27th Annual INCOSE International Symposium (IS 2017)
Adelaide, Australia, July 15-20, 2017

Using MBSE to Evaluate and Protect the Electrical Grid as a System of Systems

Matthew Hause
PTC
Engineering Fellow
Round Rock, Texas
MHause@PTC.com

Abstract. A System of Systems (SoS) is a large complex system, with varying degrees of operational independence, managerial independence, evolutionary development, geographical distribution and lifecycle independence. Critical Infrastructure such as the electrical grid contains all the aspects of a SoS. Due to the ever-increasing complexity of the grid, a single model encompassing all aspects of the grid would be impossible. Hence, we need to abstract the problem into a SoS set of aspects and examine the system both at the SoS level, as well as the detailed level. This will require the use of standardized systems modeling tools such as the Systems Modeling Language (SysML), and the Unified Architecture Framework (UAF) to define the overall goals, strategies, capabilities, interactions, standards, operational and system architecture, system patterns and so forth. This paper will examine the electrical grid as a SoS, define common characteristics, identify issues and vulnerabilities and MBSE strategies for addressing them.

Introduction

The purpose of this article is to examine the Electric Grid as a System of Systems (SoS) and discuss how taking this approach provides the tools and perspectives for addressing existing and future problems of security, resilience, expansion, vulnerabilities, etc. The paper discusses SoS and their characteristics, Model-Based Systems Engineering (MBSE) and how it is used. Also discussed is the Unified Architecture Framework (UAF) as a means of modeling an SoS and how this provides a means of addressing these issues. (UAF, 2016)

What is a System of Systems?

Critical Infrastructure such as the electrical grid contains all the aspects of a System of System (SoS). A SoS is a large complex system, with varying degrees of operational independence, managerial independence, evolutionary development, geographical distribution and lifecycle independence. (Dahman et al, 2010) The Department of Defense (DoD) Defense Acquisition Guidebook defines an SoS as a “set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities.” (DoD, 2013) The guidebook further emphasizes the importance of Systems Engineering (SE) regarding SoS. “SE is increasingly recognized as key to addressing the evolution of complex systems of systems. SE principles and tools can be used to apply systems thinking and engineering to the enterprise levels. An enterprise in this usage is understood to be the organization or cross-organizational entity supporting a defined business scope and mission, and includes the interdependent resources (people, organizations, and technology) to coordinate functions and share information in support of a common mission or set of related missions.” (FEAF), 1999). The electrical grid certainly meets these criteria and therefore, protection of the electrical grid will require both a systems engineering and a SoS approach. Let's take a look at the SoS characteristics.

Operational independence

The US national grid is operated by approximately 500 companies. They are a collection of independent operators, government institutions, municipal companies, and not for profit agencies. They operate independently to support their individual customers. Support of the overall is of secondary importance.

Managerial independence

Each of the US national grid entities must comply with a variety of different standards, rules, laws and regulations. The North American Electric Reliability Corporation (NERC) oversees all of them. However, they maintain their operational independence separate from that of the grid.

Evolutionary development

New systems, technologies or ConOps may be introduced by any of the companies as required to evolve and adapt to the changing environment, latest technology needs or stakeholder requirements. This will affect both the individual system as well as the SoS.

Geographical distribution

The Continental U.S. power transmission grid is geographically distributed by its very definition. It consists of about 300,000 km (186,411 mi) of lines and connects to Canada and Mexico.

Lifecycle independence

Even within the individual companies there will be multiple system lifecycles across asynchronous acquisition and development efforts, involving legacy systems, developmental systems, and technology insertion to meet their customer needs.

Why is this Important?

At this point it is useful to address why this is important. The system of system characteristics regarding levels of independence, management, lifecycle and control are essential if one is to attempt to understand and control a system. If one has complete control over a system then planning and executing a change to the system is relatively straightforward. The architecture of the system can be tightly coupled and interconnected as changes to systems and interfaces can be controlled and managed by a central authority. If however, one needs to negotiate any change amongst a multitude of companies, government entities, consumer groups, etc., then the architecture of the system needs to be loosely coupled with well defined, flexible and adaptive interfaces. By understanding these constraints, the system architecture can be managed in the most economical way. It also means that plans for making changes to interfaces will need to take place well in advance to provide time for the changes to be designed, negotiated and rolled out over a period of time.

Model-Based Systems Engineering (MBSE)

Due to the complexity of the electrical grid, models are routinely used throughout the complete lifecycle of the grid in the analysis, definition, construction, operation, maintenance, etc., phases. This is also the case in systems engineering. The INCOSE SE Vision 2020 defines Model-based systems engineering (MBSE) as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases." (INCOSE, 2007) The Systems Modeling Language (SysML) is the most widely used standardized systems modeling language and notation. It is used to model systems in both the abstract and concrete (logical and physical) views that include behavioral, structural, parametric and requirements views. (OMG, 2015) The SysML model is at the center of the systems engineering effort and integrates with specialist tools to provide analysis from viewpoints such as cost, resilience, structure, behavior, performance, requirements compliance, vulnerability, etc. The Unified Architecture Framework (UAF) is built on top of SysML and is used to define the overall goals, strategies, capabilities, interactions, standards, operational and system architecture, system patterns and so forth. (OMG, 2016) UAF leverages SysML capabilities such as parametrics, requirements, structure, allocation, etc. This will enable the resulting architectures to provide specifications for systems to be implemented rather than vague specifications and functional breakdown structures. The UAF was previously called the Unified Profile for DoDAF and MODAF (UPDM) and is undergoing finalization at the OMG. DoDAF is the Department of Defense Architecture Framework and MODAF is the Ministry of Defence Architecture Framework. Several papers have been written on the UPDM and its support of SoS modeling including (Hause, Dandashi, 2015) and (Hause, 2014). Details of SysML and UAF are not included here for space reasons. Please see the references for more information.

Concepts of abstraction and logical architecture

As P. E. Box said, “All models are wrong; some models are useful.” He went on to say, “Since all models are wrong the scientist cannot obtain a "correct" one by excessive elaboration. On the contrary following William of Occam he should seek an economical description of natural phenomena. Just as the ability to devise simple but evocative models is the signature of the great scientist so overelaboration and overparameterization is often the mark of mediocrity.” Due to the ever-increasing complexity of the grid, a single model encompassing all aspects of the grid would be impossible. Typical projects I have worked on encompassed millions of telemetered points just to operate a small portion of the overall grid. When the detailed mechanics of the individual equipment as well as cyber-security, connection to the internet, the internet of things (IoT), power trading components, co-generation and other aspects are added the problems quickly become too complex to analyze. Neither are such “all encompassing” models necessary for the purpose of “useful” decision support. Instead, we need to abstract the problem into a SoS set of aspects and examine the system both at the SoS level, as well as the detailed level. Analysis using these standard methods can help identify potential problems that can be analyzed by specialty tools and the results fed back into the SoS model. This is the standard way of working for most MBSE projects, and this approach should also be adopted here as well.

