Paper ID: 713 Session 2022
D2 PS2 - CYBERSECURITYTECHNIQUES, TECHNOLOGIES
AND APPLICATIONS FOR SECURING CRITICAL UTILITY ASSETS

Role of Digital Engineering and Digital Twin Technology in Cybersecurity of Electrical Grid

Djenana CAMPARA* **Andrea HRUSTEMOVIC** **Mr. Adnan AHMETHODZIC**
BH K CIGRE **JP Elektroprivreda BiH** **JP Elektroprivreda BiH**
djenana@kdmanalytics.com **Bosnia and Herzegovina**

Dr. Nikolai MANSOUROV **Dr. Meludin VELEDAR**
KDM Analytics **BH K CIGRE**
CANADA **Bosnia and Herzegovina**

SUMMARY

Global electric power systems are evolving from traditional, air-gapped control systems toward interconnected and interdependent conglomerates embracing Information Technology (IT)-enabled networks, systems, and infrastructure and Operational Technology (OT). As the result of IT/OT integration, OT components becomes exposed to the outside world that has a rather complex geopolitical and regulatory structure– with impacts on security of these systems and consequently requires more advanced ways to analyse and certify them. Attack surfaces have expanded due to the possibility of cyber threats coming from multiple new directions: direct attacks aimed at electric grid or indirect through other critical infrastructure including supply chain that could impact the operations or security of the grid. The opportunities to compromise, corrupt, and disable networks and systems have grown exponentially, resulting in new and highly automated malicious mechanisms. One of the greatest cyber threats to the grid have been intrusions causing corruption of industrial control system (ICS) through cross-border supply chains. Cyber intrusions on the electric grid have resulted in malware on ICS networks with the capability of causing damage, taking over certain aspects of system control or functionality, or total collapse of electric grid for a group of consumers or entire regions.

Due to these threats, cybersecurity of electric power systems cannot be an afterthought and requires a new approach that is based on cross-border/cross-region/cross-organization collaboration and information exchange. Security assessments cannot be about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits [4]. Rather, they should provide concrete evidence that the implementers and operators of such systems are meeting established security goals and objectives. In the next decade, the increasing demands for electricity as expected to grow exponentially. Utility organizations will need to develop

capabilities to meet these demands, making electrical power systems even more complex. Digitalization is the core enabler of power infrastructures, but the digital transformation itself comes with increased security threats that needs to be identified and addressed in a timely manner.

OT/IT integration suffers from lack of consistency across sectors, regions and countries since historically, the energy infrastructure has been structured around each regions/country's regulations and polices [4]. Currently, assessment and mitigation of the cyber risks of those systems are mostly disparate, but also highly subjective, relying on outdated manual techniques that are prone to causing inconsistency and lack of confidence in their outcome. There are efforts on multiple fronts to address this issue by introducing standards in the area of cyber risk assessment and mitigations. The trend is toward OT/IT security stack convergence standards such as NIST SP 800-37 (Risk Management Framework); NIST SP 800-53 (Security Controls), ISO 27001 (Security Management), ISO 27002 (Code of practice for information security controls). Recently, the Final Report was published by ENTSO-E/EU DSO informal drafting team on "Recommendations for the European Commission on a Network Code on cybersecurity" [1] with aim "to prepare the ground for a future Network Code on cybersecurity for the electricity sector" [1]. The team proposes the five strong recommendations for a Network Code on cybersecurity, number one being Cross border cyber risk assessment and management [1].

All these efforts are steps in the right direction; however, even the new guidelines/frameworks are still informal, facilitating the use of manual assessment techniques. If the assessment processes stay at that level, it will result in a false sense of security. Fortunately, these frameworks allow a more formal approach to particular elements of the framework, making cyber risk assessment process more systematic and objective [2,3].

In this paper we argue for "digital risk assessment" and propose a shift of emphasis in standards that can enable automation and consequently – risk assessment at industrial scale. First, we outline several challenges of manual assessment techniques. Then we outline the architecture of "digital risk assessment". Then we examine how Digital Engineering and Digital Twin Technology can be a natural fit into the proposed Cyber Risk Assessment and Management Framework enabling repeatable, industrial scale, evidence-based risk assessments. Lastly, we argue that the proposed digital risk assessment can be achieved even outside of modern digital twin technology, by outlining a lightweight bridge from existing/legacy systems into digital risk assessment.

