A Framework for Wide-Area Monitoring and Control Systems Interoperability and Cybersecurity Analysis

M. Chenine, *Student Member, IEEE*, J. Ullberg, L. Nordström, *Senior Member, IEEE*, Y. Wu, and G. N. Ericsson, *Senior Member, IEEE*

***Abstract*—Wide-area monitoring and control (WAMC) systems are the next-generation operational-management systems for electric power systems. The main purpose of such systems is to provide high resolution real-time situational awareness in order to improve the operation of the power system by detecting and responding to fast evolving phenomenon in power systems. From an information and communication technology (ICT) perspective, the nonfunctional qualities of these systems are increasingly becoming important and there is a need to evaluate and analyze the factors that impact these nonfunctional qualities. Enterprise architecture methods, which capture properties of ICT systems in architecture models and use these models as a basis for analysis and decision making, are a promising approach to meet these challenges. This paper presents a quantitative architecture analysis method for the study of WAMC ICT architectures focusing primarily on the interoperability and cybersecurity aspects.**

***Index Terms*—Communication systems, cybersecurity, enterprise architecture analysis, interoperability, wide-area monitoring and control systems (WAMCS).**

I. Introduction

THERE is a clear interdependency between modern power systems and the underlying information and communication technology (ICT) infrastructure that supports its operation and management [1]–[3]. At the core, envisioned wide-area monitoring and control (WAMC) systems are power system applications, supported by a network of intermediary devices and systems that calculate, carry, sort, and store real-time measurements. There is generally, a quite understandable focus placed on improving the functionality of these applications and supporting systems, while the quality of the supporting ICT system is often expected to be sufficient. This sometimes leads to improper quality in the power system function as such due to poor understanding of ICT limitations, see, for instance, [4], which illustrates how different architectures can impact the communication performance (in terms of delay) and, as a result, the suitability a power system control function, such as oscillation damping using a static var compensator (SVC), can fail due to increasing communication delay.

Needless to say, the functional focus leads to suboptimal solutions when the entire ICT architecture is considered. Too large of a focus on the functions of ICT over their nonfunctional aspects leads to the stove-pipe system architectures [5]. Furthermore, such functional focus, without wider nonfunctional considerations, can create a false sense of confidence that one particular function's ICT system capabilities are sufficient for that of another function merely because they are similar in nature.

Nonfunctional quality of a system describes an attribute of the system in its operational environment, such as performance, cybersecurity, and reliability [6]. In addition, there is a clear interdependency between the nonfunctional aspects and the attributes of the ICT systems that comprise them [7]. In some cases, there is even negative coupling, for instance, between interoperability and security. A more complete analysis of ICT systems requires consideration of the fact that the nonfunctional aspects of ICT are interrelated.

A. Purpose

This paper presents an analysis framework, with a supporting modeling framework and tool support, that enables objective decision making on tradesoffs between cybersecurity and interoperability in engineering of the WAMC systems. The modeling and analysis framework presented is derived from validated frameworks for interoperability and cybersecurity analysis and specialized for WAMC system analysis of these qualities. The framework includes a metamodel that contains concepts or classes that can be used to model WAMC and related ICT components. The proposed analysis framework utilizes methods and techniques from the enterprise architecture (EA) discipline to model and analyze WAMC systems. The use of EA models, supported by a formal framework for analysis, is an approach to managing and optimizing such complex ICT systems and processes. EA analysis methods have been applied in many scenarios, more specifically focusing on nonfunctional qualities of power system ICT systems, for example, in substation automation systems reliability [8] and control system security [9].

B. Outline

The rest of this paper is structured as follows:; Section II presents a brief background on interoperability and cybersecurity in WAMC systems. Section III introduces the analysis

Manuscript received January 20, 2013; revised June 23, 2013; accepted August 08, 2013. Date of publication January 09, 2014; date of current version March 20, 2014. Paper no. TPWRD-00087-2013.

M. Chenine, J, Ullberg, L. Nordström, and Y. Wu are with the Department of Industrial Information and Control Systems, School of Electrical Engineering, KTH—Royal Institute of Technology, Stockholm 10044, Sweden (e-mail: Moustafac@ics.kth.se; johanu@ics.kth.se; larsn@ics.kth.se; yimingw@ics.kth.se).

G. N. Ericsson is with the Swedish National Grid (Svenska Kraftnät), Sundbyberg 17224, Sweden (e-mail: goran.n.ericsson@svk.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRD.2013.2279182

framework proposed in this paper. This section explains the model, the basis for the model, and the analysis method behind the model. An example of using the framework to perform architectural analysis is presented in Section IV. Finally this paper is concluded in Section V.

II. Interoperability and Cybersecurity in WAMC Systems

Interoperability and cybersecurity in WAMC systems share most of the concerns and efforts in the wider modern grid initiatives. While phasor measurement units (PMUs) were proposed in the late 1980s, the deployment of PMUs into wide-area monitoring (WAM) systems has recently begun to be realized. With the short life of WAM and WAMC systems, several protocols are already in deployment side by side, for example, IEEE 1344 [12], C37.118:2005 [13], C37.118:2011 [14], and IEC 61850-90-5 [15]. Furthermore, as WAM/WAMC systems are integrated with supervisory control and data acquistion (SCADA) and other distributed control systems as well as the integration of other measurement sources, the need and complexities of interoperability become apparent.

With interoperability, we understand the ease by which a system can exchange information with another system. As explained in [16], there are several layers of interoperability. For our discussion here, it suffices to say that the interoperability issues increase the larger distance between the measurement source and the application. The distance here is not only geographical, but also has a context or organizational dimension, meaning that if data transverses several networks within, or outside a systems operator, additional interoperability issues may be experienced due to protocol conversions or communication gateways and network configurations.

Cybersecurity is perhaps the most discussed of the nonfunctional aspects of ICT systems [17]–[20] and provides the best example of the dangers of focusing ICT development merely on the function to be fulfilled. No organization would consider employing an ICT system completely without protection against cyberattacks.