UAF Views

Prior to modeling a SoS, one needs to understand the purpose of the SoS as well as the purpose of the model. In this case, the purpose of the SoS Grid model is to capture the goals, vision, capabilities, systems, requirements etc. of the energy grid. UAF has a set of views for defining the SoS Capabilities over its life-cycle phases. These are used to define the goals, vision, enterprise phases, the SoS evolution over time and the SoS Capabilities and how these are realized by systems. UAF defines traceability from these elements to the other views including the Operational Architecture which is used to define the abstract, logical and solution independent expression of the SoS. This defines what needs to be done and traces directly to the Systems views that define how these capabilities and operational architecture will be realized. To use and analogy, the operational view could define a need to generate power, and the systems views define fossil fuel, solar, wind, tidal and other means of providing the power. Standards views are used to define system standards and systems that conform to them, Services views define services to be implements by systems and the Project views define when the systems will be deployed and retired. In addition, the latest version of the UAF also defines

Security and Human Factors views. Work is also being done with the System Assurance group at the OMG to integrate threat and risk analysis as a set of cross cutting concerns.

The UAF Grid

Due to the complexity of managing the multiple viewpoints with overlapping concerns and metamodels it was decided to refactor the standard viewpoints as described in the donor frameworks into a more manageable format. Figure 1 shows the grid.

	Taxonomy Tx	Structure Sr	Connectivity Cn	Processes Pr	States St	Interaction Scenarios Is	Information If	Parameters Pm	Constraints Ct	Roadmap Rm	Traceability Tr
Metadata Md	Metadata Taxonomy Md-Tx	Architecture Viewpoints [a] Md-Sr	Metadata Connectivity Md-Cn	Metadata Processes [a] Md-Pr	-	-			Metadata Constraints [a] Md-Ct		Metadata Traceability Md-Tr
Strategic St	Strategic Taxonomy St-Tx	Strategic Structure St-Sr	Strategic Connectivity St-Cn	-	Strategic States St-St	-			Strategic Constraints St-Ct	Strategic Deployment, St-Rm Stategic Phasing St-Rm	Strategic Traceability St-Tr
Operational Op	Operational Taxonomy Op-Tx	Operational Structure Op-Sr	Operational Connectivity Op-Cn	Operational Processes Op-Pr	Operational States Op-St	Operational Interaction Scenarios Op-Is			Operational Constraints Op-Ct	-	-
Services Sv	Service Taxonomy Sv-Tx	Service Structure Sv-Sr	Service Connectivity Sv-Cn	Service Processes Sv-Pr	Service States Sv-St	Service Interaction Scenarios Sv-Is	Conceptual Data Model,	Environment Pm-En	Service Constraints Sv-Ct	Service Roadmap Sv-Rm	Service Traceability Sv-Tr
Personnel Pr	Personnel Taxonomy Pr-Tx	Personnel Structure Pr-Sr	Personnel Connectivity Pr-Cn	Personnel Processes Pr-Pr	Personnel States Pr-St	Personnel Interaction Scenarios Pr-Is	Logical Data Model,		Competence, Drivers, Performance Pr-Ct	Personnel Availability, Personnel Evolution, Personnel Forecast Pr-Rm	Personnel Traceability Pr-Tr
Resources Rs	Resource Taxonomy Rs-Tx	Resource Structure Rs-Sr	Resource Connectivity Rs-Cn	Resource Processes Rs-Pr	Resource States Rs-St	Resource Interaction Scenarios Rs-Is	Physical schema, real world results	Measurements Pm-Me	Resource Constraints Rs-Ct	Resource evolution, Resource forecast Rs-Rm	Resource Traceability Rs-Tr
Security Sc	Security Taxonomy Sc-Tx	Security Structure Sc-Sr	Security Connectivity Sc-Cn	Security Processes Sc-Pr	-	-			Security Constraints Sc-Ct	-	-
Projects Pj	Project Taxonomy Pj-Tx	Project Structure Pj-Sr	Project Connectivity Pj-Cn	-	-	-			-	Project Roadmap Pj-Rm	Project Traceability Pj-Tr
Standards Sd	Standard Taxonomy Sd-Tx	Standards Structure Sd-Sr	-	-	-	-			-	Standards Roadmap Sr-Rm	Standards Traceability Sr-Tr
Actuals Resources Ar		Actual Resources Structure, Ar-Sr	Actual Resources Connectivity, Ar-Cn	Simulation [b]					Parametric Execution/Evaluation [b]	-	-
Dictionary * Dc											
Summary & Overview SmOv											
Requirements Rq											

Figure 1. The UAF Viewpoints Grid

The grid was developed as a way of showing how the various viewpoints correspond to the generic layers of abstraction or domains (horizontal rows) and the types of model kinds or architectural representations (the columns) used to describe the viewpoints. The grid is not intended to be complete but to capture the information that is present in the frameworks that contribute to the UAF/P. Consequently some gaps are evident.

View Type

- Taxonomy Tx
  Presents all the elements as a standalone structure. Presents all the elements as a specialization hierarchy, provides a text definition for each one and references the source of the element
- Structure S
  Describes the definitions of the dependencies, connections, and relationships between the different elements.
- Connectivity Cn
  Describes the connections, relationships, and interactions between the different elements.
- Processes Pr
  Captures activity based behaviour and flows. It describes activities, their Inputs/Outputs, activity actions and flows between them.

- States St
  Captures state-based behaviour of an element. It is a graphical representation of states of a structural element and how it responds to various events and actions.
- Interaction Scenarios Is
  Expresses a time ordered examination of the exchanges because of a particular scenario. Provides a time-ordered examination of the exchanges between participating elements
- Information If
  Address the information perspective on operational, service, and resource architectures. Allows analysis of an architecture’s information and data definition aspect, without consideration of implementation specific issues.
- Constraints Ct
  Details the measurements that set performance requirements constraining capabilities. Also defines the rules governing behaviour and structure.
- Roadmap Rm
  Addresses how elements in the architecture change over time. Also, how at different points in time or different periods of time.
- Traceability Tr
  Describes the mapping between elements in the architecture. This can be between different viewpoints within domains as well as between domains. It can also be between structure and behaviours.

Domains

- Metadata Md
  Captures meta-data (definition of the data format of the model) relevant to the entire architecture. Provides information pertinent to the entire architecture. Presents supporting information rather than architectural models.
- Strategic St
  Capability management process. Describes the capability taxonomy, composition, dependencies and evolution of the enterprise and individual systems.
- Operational Op
  Illustrates the Logical Architecture of the enterprise. Describes the requirements, operational behaviour, structure, and exchanges required to support (exhibit) capabilities. Defines all operational elements in an implementation/solution independent manner.
- Services Sv
  The Service-Orientated View (SOV) is a description of services needed to directly support the operational domain as described in the Operational View. A service within MODAF is understood in its broadest sense, as a unit of work through which a provider provides a useful result to a consumer.
- Personnel Pr
  Defines and explores organizational resource types. Shows the taxonomy of types of organizational resources as well as connections, interaction and growth over time. This domain encompasses the Human Views and is the main subject of this paper.
- Resources Rs
  Captures a solution architecture consisting of resources, e.g. organizational, software, artefacts, capability configurations, and natural resources that implement the operational requirements. Further design of a resource is typically detailed in SysML or UML.
- Security Sc
  Security assets and security enclaves. Defines the hierarchy of security assets and asset

owners, security constraints (policy, laws, and guidance) and details where they are located (security enclaves).