KEYWORDS

Cybersecurity, Cyber Risk Assessment, Digital Engineering, Digital Twin, digital risk assessment

INTRODUCTION

Over many years the industry and the defense organizations have been developing in-house and 3rd party approaches to evaluate and measure security posture of systems. Although significant progress has been made in understanding and documenting "WHAT" needs to be evaluated together with expected results, the lack of efficient approaches that address the "HOW" component made these evaluation methods underutilized. In addition, most of energy organizations view cybersecurity as an IT cost and therefore are influenced by a key driver

"Fewer is Better": The fewer the security requirements to implement and evaluate, the faster and less costly will the experience be. [6] They are constantly making a trade-off between accepting the benefits of a system versus the mishap risk it presents. While achieving 100% security of all systems against all threats is not realistic economically, identifying and prioritizing all risks followed by calculating the residual risk and implementing appropriate security countermeasures to maintain order and control is absolute necessity. For example, while the trust side of the security equation has received a great deal of attention in the world of security, this growing reliance on Web and Internet Services raised security issues that cannot be mitigated by traditional authentication processes. Although it remains important to know whether to trust information, it is becoming imperative to verify that there is no threat-related activity associated with this information. This is not achievable with subjective and costly manual risk assessments. It is not a secret that current risk assessment practices involve heavy manual effort, are antiquated, and are unable to scale to the amount of software deployed. Let's explore some of key challenges and possible ways forward.

The Scalability Challenge

The main factor preventing scalability of risk assessment and certification practices is the use of human evaluators. The amount of evidence required to determine a system's conformance to certification can be overwhelming, resulting in superficial, incomplete, and/or unacceptably long evaluation cycles.

The consequences of using manual effort in risk assessment are significant: the cost of each assessment is high and dependent on the size of the system, the number of assessments conducted at any given point in time is limited, skills are hard to transfer, and lessons learned during one assessment are difficult to apply to other systems.

The risk assessment process focuses on understanding intricate attack options, connecting them to the vulnerabilities and mitigation controls, and prioritizing the resulting risks. Ideally, each risk is traceable to a collection of related attacks and failures of the system, and thus traceable to the system model. Current risk assessment practices fall short for several reasons:

1. They are informal, often consisting of an ad-hoc process that is managed from the ground up, without a formal methodology that identifies top-level system objectives and policies.
2. They are inconsistent, varying in methodology—and the interpretation of the methodology by stakeholders—from project to project.
3. They are unrepeatable. Because of lack of formality and interpretation challenges, each and every risk assessment is performed individually. This makes comprehensive risk assessment highly uneconomical.
4. They fail to establish systematic and formal traceability between the stated risks and the model of the system.

One of the greatest failings of current risk assessment practices is that they examine a system's components in isolation, leaving the system vulnerable to multi-stage cyberattacks. If risk assessment does not analyze the interdependencies of components of cyber and cyber-physical systems, it offers little value in securing critical infrastructure.

As manual techniques fail to scale and systematically address the systems and the systems they depend on, the outcomes of a risk assessment process are often uncertain often bringing a false

sense of security. In mission-critical applications, risk management that lacks diligence may bear significant legal and criminal implications as well.

The Continuity Challenge

Traditional risk assessment practices rely primarily on informal inputs, such as documentation and personnel interviews. This subjective practice is prone to inaccuracies and dependent upon well-trained, seasoned security professionals who are often hard to find and difficult to retain.

The gap related to reliance on manual effort for risk assessments becomes particularly obvious and painful in the context of Digital Engineering, more specifically Model-Based Systems Engineering (MBSE). While the trend in the engineering side is to use models and simulations, including full "digital twins" of systems, the cybersecurity side lags well behind where the digital models are inspected manually, and then laboriously (and unreliably) transformed into risk models, where belated automated risk calculation can be performed.

Manual risk assessment techniques are responsible for discontinuity between "digital twins" and digital engineering of energy systems on one side and risk assessment on other side.

Yet, the availability of system models as digital content offers a path towards an automated solution, which can (at least in theory) start with the model of the system, perform a systematic examination of the system, and construct viable attacks that are traceable to the description of the system, as well as to the formulated risk statements.

