics. We have then commented and discussed those features, identifying targets, attacks, and adversarial behaviors.

These protective measures and issues in coupled power and telecommunication networks encompassing complex infrastructures have become high profile in research. The reasons behind cyber-physical security incidents vary, and managers must be prepared for their occurrence. Analysts must also understand how to cope with dynamic attacker behaviors and harmful approaches emerging in CPS as adversaries change strategies and adapt to grid responses. They could use co-simulation and modeling features in frameworks as a meaningful mechanism to understand the consequences of attacks and direct efforts toward detection and mitigation. They could also employ measures to guide design decisions pointing out bottlenecks or improper resource allocation before physical implementation. In a co-simulation, one could model uncertainty by incorporating randomness into the parameters, which could be of value for better evaluations and predictions.

Finally, we have highlighted the importance of vulnerability assessment from authoritative bodies when performing cyber-physical security evaluations in CPS. Targeting weaknesses in the infrastructure may better inform managers as to the most susceptible regions that could be targeted by adversaries. As future work, we aim to extend the SLR and investigate other characteristics of co-simulators where security is also a concern. For example, we may address attacks toward the transactive market to address effective ways for mitigating malicious incursions.

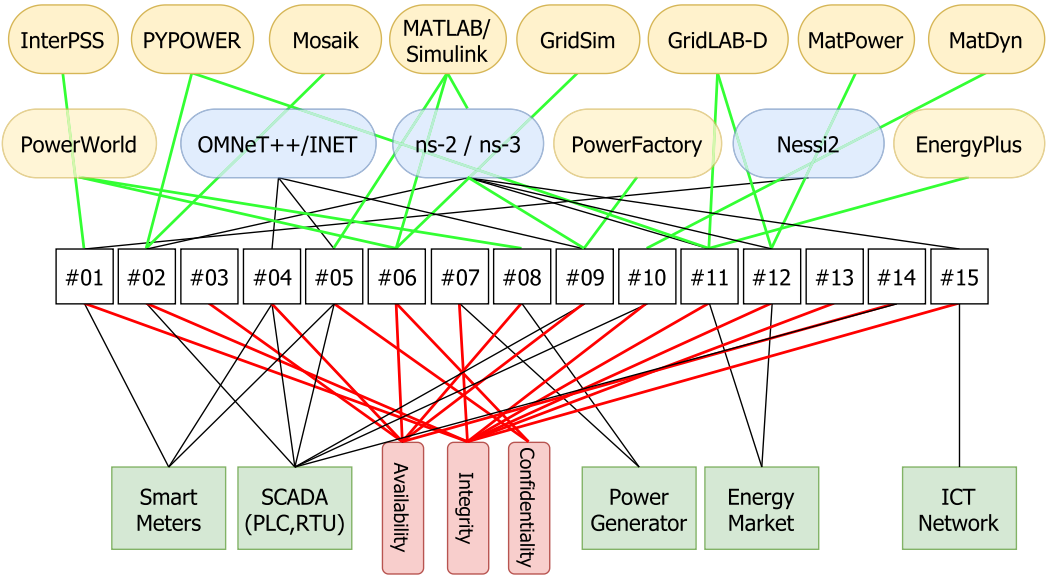


FIGURE 3 Summary of findings in the SLR addressing frameworks, targets, and security dimension

4.1 | Challenges and future research directions

As discussed in the seminal paper of Nicol et al,[77] in dependability and security simulation one models the *consequence* of attacks. In modeling and simulation, a common theme is directed on addressing *integrity* (physical attacks in power or communication lines or servers) as well as *availability* (delays caused by spurious packet injection, jamming, or other incursions). In the SG, adversaries may employ a wide range of strategies to compromise devices and modelers have a large attack surface to consider and evaluate different scopes. For instance, they could want to investigate how latency is affected or what happens if a server or measurement station gets disconnected and how the infrastructure components react.