- Projects Pj
  Describes projects and project milestones, how those projects deliver capabilities, the organizations contributing to the projects and dependencies between projects.
- Standards Sd
  Technical Standards Views are extended from the core DoDAF views to include non-technical standards such as operational doctrine, industry process standards, etc. and the set of rules governing the arrangement, interaction, and interdependence of solution parts or elements.
- Actual Resources Ar
  The analysis, e.g. evaluation of different alternatives, what-if, trade-offs, V&V on the actual resource configurations. Illustrates the expected or achieved actual resource configurations.

Implementation of the Grid

In the intersection of the matrices are the different views available for the modeler. For example, the intersection of logical connectivity is the operational node diagram and the generated report, called the node interaction view. By changing the format to the matrix view, it more clearly represents the different concerns and provides a means of defining further fit for purpose views. Additional columns and rows would also allow for other frameworks to be mapped onto the grid putting the emphasis on the underlying metamodel to support a set of concerns realized as a viewpoint and instantiated as a view. Hence this creates a semantic unification of concepts and relationships. Finally, the way that the UAF has been defined enables SysML tool vendors (if their tools allow) to carry out behavioral analysis based upon simulation and the evaluation of non-functional requirements based upon parametric diagram execution and analysis.

Enterprise Architecture Model of the Grid

This section contains a sample of views of a simplified enterprise architecture model of the electric grid. The various example views provide a means of looking at various aspects of the enterprise in various formats. Separation of the different aspects into the different viewpoints is essential as a means of providing a human readable set of semantically correct diagrams. A complete view of the architecture would result in enormously complicated and complex diagrams that would not be useful for anyone. By concentrating on a single aspect and presenting it in an understandable way, the concepts can be clearly communicated. Each diagram is a “projection” of the underlying data in the database. If the data is changed, the diagram is changed. If the diagram is changed, then the data is changed. Also, because each diagram contributes to the whole, a complete picture of the architecture can be built up over time by the specialists in each area. Human factors experts can create the personnel views, strategy experts create the capability/strategic views, project managers create the roadmap views, etc. Changes in the user interface can be evaluated to determine system usability, component updates evaluated for security threats and so forth. This integrated view of the system of systems is essential if the architect is to get a complete understanding of the architecture and how it evolves over time.

Enterprise Concept Diagram

The enterprise concept diagram describes the interactions between the subject architecture and its environment, and between the architecture and external systems. First, it communicates the essence of the scenario context in an essentially graphical form. Second, it provides a means of organizing the operational architecture models into distinct groups based on scenario context. A textual description accompanying the graphic is crucial.

Each model element depicted may include a graphical depiction to help convey its intended meaning. The spatial relationships of the elements on the diagram sometimes convey their relative position, although this is not specifically captured in the semantics. A brief description of the interactions between the elements is provided. It may represent abstract conceptual relationships and will be refined in subsequent diagrams.

Figure 2 sets the context by illustrating the operational concept. The grid is made up of traditional electrical grid elements such as transmission, distribution, generation, substations, etc. More modern elements such as the green generation, cyber criminals and power traders have also been added. The relationships between the elements describe the relationship that each element has with each other. The cyber-criminal attacks the home consumer, smart grid control and distribution. Transformers transfer power between transmission and distribution. Elements may have multiple relationship and these can also be shown. Discussion can take place regarding the relationships that the elements have with one another to determine their different purposes in the enterprise. The standard blue boxes have been replaced with graphics to aid understanding and communication with stakeholders.