On the other hand, the automation solution requires a reasonably high-fidelity description of the system as the input. Thus, an automation solution, if successful, may address the scalability challenge by constructing a risk model directly from the system model, while at the same time addressing another challenge of human risk assessment: insufficient fidelity of the assessment.

When such an automated solution is "knowledge-based" (i.e. driven by easily configurable rules and templates), it may also address the challenge of ramping up risk assessment capability throughout an organization and managing skills and corporate learning, where lessons learned during one assessment are directly channeled into the next one.

In the environment where manual methods are used, such transfer is not straightforward and requires a sophisticated training system, while an industrial-scale environment based on automated tools requires mere editing of rules and templates.

The WHAT vs. HOW Challenge

A great deal of work has been done by industry to identify WHAT criteria need to be assessed and evaluated in a cyber system, and these measures are well documented. But, there is no efficient, repeatable, and economical practice and the corresponding technology to address HOW the assessment and analysis should be conducted. For these reasons, risk managers often lack the targeted information they need to quantify a system's exposure to cyber-attacks and to properly prioritize their risk management activities. Instead, they must interpret a system's vulnerability without acceptable due diligence.

This challenge is not specific to the energy sector. This is a reality in every industry and subsector and are experienced by every company that designs electronically enabled products and services that communicate in some form, regardless of size.

Current research into risk assessment is often done in isolation from systems engineering practices—the ways engineers build and simulate models. Additionally, the risk assessment community places significant emphasis to the statistical foundation with fairly simple and abstract models, but not enough attention to the details of a comprehensive and fully traceable risk model suitable for digital ecosystem.

On the cybersecurity side, the community is doing an excellent job of collecting and understanding the universe of detailed facts related to cyber-attacks and vulnerabilities. However, little attention is given to how such content can be systematically (and justifiably) applied to a given system to argue the case of cybersecurity risks. This is especially true of systems represented by a reasonably high-fidelity model, either in a standard or a proprietary format.

When a risk model is viewed as an independent design specification, it becomes possible to examine the laws by which it can be systematically constructed based on the system model, thus addressing the HOW challenge. Only then can it be assessed, including risk calculation, performing risk analytics, visualization, and so on.

Traceability of the risk model to the system model is the key concern driving the new research into industrial scale risk assessments.

DIGITAL RISK ASSESSMENT AT INDUSTRIAL SCALE

Industrial scale risk assessment and certification of systems involves transitioning away from subjective and labor–intensive human analysis techniques to structured automated analysis driven by machine-consumable rules based on open standards. The new framework for a truly "digital risk assessment" must involve open standards to separate the analysis capability (the engine) from the rules, so that rules can be contributed by the community for different domains, and different companies can supply engines independent on the rules. This separation of concerns between two inputs are essential since it involves contribution from separate fields of expertise: (1) System & operational architecture information in the form of the model vs (2) cybersecurity knowledge containing information related to sensitive assets, threats, undesired events, attacks & vulnerability patterns, security controls, etc. (Figure 1).

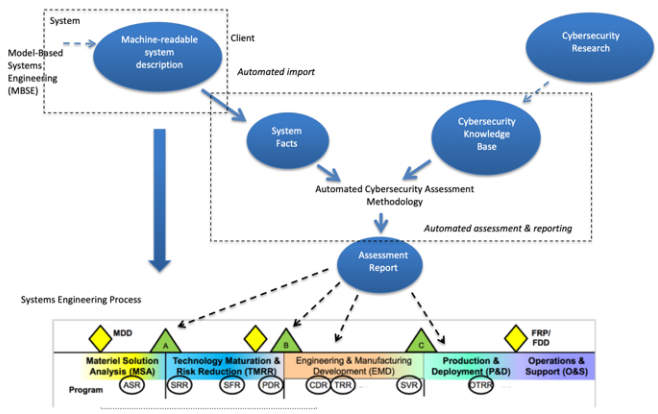

Figure 1 : Separation of concerns – System vs. Cybersecurity knowledge as inputs to automated risk assessment

This separation of concerns enables experts in each field to focus and contribute to the respective knowledge areas. This provides an opportunity for development of standards/specifications in support of a best-of-breed solutions related to cybersecurity for energy sector. The central part of the automated risk assessment is where the two inputs are integrated to enable risk analytics [7].