For WAMC systems, cybersecurity is a major concern. The WAMC system provides wide-area situational awareness in real time. If decisions were to be based on these real-time data, then they have to be highly dependable, considering the possible small response window. Therefore, attacks that can compromise the time source (major PMU deployments depend on global positioning system (GPS) pulses) or disrupt the network, causing major delays, or modification and tampering of data in real time, render WAMC systems' basic functionality useless. WAMC security has been discussed in several studies, where possible security threats and solutions have been proposed (e.g., in [21] and [22]).

III. Modeling and Analysis Framework

The framework proposed in this paper aims at modeling WAMC systems from a multi nonfunctional quality perspective. This will allow the user to make informed decisions, such as what aspects of the system could be optimized in terms of interoperability or improved to increase the overall security of the system. Specifically, the meta-model aims at capturing interoperability and cybersecurity aspects of WAMC systems. Using this model allows the analysis of several WAMC system architecture scenarios. The framework of the WAMC analysis meta model (WAMM) is composed of two parts.

TABLE I
OCL versus P2AMF Attribute Value Initialization

OCL
`context WAMC_Component:hasFirewall:Boolean init=true`
P^2AMF
`context WAMC_Component:hasFirewall:Boolean init=Bernoulli(0.75)`

The first part of the WAMM is a meta model that captures the basic concepts and relationships between these concepts that would be needed to describe a WAMC system. This meta model is defined in the unified modeling language (UML) [25], a formal language used to describe software and systems design and architecture. The visual model facilitates diagrammatic description, specification, and documentation of WAMC deployments. The second part of the WAMM is an analysis framework that uses the instance models created using the meta model to perform quantitative analysis. The rest of this section explains these two components of the WAMM.

A. WAMC Analysis Framework Method

The WAMM is associated with a quantitative analysis framework based on a Monte-Carlo sampling approach. The analysis framework used to build the WAMM is the probabilistic, predictive architecture modeling framework ($\mathrm{P^2AMF}$) [25]. $\mathrm{P^2AMF}$ is, in turn, built on the object constraint language (OCL) [27]. $\mathrm{P^2AMF}$ like OCL allows invariants conditions to be expressed on models as well as the ability to perform numeric and set calculations directly or as a result of queries performed on the model. On the other hand, unlike OCL, $\mathrm{P^2AMF}$ allows attributes of a model to be specified as random variables. The modeler, therefore, can specify the value of, for example, the attribute hasFirewall (of a WAMC Component class), not as true or false, but rather as a probability distribution [e.g., Bernoulli (0.75)]. The excerpts listed in Table I summarize this difference.

Once probabilistic values are associated with attributes of the model, the $\mathrm{P^2AMF}$ performs a Monte Carlo sampling on the model [28]. Each attribute in the model is assigned random values from the associated probability distribution and calculated. Fig. 1 illustrates the relationship between the WAMM, an instance model of WAMM, and the calculation framework.

B. WAMC Analysis Framework Model

The model used to capture concepts that describe the WAMC system ICT components is presented in Fig. 2. In the WAMC architecture evaluation process, this would be the architecture meta model as depicted in Fig. 1.

The WAMM presented in Fig. 2 contains basic classes that are meant to model real-world systems, entities, and concepts. There are four main classes in the model that can represent the basic structure of the WAMC system. These are: `WAMC Component`, `Dataflow`, `Network Zone`, and `Network Interface`. Using these basic classes, it is possible to

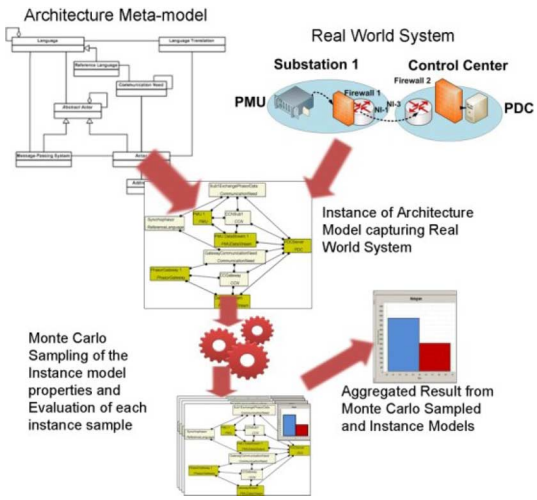

Fig. 1. Showing the process for WAMC system evaluation.

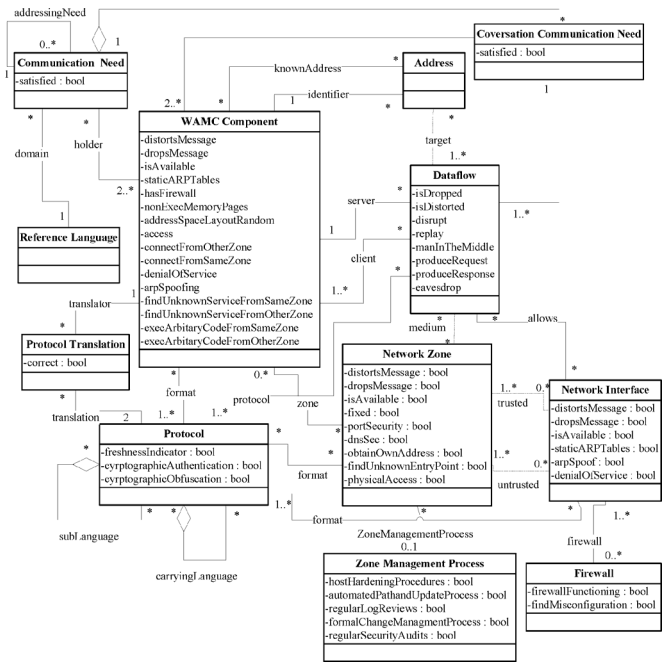

Fig. 2. WAMC analysis model.

establish where a WAMC component is located (i.e., network zone) by associating it with a `Network Zone` class, and what the role of the `WAMC Component` is, (i.e., a client or a server to a data flow) by associating it with o a `Dataflow` class.

A `WAMC Component` class is a general class that can be used to represent various types of components and systems that can be associated with WAMC components; for example, a `WAMC Component` can be further specialized to represent a `PMU`, or a `PDC`. Fig. 3 illustrates some specializations of the WAMC Component class that are relevant to WAMC systems. These specializations are a mapping of concepts outlined in [24].