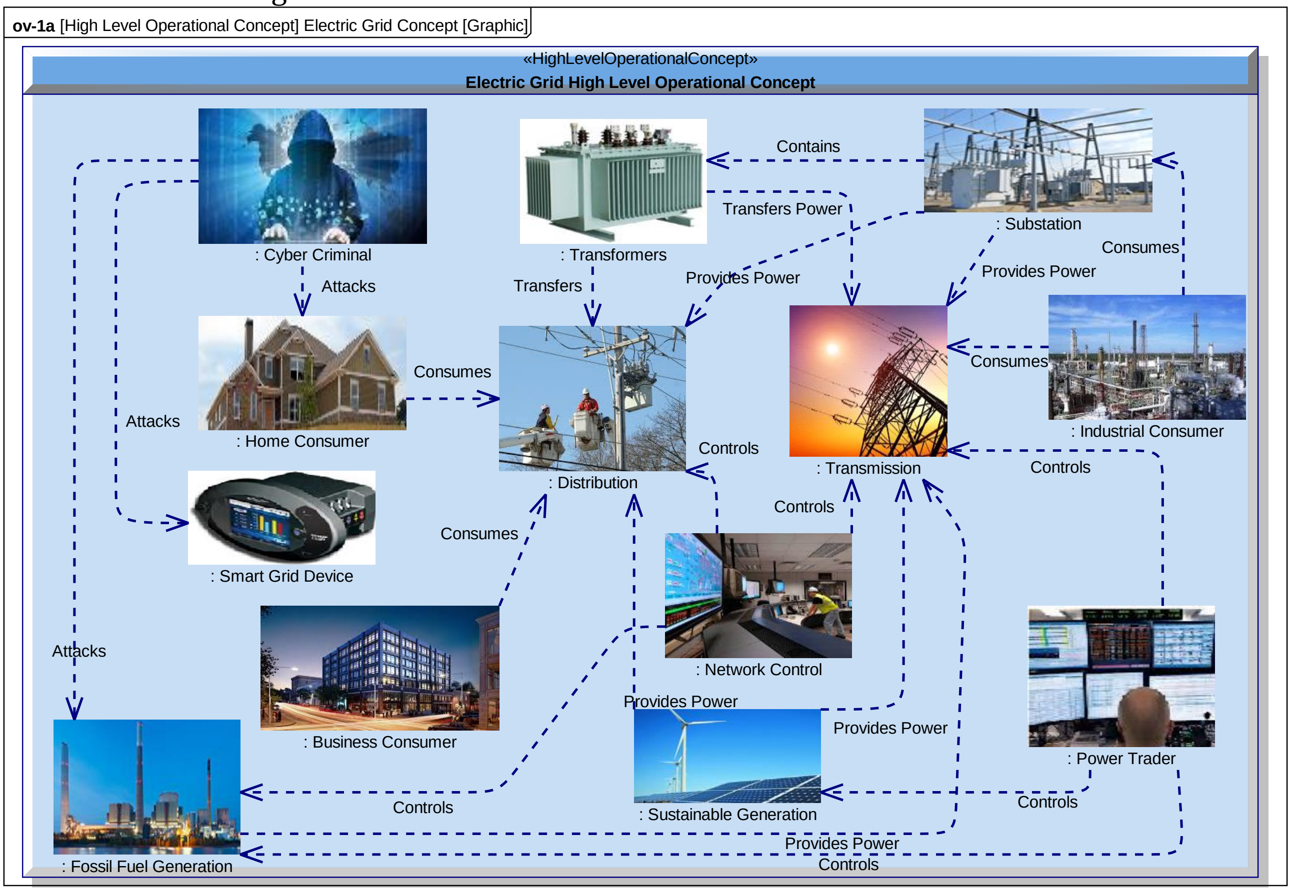

Figure 2. Electric Grid High Level Operational Concept

Capabilities

A capability is a high-level specification of the enterprise's ability to execute a specified course of action. Capabilities need to be characterized in terms of the properties they need to exhibit which enable the enterprise to use them to achieve the enterprise goals, as well as their relationships in an inheritance hierarchy. Capabilities are also defined by their desired outcomes: what benefit or tangible result occurs because of the existence of the capability. Figure 3 shows the taxonomy of capabilities of the electric enterprise. Obviously, this taxonomy of capabilities is only a partial list for reasons of space.

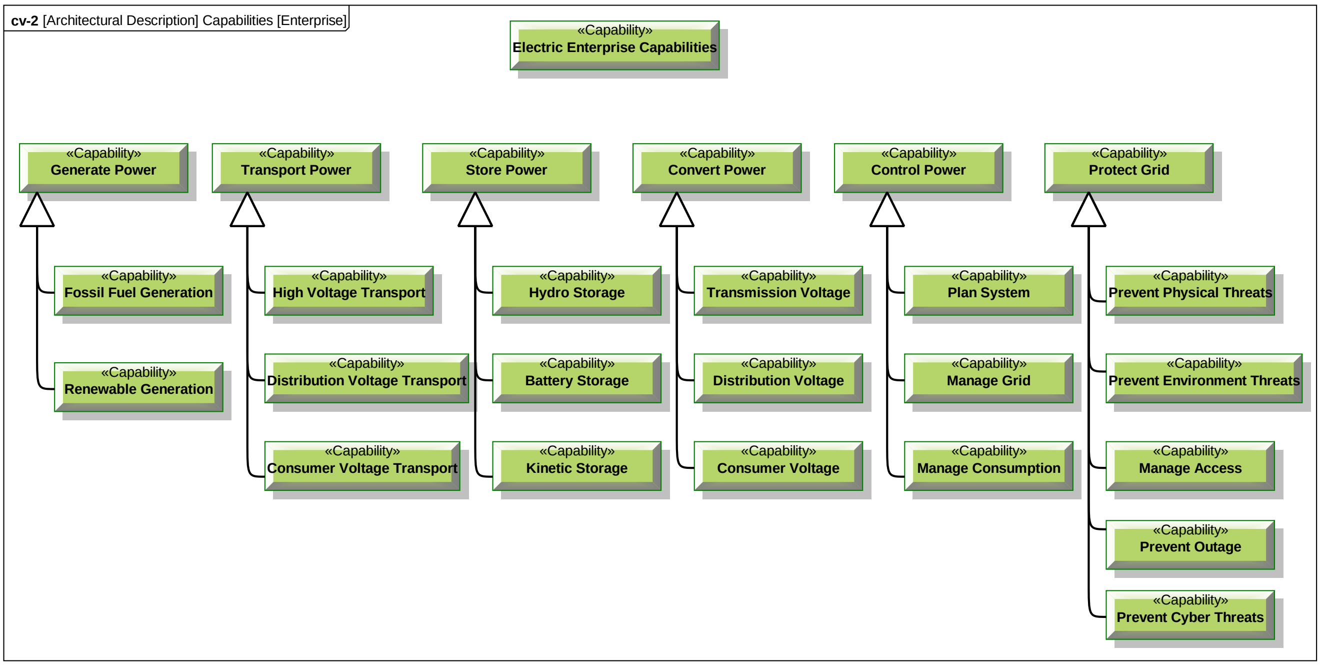

Figure 3. Electric Enterprise Capabilities

The high-level capabilities are defined as generate power, transport power, store power, convert power, control power and protect grid. Sub-capabilities of store power ae hydro storage, battery storage and kinetic storage. For protect grid these are: prevent physical threats, prevent environmental threats and manage access. As the architecture is developed, these each capability can be associated with a resource that exhibits or realizes the capability. Prevent physical threats can be provided by fencing, armed guards, locked and protected buildings, etc. Fossil fuel generation is provided by coal, natural gas, oil, etc. By defining the capabilities and linking then to their implementing systems, the architect can perform a trade-off analysis to determine which is the best system to solve a particular problem.

Enterprise Use Cases

A use case defines a functional goal that a stakeholder has. Figure 4 shows a Use Case diagrams showing the use cases, their relationships, and the stakeholders involved. For example, government regulators regulate the network, customers use electricity, carbon traders offset carbon output, etc.