We list future challenges to address in modeling and co-simulation with ramifications in the security of the SG:

1. *Realism*: improvements to represent complex environments that approximate as close as possible the intricacies of the SG at different levels of detail. These considerations are essential in data-centric environments where multiple CPS converge to provide services to stakeholders;
2. *Market*: tools must integrate the energy market into the modeling designs due to the effect on frequency regulation and the ability to manage small-scale power networks with localized decision making capabilities;
3. *Modeling attackers*: further efforts to represent adversaries' behaviors and consequences to infrastructures. Another concern is to address the propagation and synchronization of high-wattage devices with compromised IoT software[78];
4. *Coupled systems*: further effort to seamlessly integrate modeling of weather, market, buildings, households' appliances, AMI, EV, power generation devices, telecommunication networks, and mix with adversarial behaviors;
5. *Cope with emergent energy resources*: it is a challenge to address new DER participating in the network such as storage (varied capacity), EV (ie, mobile batteries), increased solar/wind penetration, and how *prosumers* may profit from incentives;
6. *Integrated Transmission and Distribution*: co-simulation models will have to consider broader aspects in power happening on the Transmission level that may include large generators integrated with distribution networks as domestic customers may add DER to help frequency balancing and market considerations;
7. *Effects of telecommunication*: analysts must also model how delays and the propagating effects of telecommunication may influence frequency or power provision under stressful conditions caused by attacks;
8. *Improved scenario management*: as the number of scenarios increases, co-simulation tools will have to provide scenario management capabilities to ensure the best analysis options to analysts;
9. *Validation*: determining whether multiple coupled systems are in fact yielding results that are in close match with real settings is an important goal. Improving the validation process for such simulations is thus essential;

10. *Performance of simulators*: a full co-simulation encompasses the use of many auxiliary simulator engines depending on the objective. For instance, if one wants to integrate buildings, telecommunication networks and ITD systems, the software will have to cope with a massive number of computations and synchronization even for reduced time simulations. In cyber-physical security, timely responses are important to contain attacks and quickly devise countermeasures to cope with malicious incursions;

The modeling possibilities should also consider the consequences of data corruption in generation, storage, or transmission as well as the effects of delays in energy aggregation and dispatch, bidding and near real-time dynamic pricing. Only a few frameworks discussed here considered the energy market and how adversaries may influence the designs of TES for increasing protections to suppliers and customers.

Capturing pieces of evidence of attacks (ie, traceability) in simulations to verify how output options could be used to improve the analysis effort of complex systems. Energy stakeholders must be able to identify customers or attackers responsible for malicious actions and provide proof for authorities.

Out of the surveyed work, only a few exceptions allowed proper download and installation of the tool (and auxiliary software and libraries) as well as access to the models. Developers of frameworks and tools must not only ensure timely execution, but also access to the source code and documentation. This is crucial to enable analysts to validate platforms and extend models when adapting to particular situations.

For improving frameworks and tools, there is a need to devise templates of topologies so modelers could easily adapt to their contexts. These systems could allow improved exploratory analysis in complex contexts such as the ones in the SG. For example, modeling predefined power schemes (test feeders), encompassing mechanisms for scaling up and down the number of building and households could be interesting for analysis. All those entities are connected altogether and mapped to the telecommunication networks, with proper Internet addressing, assigned generation units, transformers, power lines, and other components, from the template. This previously set up power topology is matched with the communication network, where the modelers' focus could be directed toward adversaries artificially increasing delay or causing corruption of data in smart meters.

ACKNOWLEDGMENTS

The authors wish to acknowledge funding from the Industrial Strategy Challenge Fund and Engineering and Physical Sciences Research Council (EPSRC/UK) EP/V012053/1 for The Active Building Centre Research Programme (ABC RP).

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

AUTHOR CONTRIBUTIONS

All authors contributed equally to the research.

ORCID

Ricardo M. Czekster https://orcid.org/0000-0002-6636-4398

REFERENCES

1. Ralph L. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security & Privacy*. 2011;9(3):49-51.
2. Case Defense Use. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center (E-ISAC); 2016;388
3. Cláudio G, Casper T, David B, Gorm LP, Hans V. Co-simulation: state of the art. *arXiv preprint arXiv:1702.00686*. 2017.
4. Barbara K, Stuart C. Guidelines for performing systematic literature reviews in software engineering; 2007.
5. Greenwood DM, Yan LK, Patsios C, Lyons PF, Seng LY, Taylor PC. Frequency response services designed for energy storage. *Appl Energy*. 2017;203:115-127.
6. He H, Jun Y. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Phys Syst: Theory & Appl*. 2016;1(1):13-27.
7. Greer C., Wollman DA, Prochaska DE, et al. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*. National Institute of Standards and Technology, U.S. Department of Commerce; 2014.
8. Kevin M, Aparicio OJ, Chris D. Combining power and communication network simulation for cost-effective smart grid analysis. *IEEE Commun Surv Tutor*. 2014;16(3):1771-1796.