This next-generation digital risk assessment must be able to analyse the system under assessment to enumerate the places where the system can be attacked, and link possible attacks to system failures. Thus, automatically produced risk is an aggregation of similar attacks causing common failures, traceable to the elements of the system. The new levels of automation and confidence can be achieved through the plug-and-play analysis rules aligned with the upcoming risk assessment standards. The new framework must also use open standards to separate the analytics engine and the rules from the representation of the system under assessment. The new automated approach shifts the human effort away from risk assessment towards the development of a hi-fidelity model of the system under assessment.

Existing risk assessment methodologies quite successfully addresses "WHAT" component while the new framework is focused on addressing "HOW" component in automated fashion, therefore has to be rooted in technology and not descriptive guidance. This technological framework focuses on the use of discernible concepts, and a sequence of steps that maximizes assurance. This approach should be based on solid engineering practices where the elements of the architecture and the corresponding elements of risk are managed together. This can be achieved by combining a risk assessment methodology with the concepts of evidence-driven system assurance, such that risk assessment steps are guided by a built-in assurance case which answers the question "How do we know that all possible risks have been identified", thus maximizing the assurance confidence [6].

The goal of the digital risk assessment is to automatically assess the system and to recommend controls and countermeasures that can enhance its resilience to cyber threats and ensure operational success. One can modify the rules and other machine-consumable content guiding this process, but the execution is fully automated. The key step in the assessment is automated construction of an attack tree. The system's operational architecture is analyzed to determine the relative operational importance of hosts and applications. The system data is combined with rules describing attack techniques to compute all possible attack paths (given the rules and data such as attack targets, vectors, entry points and entry point sources) in the system. The potential attacks are chained together with aim to compute possible attack paths and stored in a tree data structure giving the pre-conditions and post-conditions for each attack step. Attack steps in the path depend on attack goals and attack methods chosen by attacker. One can view this approach as a fully automated Cyber FME(C)A - Failure Mode, Effects and Criticality Analysis.

Furthermore, the digital risk assessment [6] brings together evidence-driven assurance capabilities and automated risk assessment solution to provide justified confidence that the operational and system architecture views adequately represent the system and provide a solid basis for selecting optimal controls to remediate security issues. Our argument here is that automation alone without built-in assurance only gets you to a false sense of security faster.

A key artifact of digital risk assessment is a standardized risk model, so that automated risk assessment tools can populate a risk analytics repository with connected objects of the risk model and evidence to the risk claims. Here we use a widely accepted terminology where a "model" represents a certain language, and an "instance" of the model is, basically, a text

written in that language. Instead of a word “instance” we can say “data”, or even “repository”. So, “model” represents a schema, and repository is populated with the data that conforms to the schema. While the model is generic enough to cover an entire industry, the data in the repository corresponds to a single system under assessment. The model has the power to an entire ecosystem, including various tools (capabilities) and content (rules, instructions). Model-based development and how models bring life to ecosystems is a vast subject [6].

As mentioned above (Figure 1), data for risk analysis comes from two sources: (1) machine-consumable description of the system under assessment and (2) machine-consumable cybersecurity knowledge base composed of information. Machine-consumable description of the system under assessment is an artifact of Digital Engineering.

DIGITAL ENGINEERING AND DIGITAL TWINS

Digital Engineering

Some industries, like defense and automotive industry apply Model Based System Engineering (MBSE) during system development lifecycle. MBSE is an emerging discipline where a formal machine-readable model of the system is used as a means of communication between various participants of the systems life cycle where each group has a viewpoint into the common model [9]. In other words, the model is used to facilitate system requirements, design, analysis, verification, and validation activities, and can be applied in different stages of the process from the conceptual design phase throughout development and later life cycle phases. It can be applied to any System or System-of-Systems.

Some of a particular MBSE approaches are Unified Architecture Framework (UAF) and SysML. Both specifications are published by Object Management Group (OMG) International Standard Organization were the language architecture is in terms of UML profiling mechanism. UAF is aligned with ISO 42010 (Architecture Description), is flexible to support all domains and supports model of models by enabling development of integrated model layers.
The input UAF model needs to be able to tell “cause-and-effect” story for system under analysis in order to provide high confidence in the risk assessment outcome. To that end, “fit-for-purpose” analysis of the developed models/views need to be performed to determine level of confidence in the outcomes of risk assessment, e.g. Correctness, Completeness, Consistency, Causality and Correlation [8].