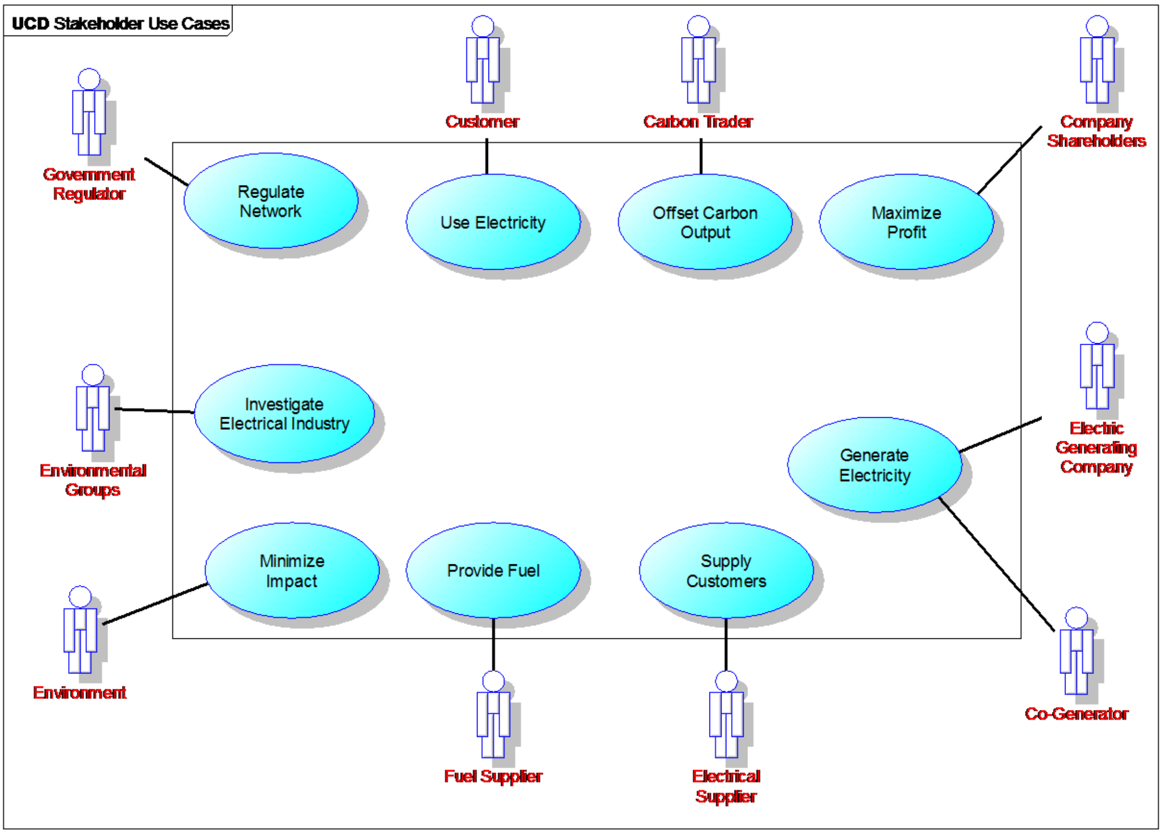

Figure 4. Stakeholder Use Cases

Operational Model

The Operational Views identify what needs to be accomplished in the enterprise and who needs to accomplish it. These views describe the tasks and activities, operational elements and exchanges of information, systems and energy that are required to conduct the operations. Stakeholders are Business Architects, Systems Engineers, Enterprise Architects, and Node Owners. It identifies the operational exchange requirements between Operational Performers. It defines operational architecture and exchange requirements necessary to support a specific set of Capability(ies).

Figures 5 depicts the key players in the electric grid operation and the interactions for information exchange. It identifies the different types of Operational Performers logical nodes: fossil fuel generation, power broker, network control, etc. Unwanted actors such as the cyber-criminal are shown attacking the smart grid controls, network controls, etc. This diagram indicates the need to exchange information between the Operational Performers and shows the interactions between these Operational Performers. Other interactions can be exchanged between the Operational Performers such as equipment, energy, and so forth. The view shows the operational activities undertaken by a few select Operational Performers.

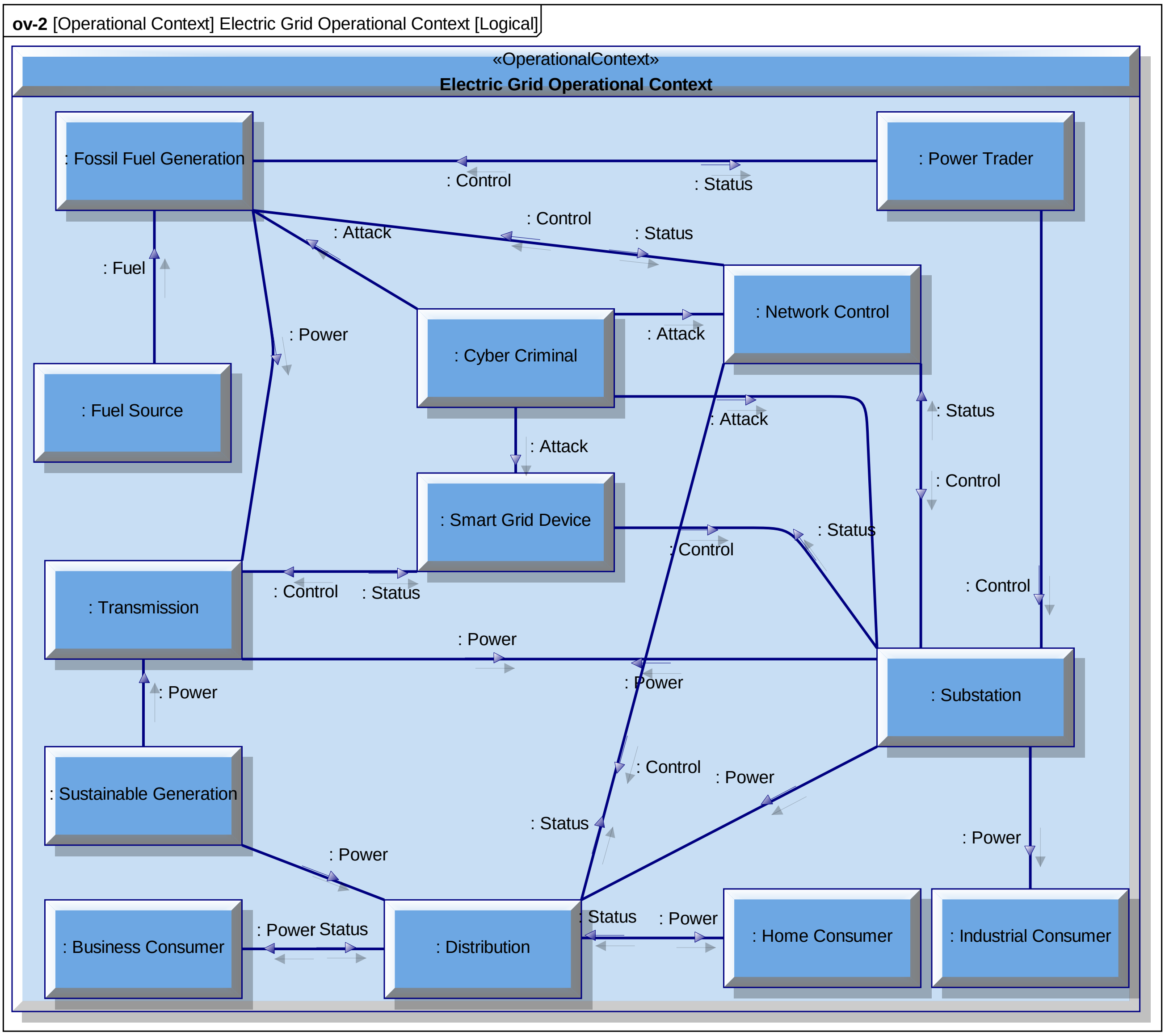

Figure 5. Electric Grid Logical Architecture

Interactions are also shown. Energy in the form of power is sent from distribution to the business and home consumer. Status information is sent from the business and home consumer to distribution. Control is sent from network control to substation, distribution, transmission, etc., and status is received from them.

Resource View: The Network Grid

The resources view is a definition of solution architectures to implement operational requirements. It captures a solution architecture consisting of resources, e.g. organizational, software, artifacts, capability configurations, natural resources that implement the operational requirements. Further design of a resource is typically detailed in SysML or UML.

These views describe the resources that realize the electric grid capabilities or implement services. They describe resource functions, interactions between resources, and can provide detailed system interface models. System views can describe the "as-is" and/or "to-be" configuration. In addition, several different configurations can be created to perform trade-off analysis. When used in conjunction with SysML, the systems should be developed to the degree that they define the requirements for actual systems that will be implemented. Developing the system views to too much detail will unnecessarily constrain the solution and will involve duplication of work.