This is also the case for other classes in the model. For example, `Dataflow` can be further specified to represent more concrete representation, that is, `PMU Dataflow` that represents a flow of measurements from a `PMU` versus a `PDC`

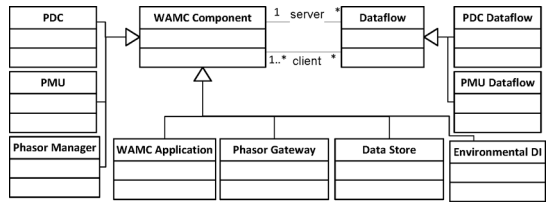

Fig. 3. Specializations of the WAMC component and data-flow classes.

`Dataflow`, which represents a concentrated flow of measurements from a phasor data concentrator (PDC). The attributes of the classes represent aspects or properties of the system which are of importance in performing interoperability or cybersecurity analysis. For example, the attribute *dropsMessage*, belonging to the WAMC Component, represents the possibility of a WAMC Component to drop or discard the data (e.g., due to a faulty setup or configuration like an improper time source). All attributes in the model can have a Boolean value, true or false, or a value for a Bernoulli distribution.

The architecture meta model illustrated in Fig. 2 is a specialization of concepts in a more general-purpose interoperability framework and extended with aspects of a language for cybersecurity modeling and predictions. By specializing the general-purpose interoperability model in the capabilities of interoperability, modeling and analysis are inherited. Specific concepts, such as Actors, Message-Passing System, Language and Language Translation, have been specialized into the central classes of the WAMM, that is, `WAMC Component` (and `Network Interface`), `Network Zone`, `Protocol` and `Protocol Translation`, respectively [10]. Cybersecurity concepts from [11] are mapped and merged to concepts in WAMM and related attacks and countermeasures are inherited.

1) Interoperability Dimension: The interoperability dimension in WAMM is based on a widely adopted definition of interoperability as the ability of two or more actors to exchange information and to use that information [29]. This is reflected in more depth from a structural and conversational viewpoint. From these viewpoints, the actors being `WAMC Components` have structural interoperability aspects (i.e., whether they are linked through a series of `Network Zones` and `Network Interfaces`), or if they share a common communication `Protocol`, etc. The structural aspects are the basis for interoperability while the more dynamic or conversational aspects deal with the realization of interoperability on specific `Dataflows`. While structurally `WAMC Components` can be interoperable, there are other practical factors that can hinder this, for example, improper `Protocol Translation`, faulty `WAMC Components`, or congested `Network Zones`, which can lead to `Dataflows` being corrupted or dropped altogether.

a) Structural Interoperability Aspects: `WAMC Components` that need to communicate with each other, in order to share and exchange information, can be said to have a `Communication Need`. The purpose of interoperability analysis, in the context of the WAMM framework, is to ensure that this communication need between `WAMC Components` is *satisfied*. To satisfy a `Communication Need`, one of the

requirements for any two WAMC Components (for example, a PMU and PDC, as shown in Fig. 3) is a clear communication path between them; this path can be modeled as a Network Zone or a series of Network Zones connected by Network Interfaces that delimit and separate them.

Network Interfaces allow the separation of the WAMC component associated network zone, so that similar concepts in the power system automation layout can also be captured. A Network Zone, for example, can be the substation zone, the utility wide-area network zone, or the control center zone. Any two WAMC Components also need to know each other's Address, and exchange of information has to be in language or Protocol that is common between them. Finally, a special type of language must be shared by the WAMC Component which is more than just related to format and rules of communication. This language, a Reference Language, determines the context of communication, that is, the content of the messages being exchanged by the actors relates to concepts in the electrical power system, such as voltages, currents, and phasors.

b) Conversational Aspects: The WAMM also captures conversational aspects of interoperability. In the conversational aspects, the data/information exchange between WAMC Components and how they transverse the Network Zones or the chain of Network Zones and Network Interfaces is achieved by the Dataflow and Conversation Communication Need.

The Conversation Communication Need enables modeling complex data flows or data exchanges between WAMC Components by associating one or more Dataflow instances with it. This, for example, can be compared to a series of data flows involved in initiating subscription to measurements between a WAMC application and a PDC, where the WAMC application sends a message to initiate communication and receives a configuration data frame from the PDC containing information about the concentrated measurements that the PDC will publish.

The WAMM also inherits from the model in [10] the ability to model more detailed conversational aspects, such as the detailed constructs that make up Dataflows and Protocols. While these are not included in the core WAMM, as illustrated in Fig. 2, they can be used for more detailed interoperability analysis.

c) Interoperability Dimension-Related Attributes: Using these classes to model a system provides insight into the structure and conversational aspects of the system, that is, whether a communication path is available and if the communication is carried out using common protocols, etc. Other aspects related to the structure also determine whether the communication need is satisfied. These aspects are captured in the attributes of the classes. Table II lists attributes relevant for interoperability analysis. The attributes associated with the Dataflow, Communication Need, and Conversation Communication Need classes are derived from the values of other attributes and from the structure of the resulting model.

The other attributes listed which cannot be derived from the structure and relationships in the model, are usually set by the modeler during the modeling process. These attributes provide further information on the characteristics of the system or data flow being modeled, for example, if the communication system, that is, the Network Zone, distorts the message due to errors in the system or drops the message due to high traffic in the network.

TABLE II
ATTRIBUTES OF THE WAMM RELATED TO INTEROPERABILITY

Attribute	Class(es)	Derived
distortsMessage	WAMC Component, Network Zone and Network Interface	No
dropsMessage		No
isAvailable		No
isDropped	Dataflow	Yes
isDistorted	Dataflow	Yes
satisfied	Communication Need	Yes
statisfied	Conversation Communication Need	Yes

The evaluation of the model in terms of interoperability is aggregated on the satisfied attribute of the each Communication Need class instance. The P^2AMF analysis engine (see Section III-A) analyzes the structure of the model, and the attributes in the model to derive if the communication need is satisfied or not, and the fulfillment of the communication need signifies the interoperability of the model.

2) Cybersecurity Dimension: The cybersecurity dimension of the WAMM is centered on the security of data flow in such systems. WAMC systems are based on real-time information which is processed instantly at the end systems. Disruption of real-time information from remote devices renders this basic functionality ineffective. Disruption could be easily detected, but the modification and tampered data are hard to detect.