9. Cláudio G, Casper T, David B, Gorm LP, Hans V. Co-simulation: a survey. *ACM Comp Surv (CSUR)*. 2018;51(3):49.
10. András V, Rudolf H. An overview of the OMNeT++ simulation environment. In: 60ICST. Institute for Computer Sciences; 2008.
11. Yentl VT, Hans V. An evaluation of DEVS simulation tools. *Simulation*. 2017;93(2):103-121.
12. Riley George F, Henderson TR. *The ns-3 Network Simulator*. Berlin, Heidelberg: Springer; 2010:15-34.
13. Irene K. *Modeling and Simulating Communication Networks: A Hands-on Approach Using OPNET*. Upper Saddle River, NJ: Prentice Hall PTR; 1998.
14. Marco T, Gianluca D, Francesco R, Alexandra S. *SEA++: A Framework for Evaluating the Impact of Security Attacks in OMNeT++/INET*. Cham, Switzerland: Springer; 2019:253-278.
15. Daniel ZR, Edmundo M-SC, John TR. MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Trans Power Syst*. 2010;26(1):12-19.
16. Peter P, Edmund W, Atiyah E. Simulating cyber-physical energy systems: challenges, tools and methods. *IEEE Trans Syst, Man, Cybernet: Syst*. 2013;44(3):318-326.
17. Chassin David P, Fuller Jason C, Ned D. GridLAB-D: an agent-based simulation framework for smart grids. *J Appl Mathemat*. 2014;2014.1–12. https://www.hindawi.com/journals/jam/2014/492320/.
18. Dugan Roger C, McDermott TE. An Open Source Platform for Collaborating on Smart Grid Research; 2011; IEEE; 1-7.
19. Crawley Drury B, Lawrie Linda K, Winkelmann Frederick C, et al. EnergyPlus: creating a new-generation building energy simulation program. *Energ Buildings*. 2001;33(4):319-331.
20. Abdalkarim A, Peter B, Reinhard G. *SGsim: co-Simulation Framework for ICT-Enabled Power Distribution Grids*. Cham, Switzerland: Springer; 2016:5-8.
21. Gonzalez-Longatt Francisco M, Rueda J L. *Power Factory Applications for Power System Analysis*. Power Systems Cham, Switzerland: Springer; 2014.
22. Steffen S, Stefan S, Martin T. Mosaik: A Framework for Modular Simulation of Active Components in Smart Grids. 2011; IEEE; 55-60.
23. Lin H, Veda Santhosh S, Shukla Sandeep S, Lamine M, James T. GECO: global event-driven co-simulation framework for interconnected power system and communication network. *IEEE Trans Smart Grid*. 2012;3(3):1444-1456.
24. Gorm LP, John F, Jim W, et al. Integrated Tool Chain for Model-based Design of Cyber-Physical Systems: The INTO-CPS Project; 2016; IEEE; 1-6.
25. Nouidui Thierry S, Jonathan C, Christoph G, Michael W, Jhi-Young J, Evangelos V. CyDER - an FMI-based co-simulation platform for distributed energy resources. *J Build Perform Simul*. 2019;12(5):566-579.
26. Pablo P, Edmund W, Jessen P. ZerOBNL: A Framework for Distributed and Reproducible Co-simulation; 2019; IEEE; 1-6.
27. Leon T, Alexander S, Florian S, et al. Pandapower—an open-source python tool for convenient modeling, analysis, and optimization of electric power systems. *IEEE Trans Power Syst*. 2018;33(6):6510-6521.
28. Thomas M, Collett Katherine A, Avinash V, et al. OPEN: an open-source platform for developing smart local energy system applications. *Appl Energy*. 2020;275:115397.
29. Sajid N, Shushma P, Dilip P. Assessing and augmenting SCADA cyber security: a survey of techniques. *Comput Secur*. 2017;70:436-454.
30. Xi F, Satyajayant M, Xue G, Yang D. Smart grid—the new and improved power grid: a survey. *IEEE Communications Surveys & Tutorials*. 2011;14(4):944-980.
31. Andrés MC, Nicanor Q, Eduardo MN. A Survey on Cyber Physical Energy Systems and Their Applications on Smart Grids. 2011; IEEE; 1-7.
32. Gao J, Yang X, Jing L, Liang W, Philip Chen CL. A survey of communication/networking in smart grids. *Future Gen Comp Syst*. 2012;28(2):391-404.
33. Volkan G, Steffen P, Tony G, Frank V. A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Trans Internet Inform Syst*. 2014;8(12):4242-4268.
34. Gupta BB, Tafseer A. A survey on smart power grid: frameworks, tools, security issues, and solutions. *Annals Telecommun*. 2017;72(9–10):517-549.
35. Boroojeni Kianoosh G, Amini MH, Iyengar Sundararaja S. *Smart Grids: Security and Privacy Issues*. Cham, Switzerland: Springer; 2017.
36. Deepa K, Xianyong F, Shan L, Takis Z, Butler-Purry Karen L. Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. 2010; IEEE; 244-249.
37. Cintuglu MH, Mohammed OA, Akkaya K, Uluagac AS. A survey on smart grid cyber-physical system testbeds. *IEEE Commun Surveys & Tutorials*. 2017;19(1):446-464.
38. Aditya A, Siddharth S, Tamara B, et al. A multi-level fidelity microgrid testbed model for cybersecurity experimentation. 12th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 19). 2019.
39. Jay J, Ifeoma O, Patricia C, Wright Brian J, Nicholas J, Christine L. Assessing DER network cybersecurity defences in a power-communication co-simulation environment. *IET Cyber-Phys Sys: Theory & Appl*. 2020;5(3):274-282.
40. Leigh T. *Electric Power Markets in Transition: Agent-Based Modeling Tools for Transactive Energy Support*. North Holland, Netherlands: Elsevier; 2018:715-766.
41. Qiuhua H, McDermott Thomas E, Yingying T, et al. Simulation-based valuation of transactive energy systems. *IEEE Trans Power Syst*. 2019;34(5):4138-4147.
42. Trung NH, Swathi B, Reddy TR, Zhaoyu W, Leigh T. An integrated transmission and distribution test system for evaluation of transactive energy designs. *Appl Energy*. 2019;240:666-679.