System elements can include more than just physical systems. They can include software, organizational resources such as organizations, posts and roles. Resources are a composition of resources that can deliver a capability. As in the operational views, interactions can consist of more than just information and can include Posts, organizations, capability configurations, energy and software. Figure 6 shows the simplified physical systems for the electrical grid.

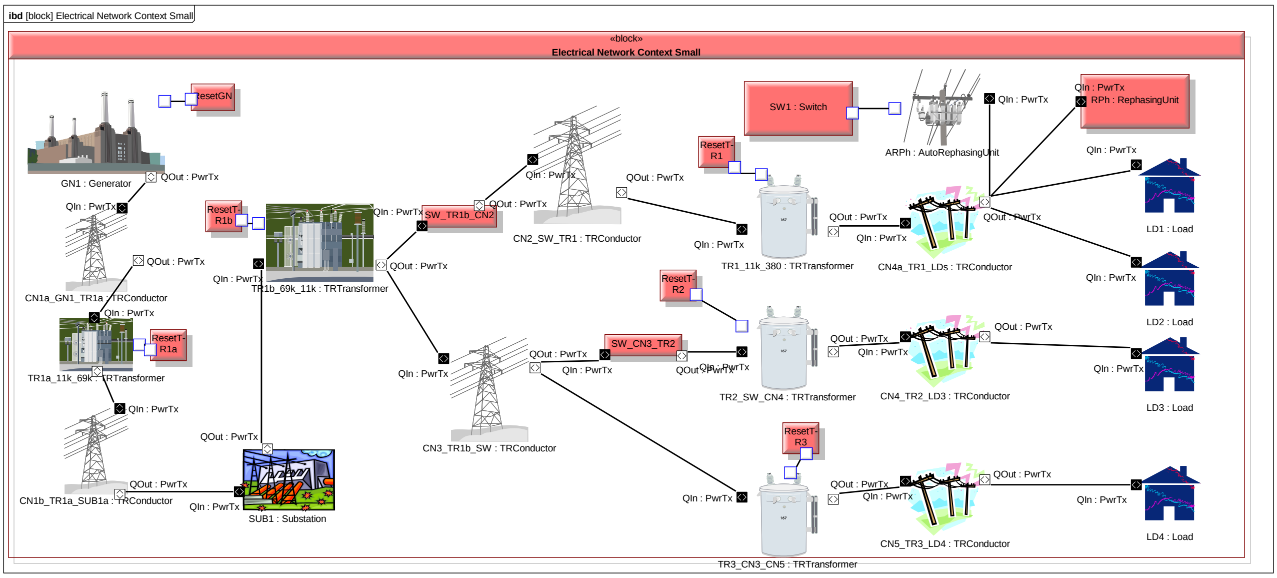

Figure 6. Simplified Electric Grid System Context

The resource structure view defines the structure and internal flows of the system architectures to demonstrate how they realize the logical architecture defined in the operational views. The interfaces and interactions are defined at the level of specifying a need for the systems to interact and the way in which the do so. These systems can be decomposed to any level required. Figure 6 shows the Capability Configuration of the electric grid is comprised of substations, transformers, generators, consumers, etc., and the roles that make up the system, as well as the components that enable them to fulfill their role.

Component Level State Behavior

State diagrams can be created to capture state-based behavior of a resource. It is a graphical representation of states of a resource and how that resource responds to various events and actions. The state diagram is used to describe the resource's responses to the various events that it can receive. It can also be to show the operational states of the resource. Figure 7 shows the state based behavior for the conductor.

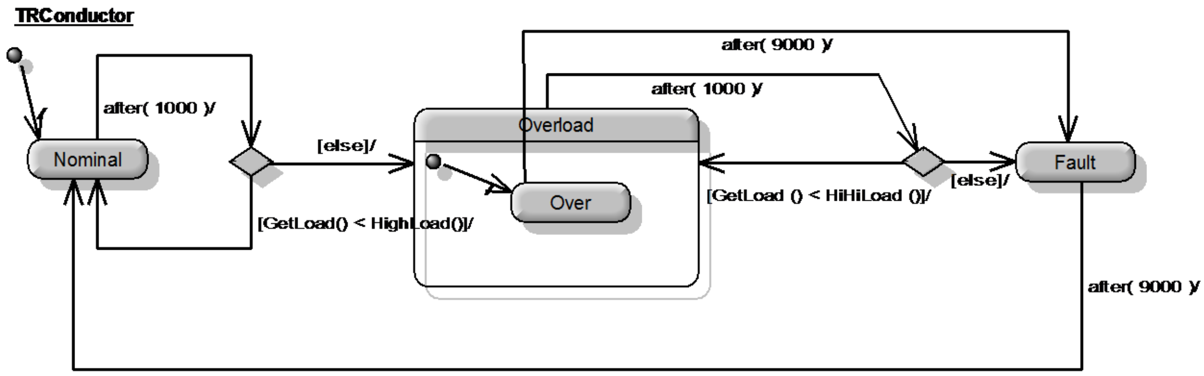

Figure 7. Conductor State Based Behavior

This simple diagram was chosen to show the states of a simple system component. In this case, it defines the conductor states when the line is overloaded and causes a fault condition. This was created for a simulation and was used to show how the drooping conductors would cause a fault when it struck tree branches.

Security

The security views are a specification of the Security Control families, security controls, and measures required to address a specific security baseline. A security profile defines the controls (actions) allocated to assets. Stakeholders re Security Architects, Security Engineers, etc. It provides a set of Security Controls and any possible enhancements as applicable to assets. The activity diagram in Figure 8 describes operational or resource level processes that apply (operational level) or implement (resource level) security controls/enhancements to assets located in enclaves and across enclaves. This Security Process view can be instantiated either as a variant of an activity/flow diagram or as a hierarchical work breakdown structure.