As mentioned earlier, this dimension of the WAMM draws from the work in [11], [24], and [31] to define the semantic and structural requirements needed to model cybersecurity-related aspects. The attacks and countermeasures are represented as attributes associated with classes in the model. An attack's success or failure is dependent on the success or failure of a series of attacks that belong to certain classes or from attacks belonging to other related classes. Countermeasures, in turn, help decrease an attack. As with the interoperability dimension of the WAMM, the structure of the model also plays an important role in the security evaluation. The structure provides insight into the configuration of the WAMC architecture and, therefore, can influence the possibility of an attack taking place. For example, if a certain trusted network zone is connected to another network zone, which is considered untrusted, then the risk on the trusted zone is high. The security in an untrusted zone may be suboptimal or may be more prone to attacks.

Referring to Fig. 2, the main classes that are used in the security evaluation are the Network Zone, Zone Management Process, Network Interface, Firewall, WAMC Component, and Dataflow. These classes have attacks and/or countermeasures associated with them. As mentioned earlier, the WAMM places special focus on the data flow, and Table III lists the attacks possible on the Dataflow class. These attacks represent attacks on the Confidentiality, Integrity and Availability (CIA) of the Dataflows. The list of other possible attacks (A) and countermeasures (C) in the WAMM are listed in Table IV.

TABLE III
GENERIC ATTACKS AND THE IMPACT OF THE CIA ON WAMC DATA FLOWS

Attribute	Attack goal
disrupt	Disrupting a data stream
replay	Hijacking the data stream to replay same values
manInTheMiddle	Intercepting a data stream in which it is possible to modify the content
produceRequest	Involves initiating communication as if legitimate client
produceResponse	Imitating legitimate server
Eavesdrop	Listen in to the stream with no modification

TABLE IV
ATTACKS (A) AND COUNTERMEASURES IN THE WAMM (EXCLUDING THE DATA-FLOW CLASS)

Attribute	Class	Derived	Type
access	WAMC Component	Yes	A
connectFromOtherZone		Yes	A
connectFromSameZone		Yes	A
findUnknowServiceFromOther		Yes	A
findUnknowServiceFromSame		Yes	A
execArbitaryCodeSame		Yes	A
execArbitaryCodeOther		Yes	A
findHighSeverityExploit		No	A
execSpaceProtection		No	C
hasfirewall		No	C
addressSpaceLayoutRandom		No	C
denialOfService	WAMC Component, Network Interface	Yes	A
arpSpoofing		Yes	A
staticARPTables		Yes	C
portSecurity	Network Zone	No	C
dnsSec		No	C
physicalAccess		No	A
obtainOwnAddress		Yes	A
FindUnknownEntryPoint		Yes	A
hostHardeningProcedures	Zone Management Process	No	C
automatedPatchandUpdateProcess		No	C
regularLogReviews		No	C
formalChangeManagementProcess		No	C
regularSecurityAudits		No	C
freshnessIndicator	Protocol	No	C
cryptographicAuthentication		No	C
cryptographicObfuscation		No	C
firewallFunctioning	Firewall	No	C
findMisconfiguration		No	A

The attacks and countermeasures in Table IV contribute to the realization of the attacks in the `Dataflow` class. In fact, the security in the WAMM is evaluated on the data-flow class much like the interoperability is evaluated on the `Communication Need` class. A full explanation of the attacks listed in Tables III and IV and their dependency is explained in detail in [31].

a) Network Zone, Zone Management, and Network Interfaces: The attacks and countermeasures in the `Network Zone` class are intended to capture the probability that a malicious agent can get access to the network zone by obtaining an address local to that network zone or one which would allow access to the network zone. These are modeled by the *findUnknownEntryPoint* and *obtainOwnAddress* attributes, respectively. Countermeasures that can help avoid this are port security and domain name service (DNS) security procedures. These are modeled by the *portSecurity* and *dnsSec* attributes, respectively. The `Network Zone` is also associated with the `Zone Management Process` class, models an organization security process related to auditing, log reviews, and formal change-management procedures captured by *regularSecurityAudits*, *regularLogReviews*, and *formalChangeManagementProcess*, respectively. These can be considered as countermeasures which decrease the possibility of attackers succeeding in compromising or penetrating a secure network.

`Network Zones` are linked together through `Network Interfaces`, and these should be viewed as the primary transit points between networks. `Network Interfaces` also have a set of attacks which a malicious agent can perform to disrupt the network or to gain further access. These namely address resolution protocol (ARP) spoofing attacks (*arpSpoofing*) in order to redirect traffic or inject traffic or denial-of-service (denialOfService) attacks to disrupt traffic. Several countermeasures can exist on network interfaces, and the WAMM takes into account countermeasures against *arpSpoofing* attacks and, namely, whether a network interface has static ARP tables (*staticARPTables*) and/or is aasssociated with a firewall represented by an association with the `Firewall` class.

b) WAMC Component: The `Network Zone` and `Network Interface` attacks are also associated with the `WAMC Component` attacks. The WAMC components" attacks and countermeasures focus on modeling the possibility of an attacker gaining access to the end system. This is represented by the *access* attack attribute and is dependent on a series of attacks which the malicious agent needs to accomplish first. These are finding unknown services from the same zone or from another zone (*findUnkownServiceSame* and *findUnknowServiceOther*). These services are unknown to the administrators (therefore, they could contain exploits). The *connectFromOtherZone* and *connectFromSameZone* represent attacks that the attacker may also try, where the goal is to connect to the `WAMC Component` as a combination of attacks on the `Network Interface` and `Network Zone` to bypass the firewall or obtain a local network address. If the aforementioned attacks are successful several other attacks can be attempted such as denial of service (*denialOfService*) and ultimately system *access*.

c) Data Flow and Protocol: In all cases, the eventual result of a series of successful attacks could be a breach in data confidentiality where the attacker can *eavesdrop* on `Dataflows` in the system or more serious on the integrity of the data where the attack can act as a man in the middle (*manInTheMiddle*) modifying the data flow, *replaying*, or sending and receiving unauthorized request or replies (*produceRequest* and *produceResponse*, respectively). Finally the most serious consequence of the series of attacks is the disruption (*disrupt*) of the data flows, making the system inoperable.