43. Todd B. *Literature Review on Smart Grid Cyber Security*. Collaborative Software Development Laboratory Honolulu, HI: Collaborative Software Development Laboratory at the University of Hawaii; 2010.1–34.
44. Massoud Amin S. Smart grid: overview, issues and opportunities. Advances and challenges in sensing, modeling, simulation, optimization and control. *Eur J Control*. 2011;17(5–6):547-567.
45. Yilin M, Hyun-Jin KT, Kenneth B, et al. Cyber–physical security of a smart grid infrastructure. *Proc IEEE*. 2011;100(1):195-209.
46. Ye Y, Yi Q, Hamid S, David T. A survey on cyber security for smart grid communications. *IEEE Commun Surveys & Tutorials*. 2012;14(4):998-1010.
47. Jairo G, Esha S, Cardenas Alvaro A, Michail M, Murat K. Security and privacy in cyber-physical systems: a survey of surveys. *IEEE Design & Test*. 2017;34(4):7-17.
48. Dagle J. Vulnerability assessment activities [for electric utilities]; 2001; 108-113.
49. Andrea T, Rolf E, Max M. Attack Scenario Modeling for Smart Grids Assessment Through Simulation. 2017; ACM; 13.
50. Joel C, Karsten B, Aubrey-Derrick S, Rainer B, Ahmet C, Sahin A. A Simulation Framework for Smart Meter Security Evaluation. 2011; IEEE; 1-9.
51. Çetinkaya Egemen K, Dan B, Amit D, Sripriya S, Sterbenz James PG. Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: a simulation-based approach. *Telecommun Syst*. 2013;52(2):751-766.
52. Paul M, Yu W, David G, Nada G. On Effectiveness of Smart Grid Applications Using Co-simulation. 2015; IEEE; 1-8.
53. Selim C, Jeff D, Jason F, Andrew F, Laurentiu M, Khushbu A. Proceedings of the Symposium on Theory of Modeling & Simulation (DEVS '14). *FNCS: A Framework for Power System and Communication Networks Co-Simulation*. DEVS Integrative San Diego, CA: Society for Computer Simulation International; 2014:1-8.
54. Abdullah AFM, Fereidoun A. A Model-Based Design of Cyber-Physical Energy Systems. 2014; IEEE; 97-104.
55. Pan K, André T, David LC, Peter P. Co-simulation for Cyber Security Analysis: Data Attacks Against Energy Management System. 2017; IEEE; 253-258.
56. Krishnan VVG, Zhang Y, Kaur K, Hahn A, Srivastava A, Sindhu S. Cyber-Security Analysis of Transactive Energy Systems; 2018; IEEE; 1-9.
57. Siddharth S, Manimaran G. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans Smart Grid*. 2014;5(2):580-591.
58. Hossain SMA, Hasan AM, Dipankar D, Abercrombie Robert K, Shubhalaxmi K. Co-simulation Platform for Characterizing Cyber Attacks in Cyber Physical Systems. 2015; IEEE; 1244-1251.
59. Lin H, Deng Y, Sandeep S, James T, Lamine M. Cyber Security Impacts on All-PMU State Estimator—A Case Study on Co-Simulation Platform GECO. 2012; IEEE; 587-592.
60. Gustavo WA, Cardoso BM, Germano SE, Alberto SF, Paschoal GL, Marinho B. ASTORIA: A Framework for Attack Simulation and Evaluation in Smart Grids; 2016; IEEE; 273-280.
61. Béla G, Christos S. Developing Cyber-physical Experimental Capabilities for the Security Analysis of the Future Smart Grid. 2011; IEEE; 1-7; IEEE.