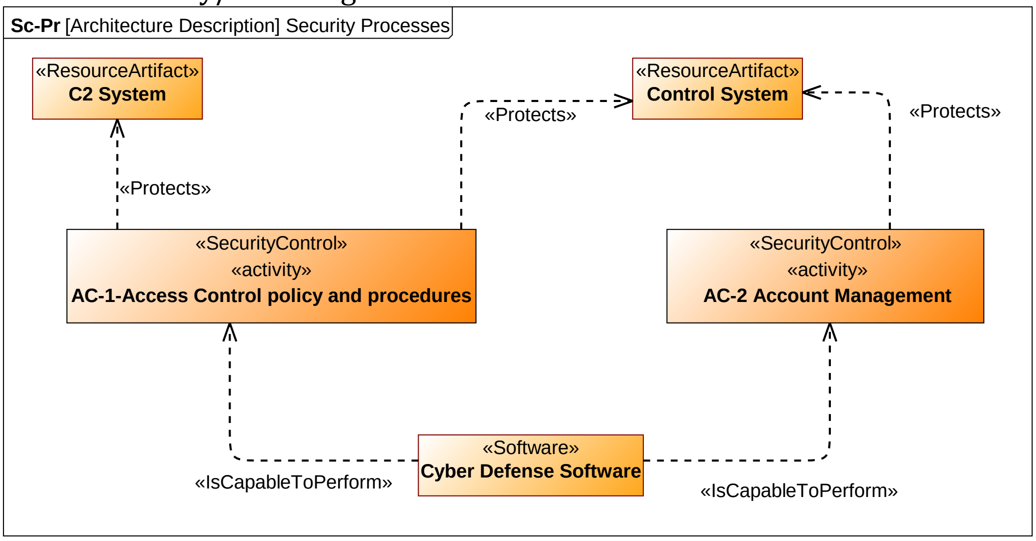

Figure 8. System Cyber Controls

In this case, the cyber defense software provides access control policy and procedures and account management for the C2 system and the control system. Figure 9 shows how risk and risk mitigation may be associated with systems and information/data.

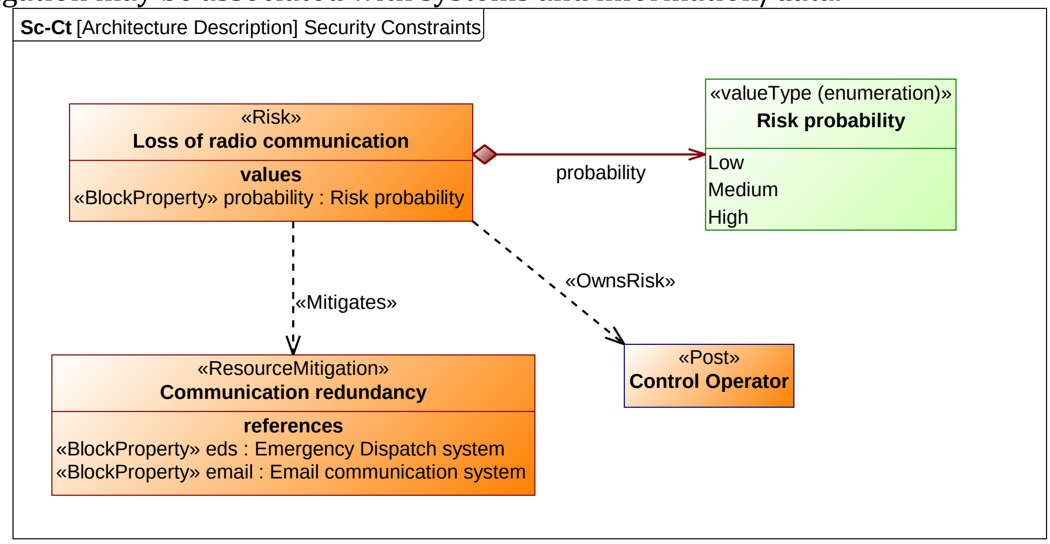

Figure 9. Security Constraints for Communication Systems

Figure 9 describes the security constraints for the Communications Systems. This is for the emergency dispatch system. It defines the risk probabilities, who owns the risk and the mitigating elements. The UAF security views are being further developed and enhanced by the UAF task force at the OMG. This is being done with military and civilian security experts and the updated views will be submitted in the revised specification in June 2017. There are several projects making use of these views and it is hoped that their results will be presented at future conferences.

Architecture Cross Cutting Concerns

Cross cutting concerns are those characteristics of an architecture that by definition cannot be modular and cuts across other aspects. A simple example would be vehicular safety. When a car is designed, there is no specific component of the car that is the safety module. Safety needs to be inherent and intrinsic to the car design and implementation or the car will not be safe. Furthermore, overall safety performance must also be attributed to the vehicle operator, as well as the environment in which the vehicle operates. In the same way, the electric grid contains a variety of cross cutting concerns that need to be addressed. These include security, safety, resilience, flexibility, robustness and others. The examples listed below are not just previous research or a literature review. They have been included at the end of the paper because they interface, inter-operate, and work in conjunction with the UAF. Additionally, new products and research are currently being developed regarding threat and risk, resilience, as well as further development of the security views. They are currently works in progress, and further papers will examine these in more detail. Let's look at some of these.

Security

Security for the energy grid is not contained in a single component but needs to reside throughout the entire system of systems. This is problematic as the grid needs to be open and ubiquitous since it connects to almost every building on the planet as well as secure and protected to ensure safe and secure operations. Security includes both physical and cyber-attacks and that UAF and SysML can be used to address these from both a system and human perspective. When designing a system, every interface is a potential point of vulnerability. This can be a simple attack such as hacking a smart meter to turn off someone's electricity, or the cyber-attack on the Ukrainian power grid that affected 225,000 customers and shut down the power for several hours. Risk analysis and risk mitigation of interdependent elements of systems are too often done in isolation, making these systems vulnerable to multi-stage cyber-attacks. Companies such as KDM analytics provide tools that can examine UAF models providing efficient, formal, systematic and comprehensive performance of risk analysis using the system architecture as well as the UAF security views. The constructs in Figures 8 and 9 are used by this software as well as the physical system.

Resilience

Resilience is the capacity of the system to recover quickly from faults and errors, a key characteristic in an electrical grid. J. Marvin (2015) presented the quantified results of an Energy Grid Management Use Case to explore grid performance boundaries in the face of proliferated residential solar array deployments. The Use Case demonstrated how modern IT open source tools can be integrated into a grid simulation that provides a decision support tool for the utility industry to manage future change. The resulting simulation environment executes the simulated grid network with structured and unstructured data results stored in the graph database. The work leverages DoD sponsored research in Uncertainty Quantification in complex System of System Modeling and Simulation environments and demonstrates future model based techniques for risk management, financial modeling, grid resiliency and critical infrastructure protection. (Marvin, 2015)

Cyber Attacks

Kam (2016) presented a paper on the problem of cyber-attacks on the electric grid. The problem statement was defined as follows: "Our nation's energy infrastructure is probably one of the most critical (yet most vulnerable) systems. If the infrastructure is crippled even temporarily, it can cause significant damages socially, financially and economically. Case in point was the Northeast Blackout in 2003 which had impacted 55 million people across US and Canada. This issue is further exacerbated by the cyber threats that are so prevalent today both in the commercial and defense sectors. Cyber-attacks are real and are constantly evolving. In Dec 2015, the Ukraine's power grid was hacked; the cyber attackers shut down several power generators simultaneously causing havoc. To ensure cyber threats will not adversely impact energy infrastructure in the US, it is critical that we examine the attack surface and assess the cyber risks." (Kam, 2016) The methodology was as follows:

- "Develop a cyber-attack scenario that involves industrial control system (ICS) hacking
- Leverage Global IT Infrastructure Simulator (MIT) and Cyber Attack Network Simulation (LM) to model threat behaviors and attack surface characterization
- Define attack surface and capture relevant metrics (MOP/MOE)
- Identify capability and operational gaps through assessing effectiveness of existing cyber protection system against malicious attacks" (Kam, 2016)

This detailed simulation system could be combined with the enterprise architecture view to define the elements at the high level and develop the strategy, as well as simulate the individual aspects of the system. In addition, the solution could be evaluation in conjunction with the higher-level goals and capabilities of the architecture to determine if there are conflicts and issues.