The `Protocol` class is associated with the `Dataflow` and enables modeling of countermeasures inherent in typical protocols, such as cryptographic obfuscation and authentication (*cryptographicObfuscation* and *cryptographcAuthentication*).

d) Impact of Cybersecurity Attacks on Interoperability Attributes: The `Dataflow` also contains derived attributes related to interoperability, namely, *isDropped and isDistorted.* These two attributes from the interoperability dimension depend on whether the `WAMC Component, Network Zone`, or `Network Interface` distort or drop the data that they

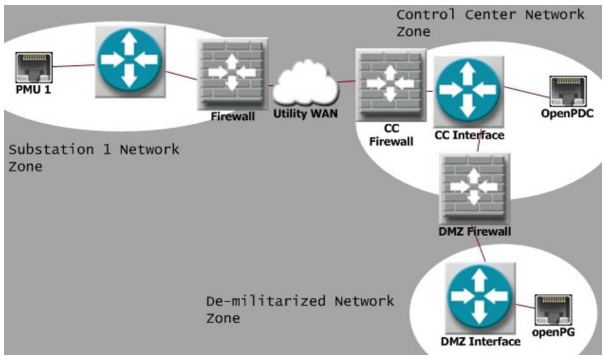

Fig. 4. Instance model concept diagram.

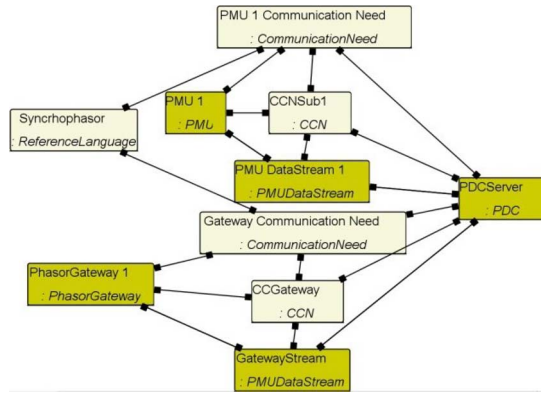

Fig. 5. WAMC components and their associated data flows and communication needs.

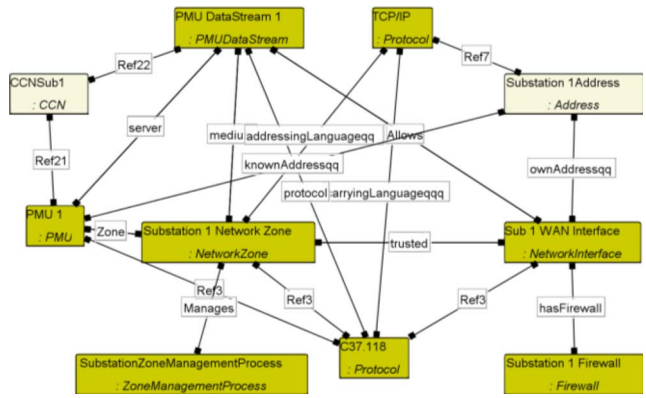

Fig. 6. Substation 1 modeled according to the WAMM classes.

send, receive, or pass on through them (represented by the nonderived attributes *distortsMessage* and *dropsMessage*). The *isDropped* and *isDistorted* are also impacted by the security attacks on the `Dataflow` class, specifically *disrupt* impacts *isDropped* (i.e., when *disrupt* is true, *isDropped* is true). Finally, if *replay* or *manInTheMiddle* is true, then isDistorted is also true.

IV. Application of the Analysis Framework

This section provides an example on the application of the WAMM. The case study is illustrated in Fig. 4.

The figure shows a PDC located at a control center, connected to a PMU 1 located at substation 1 and a phasor gateway located in a demilitarized zone. PMU 1 streams phasor data over the IP protocol using C37.118 [13]. The gateway receives PMU measurements from other grid operators and forwards these measurements to the PDC using the gateway exchange protocol (GEP) [35]. Substation 1 is connected to the utilities private wide-area network, while the de-militarized zone is connected directly to the control center.

This case study was based on a laboratory setup, in which real-world components are connected with emulated/real-time simulation systems. The demonstration platform included: openPDC and openPG [36], which are used for the PDC and phasor gateway, and softPMU [37] to represent a PMU. Finally, these are connected together using the OPNET modeler with a system-in-the-loop (SITL) module [38] to provide realistic emulation of various network zones.

The modeling of the case study example illustrated in Fig. 4 is performed using the enterprise architecture analysis tool (EAAT) [30], [33], where the WAMM depicted in Fig. 2 and the specializations illustrated in Fig. 3 are implemented. EAAT also supports several sampling techniques. In this example, forward sampling is used [34]. In the remainder of this section, figures illustrating the case study are screenshots from EAAT.

From the example, three main `WAMC Components` can be instantiated. These are *`PMU 1`*, *`Phasor Gateway`*, and the *`PDC Server`*. *`PMU 1`* and the *`Phasor Gateway`* are each associated with a data flow destined to the *`PDC Server`*. These two components also share a *`Communication Need`*, each with the *`PDC Server`*. This setup is illustrated in Fig. 5. Note that the attributes are not shown in the instance figures, but these can be seen in Fig. 2.

Fig. 6 illustrates the classes and relations used to describe components and relations in Substation 1. Substation 1 consists of *`PMU 1`* that is a sending out a data flow, *`PMU Data Stream 1`* over a substation network (*`Substation 1 Network Zone`*) to the *`PDC Server`* located at the control center. *`PMU 1`* sends out *`PMU Data Stream 1`* in the *`C37.118`* protocol. The *`Substation 1 Network Zone`* is a *`TCP/IP`* network that can support *`C37.118`* (thus, the association with these protocol instances) and is separated from the rest of the utility network through the *`Sub 1 WAN interface`*. This network interface also has a Firewall (*`Substation 1 Firewall`*) associated with it that protects the substation network from unauthorized access or data streams.