Digital Twins

Digital Twin refers to a machine-consumable model of physical assets, processes, and systems that can be used for various purposes [5]. Operators can visualize a digital twin and cross-examine it (also with virtual, augmented and immersive reality), execute queries, ask questions, compute and compare scenarios, monitor and predict the performance of the physical assets [5]. By transforming unstructured information into a smart model, plant and grid operators are empowered to visualize, build, and manage power systems, sub-stations and facilities of all complexities, ensuring safe and efficient operation throughout the entire life cycle. By using electric network digital twin, utilities can shape the operations and maintenance strategies of the future [5].

Digital Twin produces high level fidelity information for automated cyber risk analysis of the power system such as

- List all components involved in the system;
- Identify all entry points into system
- Identify dependencies and interfaces between components and their interaction with cross-boundary systems (systems that are outside internal network) I n operational environment
- Identify critical cross-boundary processes
- Identify sensitive assets and their dependencies to operational environment;
- Identify of key capabilities.

In the context of fully digital assessment and certification of the security of the power systems, the digital twin aligns well with the model-based automated risk assessment framework, Thus the use of the digital twin can be extended to understanding how the power system can be attacked and what the consequences of these attacks might be, feeding the information into an automated risk assessment framework.

What about existing systems?

Despite the apparent benefits of automated risk assessment, there is a significant barrier to its adoption – existing systems. From the perspective of one innovative technology (such as digital, engineering, digital twins), any system developed without the use of this technology is considered "legacy". At this point, detailed high-fidelity models of the control systems are few and far between as not many utility companies are using MBSE and even less of them use Digital Twins. For many existing systems even a high-level description in a machine-consumable format may be not readily available. However, we argue, that the standards community shifts attention towards digital risk assessment ecosystem built around a risk model. Capabilities for incorporating existing/legacy systems becomes yet another part of the mosaic that we call an ecosystem. For existing systems, the machine-consumable data to feed the digital risk assessment capability can be (1) reverse engineered automatically or semi-automatically by discovering the network elements, their connectivity, etc. by querying the actual system; or (2) reverse engineered manually, for example using a light-weight modelling approach involving simple table templates. In both cases, the reverse-engineered pseudo-model will be fed into an automated and repeatable risk assessment tool, so any adjustments can be made, and assessment repeated. Granted that a manual reverse engineering step does not fully eliminate the discontinuity between the system and the risk assessment, however in terms of cyber security capability of the organization this represents a tremendous improvement, because the risk assessment step becomes repeatable and objective, can be done multiple time, exploring different scenarios, and the model of the system can be maintained.
To lower the barrier to entry into repeatable and objective risk assessments using the automated capability, a light-weight approach to modelling control systems can be designed utilizing table templates providing the following information:

- the list of components (physical or logical devices) with the sub systems that are considered as being relevant to the context of the system ("inside" the boundary) or as being influential on the system ("outside" of the boundary),
- interfaces between components, specifically classified as internal vs. external information exchanges
- the data types with their security classifications (e.g. Classified/Unclassified, Secret, ..) and impacts (Confidentiality, Integrity and Availability)
- the data flows of the system under assessment describing system activities/scenarios
- system capabilities as they relate to defined activities

- Persons/operators involved with devices (this is to ensure that insider attacks are considered: e.g. malicious, clueless or carless operator)

These tables serve as machine readable model of system under assessment and are interpreted in the context of the selected knowledge base to build the model of the system under assessment.

There are Word document-based templates for describing systems, one of them is IEC 62559-2, Use case methodology with focus on defining requirements for the system. Although the IEC 62559-2 Use case Word document-based template consists of some key information needed for risk assessment, it has some gaps that needs to be addressed, possibly by extending this standard to accommodating input of additional system information.

Also, information captured in the template needs to reflect system throughout its lifecycle (become living document), ensuring that system information provided in the template accurately reflects system as implemented and not its assumptions.