Integration into the Architecture

Defining the capabilities, logical architecture and physical architecture allows the architect to get the big picture of the enterprise as well as the detailed strategy for implementation. Defining the points of vulnerability for security and resilience allows engineers to perform trade-off and threat and risk analysis on the architecture as a whole. Integrating the analysis tools with the UAF architecture provides a means of defining the problem, designing possible solutions, and then performing trade-off analysis to determine the best fit.

Integrating the System and the SoS Views

UAF models can be integrated and traced to SysML models. Using UAF, the SoS model can define the requirements for a set of systems, interfaces, multi-system performance, etc. and SysML can be used to further specify and analyze the requirements for each system and their hardware & software components, personnel roles/responsibilities (both good and bad), detailed interfaces, performance, etc. This was discussed in Hause, Thom (2007). Using requirements traceability, allocation, and viewpoints, traceability and interoperability can be created between the UAF SoS the SysML systems view. Techniques in this area have evolved in the past 8 years since this paper was written, and will be the subject of a future INCOSE paper. By integrating and tracing these concerns from the SoS to the systems views, engineers can plan the deployment and implementation on the different parts of the grid and examine cost and impact analysis, develop trade studies for optimum solutions, etc. These can then be further evaluated using the specialty tools of the electric industry. They could also identify the need for new and innovative ways of analyzing and evaluating these systems.

Future Work

Work on the UAF is carrying on in this and other industries. A paper entitled "An industrial example of using Enterprise Architecture to speed up systems development" (Sjoberg, et al, 2017) will also be presented at INCOSE IS 2017. It discusses uses the UAF to analyse the operations of a rock quarry for electrification and possible autonomous vehicle testing. Future work on the security views is being developed at the OMG with cyber-security experts to develop the views to support threat and risk as well as for customization with additional areas. System assurance work being done at the OMG will look at evaluating architectures for safety, security and resilience. These and other efforts involve defining the architectures and using specialist tools for more detailed analysis.

Summary and Conclusions

There are a variety of tools in use in the electrical industry for designing, managing, controlling, running, evaluating and forecasting the electric grid and its needs. These are specialty tools developed over a number of years that are well suited to the energy industry of the 20th century. The electric grid of the 21st century and beyond will need to cope with the smart grid, cyber-attacks, space weather, Electro-Magnetic Pulse (EMP) weapons, proliferation of clean energy sources, phase-out of fossil fuels, and many other aspects that we have not yet dreamed of or (to coin a term) “nightmared” of. We need to approach the problem from a systems engineering point of view that examines the entire problem and derives creative ways to cope with the problems of the 21st century and beyond. As Einstein said, “We can't solve problems by using the same kind of thinking we used when we created them.” Systems engineering will provide that new way of thinking, and MBSE for SoS with UAF in the form of a grid model integrated with specialty tools will provide the means to realize the solutions.

References

DoD, 2013, Defense Acquisition Guidebook, Production Date:15 May 2013 Available at http://at.dod.mil/docs/DefenseAcquisitionGuidebook.pdf, Accessed Nov, 2013

Federal Enterprise Architecture Framework (FEAF), Version 1.1, September 1999, Available online at http://www.enterprise-architecture.info/Images/Documents/Federal%20EA%20Framework.pdf, Accessed Nov, 2013

Hause M., SOS for SoS: A New Paradigm for System of Systems Modeling, IEEE, AIAA Aerospace Conference, 2014

Hause M., Dandashi F., UAF for System of Systems Modeling , Systems Conference (SysCon), 2015 IEEE International

Hause M., Thom F., 2007, Bridging the Chasm - Tracing from Architectural Frameworks to SysML, presented at the INCOSE IS, 2007

INCOSE SE Vision 2020, September 2007, Available at http://www.incose.org/ProductsPubs/pdf/SEVision2020_20071003_v2_03.pdf, Accessed Nov 2013

J. Dahmann, G. Rebovich, J. Lane, R. Lowry, “System Engineering Artifacts for SoS,” Systems Conference, 2010 4th Annual IEEE, DOI: 10.1109/SYSTEMS.2010.5482491, 2010

Kam A., Lockheed Martin, Modeling Cyber Attack Surface on the Power Grid, Presented at the 2016 NDIA Systems Engineering Conference

Marvin J, Complex Energy Grid Management in a Changing and Dynamic Future, EnergyTech 2015, Cleveland

Object Management Group (OMG), June, 2012, OMG Systems Modeling Language (OMG SysML™), V1.3, OMG Document Number: formal/2012-06-01, http://www.omg.org/spec/SysML/1.3/PDF/, Accessed November, 2013

OMG, “Unified Profile for DoDAF/MODAF (UPDM) V2.1,” OMG Document Number: formal/2013-08-04, OMG, 2013, http://www.omg.org/spec/UPDM/2.1/PDF

OMG, 2015, Systems Modeling Language, Available at http://www.omg.org/spec/SysML/1.4/PDF

OMG, 2016, Unified Architecture Framework Profile (UAF), available at http://www.omg.org/spec/UAF/1.0/Beta1/

Sjoberg P., Hause M., Kihlstrom L., 2017, An industrial example of using Enterprise Architecture to speed up systems development, to be presented at INCOSE IS, Adelaide Australia

Biography

Matthew Hause is a PTC Engineering Fellow and GTM Technical Specialist, the co-chair of the UPDM group a member of the OMG Architecture Board, and a member of the OMG SysML specification team. He has been developing multi-national complex systems for over 35 years. He worked directly in the power systems industry for over 20 years at energy companies, control and SCADA companies, as well as component suppliers. He has experience in military command and control systems, process control, manufacturing, factory automation, communications, SCADA, distributed control, office automation and many other areas of technical and real-time systems. His roles have varied from project manager to developer. His role at PTC includes mentoring, sales presentations, standards development, presentations at conferences, specification of the UPDM profile and developing and presenting training courses. He has written over 100 technical papers on architectural modeling, project management, systems engineering, model-based engineering, human factors, safety critical systems development, virtual team management, product line engineering, systems of systems, systems and software development with UML, SysML and Architectural Frameworks such as DoDAF and MODAF. He has been a regular presenter at INCOSE, the IEEE, BCS, the IET, the OMG, AIAA, DoD Enterprise Architecture, Embedded Systems Conference and many other conferences. He was recently a keynote speaker at the Model-based Systems Engineering Symposium at the DSTO in Australia. Matthew studied Electrical Engineering at the University of New Mexico and Computer Science at the University of Houston, Texas.