The *`PMU Data Stream 1`* has to transverse the *`Sub-station 1 Network Zone`* into the *`utility WAN`* network zone. This can be captured by the relation that is allowed between the *`PMU Data Stream 1`* and *`Sub 1 WAN Interface`*. This relation has to exist between all *`Network Interfaces`* instances until the destination network zone. Finally, *Substation 1 Network Zone* is associated with a *`Zone Management Process`*, which represents auditing and management procedures that the utility may implement for that substation.

Substation 1 is also connected to the *`Utility WAN`* network zone through the *`Sub 1 WAN Interface`*, where the relation between the *`Substation 1 Network Zone`* and the *`Sub 1 WAN Interface`* is *trusted*. This is because the

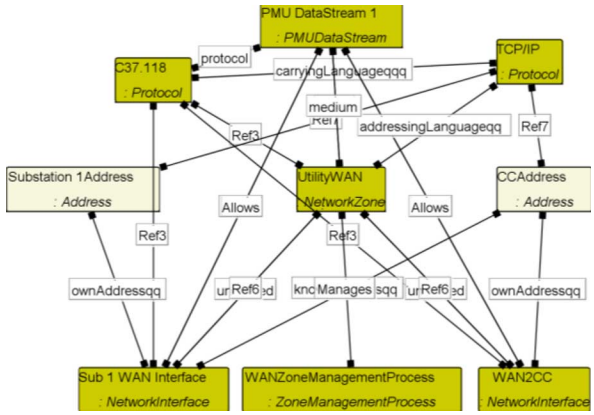

Fig. 7. WAMM instances describing the private WAN.

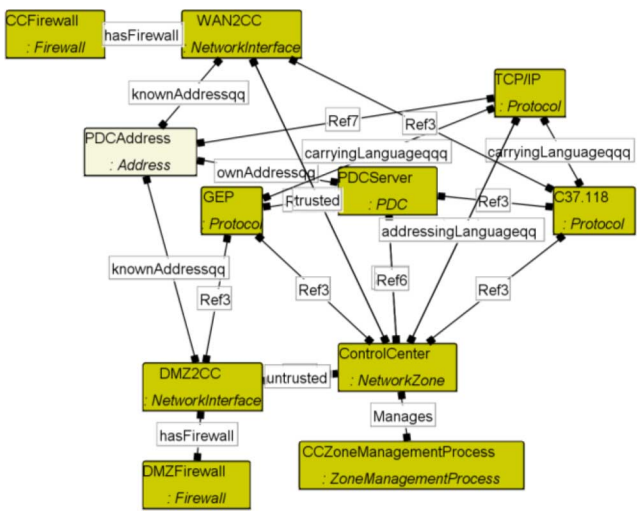

Fig. 8. WAMM classes for the control center.

Utility WAN is a trusted network zone since it represents a private and control wide-area utility network. The utility WAN network and control center models are illustrated in Figs. 7 and 8, respectively. The figures shows the components needed to model these two network zones, including zone-management processes, protocols, data flows, and network interfaces. Notice that since `PMU Data Stream 1` transverses the wide-area network, it shares relations with instances in that model to indicate, for example, which instance is the carrying medium and whether network interfaces along the path allow the PMU data stream to be passed on.

Modeling the de-militarized zone (DMZ) with the *Phasor Gateway* depicted in Fig. 4 is essentially the same as Substation 1 and, therefore, is not shown here. The difference is that the gateway-exchange protocol (*GEP*) is modeled, instead of C37.118. The demilitarized network zone also has its own `Zone Management Process` instance and, finally, the relation between the demilitarized `Network Zone` and the `Network Interface` to the control center network zone is "untrusted."

Next, the attributes of the model that are not derived have to be set; the value for these attributes can be obtained by examining the system under study. Table V lists the values of these attributes for the relevant instances.

TABLE V
VALUES FOR NONDERIVED ATTRIBUTES

	Substation 1		WAN	DMZ	Control Center
	Initial	Adjusted			
Network Zone					
physicalAccess	0.3	0.3	0.15	0	0
portSecurity	0.7	1	0.7	1	1
dnsSec	0.9	1	0.9	1	1
Network Interface					
staticARPTables	0.9	1	0.9	0.9	
Firewall					
functioning	0.75	0.9		1	1
findMisconfiguration	0.2	0.2		0.05	0.05
WAMC Component (PMU, PDC and Gateway)					
hostFirwall	0	0		1	1
findHighSeverityExploit	0.1	0.1		0.4	0.4
Zone Management Process					
hostHardeningprocedures	0.85	0.85	0.9	1	1
regularLogreviews	0.5	0.5	0.5	1	1
regularSecurityAudits	0.6	0.6	0.9	1	1

In this case study, it is assumed that the organization using the modeling framework is confident about the configurations in the control center and the DMZ and has a good idea about the configurations in the WAN and substation 1. This is reflected in the values of the attributes in Table V, (the "Initial" column in the case of substation 1) where the organization is certain, for example, that the firewall is functioning on the network interfaces between the DMZ and control center and between the control center and the WAN, but not entirely confident about the substation 1 firewall.

Another assumption here is that since the PDC and Gateway are built on open-source technology, this implies that the source code is available for scrutiny which, in turn, increases the possibility of an attacker discovering an exploit, this is reflected by the high value assigned to find high severity exploited in Table V. For all other attributes of the PDC and Gateway, the modeler is confident that they are positive, that is, the host firewall is turned on and functioning, static ARP tables is implemented, etc. On the other hand, the PMU 1 system is a closed system. Not so much is known on the internals of the systems; therefore, all other attributes are false, except for find high-severity exploits shown in Table V.

One set of attributes not shown in Table V is that related to the protocol used for sending synchrophasor data. For these, the values are as follows: C37.118 has a freshness indicator, but does not support any form of security so cryptographic authentication and obfuscation are false, while the GEP has a freshness indicator and supports cryptographic authentication.