62. Neetesh S, Victor C, Leilei X, Santiago G. CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid. 2017; ACM; 69-79.
63. Jens D, Koojana K, Anna F, Okko N, Sebastian L. OMNeT++ and Mosaik: enabling simulation of smart grid communications. *arXiv preprint arXiv:1509.03067*; 2015.
64. Hossain SMA, Hassan AM, Dipankar D, Abercrombie Robert K. OPNET/simulink Based Testbed for Disturbance Detection in the Smart Grid. 2015; ACM; 17.
65. Carlos Q, Abdun M, Zahir T. SCADASim – a framework for building SCADA simulations. *IEEE Trans Smart Grid*. 2011;2(4):589-597.
66. Stephan S, Rainer B, Joël C, Karsten B, Ahmet C, Sahin A. Application-level simulation for network security. *Simulation*. 2010;86(5–6):311-330.
67. Mike Z, Qiuhua H. InterPSS: A new generation power system simulation engine. *arXiv preprint arXiv:1711.10875*; 2017.
68. Sgouras Kallisthenis I, Birda Athina D, Labridis DP. Cyber Attack Impact on Critical Smart Grid Infrastructures. 2014; IEEE; 1-5.
69. Thomas G, Michael S. *Realistic Simulation Environments for IP-based Networks*. Brussels, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering; 2008:83.
70. Vignesh B, Rakesh K, Hai NH, Nicol David M, Kartik P, Elizabeth R. Melody: Synthesized Datasets for Evaluating Intrusion Detection Systems for the Smart Grid; 2017; IEEE; 1061-1072.
71. Brian W, Jay L, Leigh S, et al. An integrated experimental environment for distributed systems and networks. *ACM SIGOPS Operating Syst Rev*. 2002;36(SI:255-270.
72. Zhang Y, Eisele S, Dubey A, Laszka A, Srivastava AK. Cyber-physical Simulation Platform for Security Assessment of Transactive Energy Systems. 2019; 1-6.
73. Renke H, Rui F, Jeff D, Andrew F, Jason F. Open-source framework for power system transmission and distribution dynamics co-simulation. *IET Generation, Trans & Distrib*. 2017;11(12):3152-3162.
74. Amir-Hamed M-R, Alberto L-G. Distributed internet-based load altering attacks against smart power grids. *IEEE Trans Smart Grid*. 2011;2(4):667-674.
75. Ruben B, Roel DC, Juan VR, et al. Assessing electrical bottlenecks at feeder level for residential net zero-energy buildings by integrated system simulation. *Appl Energy*. 2012;96:74-83.
76. Zekeriya GM, Resul D. Cyber-security on smart grid: threats and potential solutions. *Computer Networks*. 2020;169:107094.

77. Nicol David M, Sanders William H, Trivedi KS. Model-based evaluation: from dependability to security. *IEEE Trans Depend Secure Comput*. 2004;1(1):48-65.
78. Adrian D, Johanna U, Weippl Edgar R. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: the Non-smart Power Grid Is Vulnerable to Cyber Attacks As Well. 2017; ACM; 303-314.

How to cite this article: Czekster RM, Morisset C, Clark JA, Soudjani S, Patsios C, Davison P. Systematic review of features for co-simulating security incidents in Cyber-Physical Systems. *Security and Privacy*. 2021;4:e150. https://doi.org/10.1002/spy2.150