CONCLUSION

Instigating a paradigm shift in an industry is not a trivial undertaking. Standards is a good place to start. One community understands this – the Object Management Group consortium develops standards as machine-consumable specifications. And such standards bring life to vibrant ecosystems. The original CORBA is one: many tools have been developed that support CORBA, and many developers are developing code using CORBA and the new tools. UML is another example. Many people are developing models in UML, and there are many tools – some competing, for example UML visual editors, and some complimentary, for example code generators that transform UML models, simulators, analysers, distributed repositories, etc. These ecosystems are possible because of an open standard in machine-consumable format.
In our book [6] we've described various ecosystems in the area of cybersecurity. These ecosystems involve another component – standard content. In the two examples of ecosystems-built-around-a-standard, there are two components: publicly available tools that support a standard, and (usually) proprietary code that uses the standard and the tools. In the area of cybersecurity an ecosystem, such as one built around National Institute of Standards and Technology's (NIST) Security Content Automation Protocol (SCAP), includes publicly available content in standard machine-consumable format, as well as publicly available or proprietary tools. For example, the content for SCAP includes the Common Vulnerabilities and Exposures (CVE) catalog.
In this paper we argue that the risk assessment and cybersecurity for the energy sector are in need of a paradigm shift in order to overcome the gaps caused by manual risk assessment techniques. In facts, many other industries face similar problems, and can benefit from the new technologies too. We outlined the new "digital risk assessment" approach, and what is needed to bring it to life: specification of the input describing the system under assessment, capability to automatically construct a risk tree for the system under assessment, capability to perform risk analytics, once the risk tree is available. We argued that it is beneficial to introduce a specification of the risk model to separate code and content. Thus, the digital risk assessment capability can be made data driven.
Success of the effort is largely determined by the choice of the input specification. In this paper we argued, that the input format must be aligned with the technologies that are already being adopted in the industry for "digital engineering", model-based systems engineering and for building digital twins. Thus, the paradigm shift of the digital engineering can happen

simultaneously with the one required for risk assessment. In fact, the two new technologies can support each other quite naturally.
Obviously, “digital risk assessment” can be implemented by a single company or by multiple companies. In fact, there are companies that already have products that implements digital risk assessment. Understanding that Digital Engineering and Digital Twin processes are currently not mainstream, the companies also support a lightweight modelling approach in the form of simple tables to accommodate existing systems [2, 3, 4].
However, we want to look at digital risk assessment as an ecosystem built around open standards in order to facilitate its wider adoption by the industry. We chart a path that would be able to take advantage of digital assessment at industrial scale. This path takes us through standardization of the following information:

1. Set of system information that would give us comprehensive and high-fidelity cause-and-effect story of system under assessment
2. The agreed upon machine readable format of representing such an information
3. Risk model

BIBLIOGRAPHY

[1] ENTSO-E/EUDSO Informal Drafting Team “Network Code on Cybersecurity-Final Report” [19 February 2021]

[2] Dr. N. Mansourov, D. Campara, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar, “Understanding and mitigating cyber risk in Smart Grid” [BH K CIGRE, Neum, Bosnia and Herzegovina, Oct. 2019]

[3] D. Campara, Dr. N. Mansourov, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar “Applying Automated Cyber Risk Assessment for the Smart Grid” [CIGRE Paris 2020]

[4] D. Campara, Dr. N. Mansourov, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar “Cooperation through Automation: Applying Automated Cyber Risk Assessment for the Smart Grid” [CIGRE South East European Regional Council, Conference 2020 in Vienna, Austria]

[5] Slavco Velickov, “Energy 4.0: Digital Twin for Electric Utilities, Grid Edge and Internet of Electricity” [Published on April 6, 2020]

[6] Dr. N. Mansourov, D. Campara, “System Assurance: Beyond Detecting Vulnerabilities” [Morgan Kaufmann Publishers, De. 2010]

[7] D. Campara, “Threat Modeling and Automated Risk Analysis” [Cybersecurity Workshop, Coronado, CA USA, Dec. 2016]

[8] Dr. N. Mansourov, “Automated Model-Based Risk Assessment”, MBSE Cyber Experience Symposium [Allen, TX, USA, May 2019]

[9] Joint INCOSE WG Project (Power&Energy/CIPR/OOSEM), “Applying MBSE to Develop a Microgrid Reference Model” [EnergyTech and Expo, Cleveland, OH USA, Nov. 2017]