Finally, the model can be evaluated; the EAAT samples the model and for each sample, the derived attributes in the model are calculated. Table VI lists the results for the disrupt attribute on the data-flow instances (i.e., `PMU Data Stream 1` and `Gateway Stream`) and the related interoperability attributes for each data flow. Due to space limitations, only these attributes will be shown and discussed. The results shown in the "initial" column of Table VI provide insight into the risks involved in the simple setup. The results show the probability that the `PMU Data stream 1`, which is on a private network, would be disrupted. Since the network and system properties are 0.12,

TABLE VI
RESULTS SHOWING EVALUATION FOR TWO SECURITY AND TWO INTEROPERABILITY ATTRIBUTES

Dataflow	Derived Attributes	Initial	Adjusted
PMU 1	Disrupt	0.123	0.036
	Man In The Middle	0.006	0.006
	Communication Need	1	1
	Conversation Communication Need	0.877	0.095
Gateway	Disrupt	0.004	
	Communication Need	1	
	Conversation Communication Need	0.997	

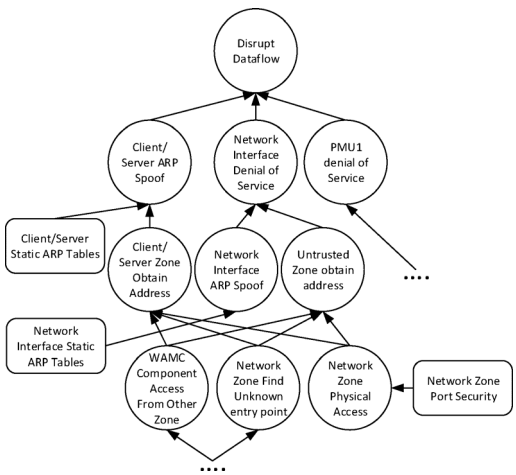

Fig. 9. Example showing partial tree of attacks and countermeasures leading to data-flow disruption.

this is actually quite risky considering this is a system where the requirement to analyze data and act upon these data in real time is a basic functionality.

The probability that an attacker can gain physical access to the substation or at some access point in the WAN network increases the chance of the attacker obtaining an address on the network, by finding an unknown entry point. Obtaining an address can lead to an entire series of attacks, such as DNS and ARP spoofs, denial of services on network interfaces, and access to WAMC components. If these attacks are successful, then the attacker can execute attacks on the PMU or gateway data flows, such as *Disrupt*, *man-InTheMiddle*, *Eavesdrop*, etc. A countermeasure or a combination of countermeasures can make an attack highly improbable or lower the possibility of the attack being successful; for example, ARP spoofs can be limited by implementing static ARP tables, and likewise port security can limit an attacker by finding an unknown entry point. Fig. 9 illustrates a partial attack (circle) and countermeasure (rounded corners rectangle) tree for the `PMU Data Stream 1`.

In terms of interoperability, Table VI shows that the Communication Need is *satisfied* for both data flows in the case study. This is because the `Communication Need` is evaluated based on static properties of the model, that is, whether the `WAMC Components` share the same reference language and protocols, and whether a communication path exists between actors. On the other hand, due to the security or specifically the probability of the data flow being disrupted or distorted, the `Conversation Communication Need` is impacted. This is because the *disrupt* attack and the *manInTheMiddle* attacks impact the *isDropped* and *isDistorted* properties of the data flow, respectively.

To illustrate how the countermeasures can improve security (and, in turn, the conversational aspects of interoperability), the organization decides to address issues of substation 1 by improving the countermeasures on the network zone and network interface, as well as increasing the reliability of the firewall. These changes can be seen in the "adjusted" column in Table V and the corresponding results in the "adjusted" column in Table VI. The probability of the data flow being disrupted sharply decreases to 0.036 while the probability of *manInTheMiddle* attack remains the same. As a result of this decrease in disruption, the probability of the *CCNSub1* (the conversation communication need between PMU 1 and the PDC) being *satisfied* proportionally increases.

V. DISCUSSION AND CONCLUSION

The real-time nature of the WAMC system makes it susceptible for variations in nonfunctional quality. While performance is an important fundamental requirement, other qualities are just as important. This paper demonstrates how cybersecurity aspects can adversely impact WAMC systems by disrupting data flows. This is quite critical, especially when control and protection functions are taken into consideration where it can be assumed that such functions are designed for fast action. Security incursions and the resulting impact on interoperability can have a devastating outcome.

While the initiatives that describe possible failure points, security measures, and interoperability architecture guidelines, such as those described in [16], [17], and [24], are extremely important and useful, there is still a need to quantitatively evaluate how well such guidelines have been implemented or addressed in actual deployment scenarios. The contribution of this paper is a modeling and analysis framework to meet this need. The framework aids decisions makers and architects on analyzing current deployments and on how to best build or integrate WAMC systems into existing operational systems, taking into account interoperability and cybersecurity aspects.

Future work will include an extension of security aspects to include other concerns which are not specific to network architecture, such as general security practices as authentication and more specialized attacks on WAMC component services. In parallel, the model will be applied to real-world scenarios, at a transmission system operator, to further validate the model.

REFERENCES

[1] J. W. Bialek, "Critical interrelations between ICT and electricity system," in *Securing Electricity Supply in the Cyber Age*, Z. Lukszo and M. Weijnen, Eds. New York: Springer, 2010.
[2] N. Hadjsaid, M. Viziteu, B. Rozel, R. Caire, J. Sabonnadiere, D. Georges, and C. Tranchita, "Interdependencies of coupled heterogenrous infrastructures: The case of ICT and energy," presented at the 3rd Int. Disaster Risk Conf., Davos, Switzerland, 2010.
[3] C. Tranchita, N. Hadjsaid, M. Viziteu, B. Rozel, and R. Caire, "ICT and Power Systems: An Integrated Approach," in *Securing Electricity Supply in the Cyber Age*, Z. Lukszo and M. Weijnen, Eds. New York: Springer, 2010.
[4] K. Zhu, M. Chenine, and L. Nordström, "ICT architecture impact on wide area monitoring and control systems' reliability," *IEEE Trans. Power Del.*, vol. 26, no. 4, pp. 2801–2808, Oct. 2011.

[5] D. E. Bakken, R. E. Schantz, and R. D. Tucker, "Smart grid communications: QoS stovepipes or QoS interoperability," Pullman, WA, USA, Tech. rep. TR-GS-013, Nov. 2009. [Online]. Available: http://gridstat.net/publications/TR-GS-013.pdf
[6] I. Sommerville, *Software Engineering*, 7th ed. Reading, MA: Addison-Wesley, 2004.
[7] M. Barbacci, M. Klein, T. Longstaff, and C. Weinstock, "Quality attributes" Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-95-TR-021, 1995.
[8] J. König, L. Nordström, and M. Österlind, "Reliability analysis of substation automation functions using PRMs," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 206–213, Mar. 2013.
[9] M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," presented at the IEEE Power Energy Soc. Power Syst. Conf. Exibit., Seattle, WA, USA, Mar. 2009.
[10] J. Ullberg, P. Johnson, and M. Buschle, "A language for interoperability modeling and prediction," *Comput. Ind.*, vol. 63, no. 8, pp. 766–774, Oct. 2012.
[11] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Syst. J.*, vol. 7, no. 3, pp. 363–373, Sep. 2013.
[12] *IEEE Standard for Synchrophasers for Power Systems*, IEEE Standard 1344-1995(R2001), 2001.
[13] *IEEE Standard for Synchrophasors for Power Systems*, IEEE Standard C37.118-2005 (Rev. IEEE Standard 1344-1995), 2006.
[14] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, IEEE Standard C37.118.2-2011, 2011.
[15] *Use of IEC 61850 to transmit Synchro-phasor Information according to IEEE C37.118, IEC*, IEC/TR 61850-90-5, 2012, ed. 1.0 .
[16] GridWise Architecture Council, GridWise Interoperabilty Context Framework (v1.1), Mar. 2008. [Online]. Available: www.gridwiseac.org
[17] National Institute of Standards and Technology, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," USA, NIST IR 7628, Sep. 2010, The Smart Grid Interoperability Panel, Cyber Security Working Group, Sep. 2010. [Online]. Available: csrc.nist.gov/publications/
[18] Eur. Comm. Smart Grids Task Force (SGTF), Expert Group 2 Deliverable, "Regulatory recommendations for data safety, data handling and data proctection," Dec. 2011. [Online]. Available: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf
[19] G. Ericsson, "Information security for electric power utilities (EPUs) cigré developments on frameworks, risk assessment and technology," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1174–1181, Jul. 2009.
[20] L. Pièrre-Cambacédès, "Cybersecurity myths on power control systems: 21 Misconceptions and false beliefs," *IEEE Trans. Power Del.*, vol. 26, no. 1, pp. 161–172, Jan. 2011.
[21] M. D. Hadley, J. B. McBride, T. W. Edgar, L. R. O'Neil, and J. D. Johnson, *Securing Wide Area Measurement Systems*. Richland, WA: Pacific Northwest Nat. Lab., Jun. 2007, PNNL- 17116.
[22] A. R. Wasicek, "Security in time-triggered systems," Ph.D. dissertation, Tech. Univ. of Vienna, Vienna, Austria, 2011.
[23] J. Hauer and J. DeSteese, *Descriptive Model of Generic WAMS*. Richland, WA: Pacific Northwest Nat. Lab., 2007.
[24] Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). "Wide area monitoring protection and control security profile V.08.", May 16, 2011, USA. [Online]. Available: http://www.smartgridipedia.org/images/4/43/Security_Profile_Blueprint_-_v1_0_-_20101006.pdf
[25] OMG Unified Modeling Language (OMG UML). ver. 2.4.1, Object Management Group (OMG), 2011.
[26] P. Johnson, J. Ullberg, M. Buschle, U. Franke, and K. Shahzad, "P2AMF: predictive, probabilistic architecture modeling framework," *Lecture Notes Bus. Inf. Process.*, vol. 144, pp. 104–117, Mar. 2013.
[27] Object Constraint Language specification. ver. 2.2 Formal/2010-02-01, Object Management Group (OMG), 2010.
[28] C. Lemieux, *Monte Carlo and Quasi-Monte Carlo Sampling*, ser. Springer Ser. Stat. New York: Springer, 2009.
[29] *IEEE Standard Glossary of Software Engineering Terminology*, IEEE Standard 610.12, 1990.
[30] J. Ullberg, U. Franke, M. Buschle, and P. Johnson, "A tool for interoperability analysis of enterprise architecture models using P-OCL," in *Enterprise Interoperability IV*. London, U.K.: Springer, 2010, pp. 81–90.
[31] Viking Consortium, D 2.2 Threats and Vulnerabilities, Final Report Vital Infrastructure, Networks, Information and Control System Management (VIKING) KTH, Rep. no. D2.2. 2011, May 30, 2011, EU FP7 Project. Prepared by Industrial Information and Control Systems.
[32] T. Sommestad, "Exploiting network configuration mistakes: Practitioners self-assessed success rate," Stockholm, Sweden, KTH, Tech. Rep. TRITA-EE 2011:069, 2011.
[33] M. Buschle, J. Ullberg, U. Franke, R. Lagerström, and T. Sommestad, "A tool for enterprise architecture analysis using the PRM formalism," presented at the CAiSE Forum, Tunisia, 2010.
[34] D. Koller and N. Friedman, *Probabilistic Graphical Models: Principles and Techniques*. Cambridge, MA: MIT Press, 2009.
[35] J. R. Caroll, GPA's Gateway Exchange Protocol: GEP Wire Format, 2012-02-29 (Presentation Slides). [Online]. Available: www.code plex.com/Download?ProjectName=openpg&DownloadId=360938
[36] Grid Protection Alliance, Grid Solutions. [Online]. Available: http://www. gridprotectionalliance.org/gsdefault.htm
[37] A. T. Al Hammouri, L. Nordström, M. Chenine, L. Vanfretti, N. Honeth, and R. Leelaruji, "Virtualization of synchronized phasor measurement units with real-time simulators for smart grid applications," presented at the IEEE Power Energy Soc. Gen. Meeting, San Diego, CA, USA, 2012.
[38] OPNET SITL, System In The Loop Module, Sept. 28, 2012. [Online]. Available: http://www.opnet.com/solutions/network_rd/system_in_the_loop.html

M. Chenine (S'12), photograph and biography not available at the time of publication.

.

J. Ullberg, photograph and biography not available at the time of publication.

L. Nordström (SM'12), photograph and biography not available at the time of publication.

Y. Wu, photograph and biography not available at the time of publication.

G. N. Ericsson (SM'06), photograph and biography not available at the time of publication.