Smart Power Grid Security: A Unified Risk Management Approach

Partha Datta Ray  Rajgopal Harnoor  Dr. Mariana Hentea
Albeado Inc. ABB Inc. Albeado Inc
Saratoga, CA 95070 Santa Clara, CA 95050 Saratoga, CA 95070
USA USA USA
parthadattaray@ieee.org rajgopal.harnoor@us.abb.com mariana.hentea@ieee.org

Abstract - Power grid information security and protection has aspects of both Industrial Control Systems (ICS) as well as Information Technology (IT) Systems. Although both ICS and IT systems require information security services to combat malicious attacks, the specifics of how these services are used for the power grid depend upon appropriate risk assessment and risk control. Distinct types of attacks targeting ICS and IT systems as well as different performance requirements of these systems determine a specific priority order of the security services implemented for each system.

Threat profiles of the power transmission and distribution management functions, where availability is paramount to all other security services, differ significantly from threat profiles of IT functions such as utility customer billing where confidentiality is a greater concern – hence warranting different security posturing.

This paper discusses different approaches for security risk management in the context of the smart power grid. Methodologies proposed for risk assessment include threat and vulnerability modeling schemes which help in identifying and categorizing the threats, as well as in analyzing their impacts, and subsequently prioritizing them. Risk management planning techniques as they apply to both ICS and IT systems are also discussed.

Index Terms – Smart Grid Cyber Security, Unified Risk Management, Smart Grid Risk Assessment, Smart Grid Security Risk, Smart Grid Vulnerabilities and Threat, DMS

I. INTRODUCTION

The smart power grid is slated to usher in a paradigm shift in ways electric energy is produced, traded and consumed. Most visions of modernization of the electricity generation and delivery infrastructure would involve integration of diverse, connected, interdependent and adaptive functions and applications to enhance grid reliability, improve capital and operational efficiency and ensure security of the electric grid. By combining various power generation and storage technologies with overlaid digital technology comprising of advanced sensing, control, communication and information processing, emergent intelligence distributed across various segments of the power grid will transform the grid to a highly interactive and adaptive system.

Today’s competitive market forces make utilities rely heavily on a robust business information environment that requires interconnections among the control and business information system domains, the external internet, and other peer organizations. Integrating operational information like equipment status, phasor measurements, distributed generation and storage status with business level information such as consumer preferences and energy usage and market pricing allows organizations to achieve higher end to end business and operational efficiency, reduce grid stress and improve overall enterprise productivity.

Historically, proprietary and intricate information exchange architecture ensured ‘security through obscurity’ provided secure means for data sharing, data acquisition, peer-to-peer data exchange, and other business operations between well separated corporate business system and control system domains. Security threats for such systems were mostly limited to physical access to the system. The power grid control information system is evolving from isolated clusters of computers running stand alone applications on a proprietary platform to a highly interconnected and interdependent system of local and wide area information and communication systems. Consequently, it is being exposed to new and emergent vulnerabilities and risks, very different in size, scope, likelihood and frequency of occurrence than what traditional system analysis would suggest.

The power grid operation systems have unique performance and reliability requirements. Often limited availability of computation and communication capabilities in legacy control system information platforms make repurposing security mitigations commonly effective in IT domain much more challenging for the power grid operation domain. Examples of such limitations include legacy Intelligent Electronic Devices (IED), the slow serial links through which communications among substations, control centers and field equipments take place and plain absence of security functionalities in control system communication protocols like Supervisory Control & Data Acquisition (SCADA) over Modbus or Distribution Network Protocol (DNP3).

Organizations rely on sound risk management frameworks to analyze and monitor different risk mitigation measures deployed for lowering vulnerabilities, deterring threats, minimizing the consequences of attacks, failures and errors, and expediting recovery. Without a formal and objective risk management framework, security control implementations often reduce to ad hoc decisions driven by guidelines and alerts issued by government agencies and third parties. While mature in several areas like finance, aviation, actuarial applications or even business information system, risk management for power grid control information system lacks standardized security metrics, objective risk analysis processes, historical vulnerability and threat data (anomaly in traffic, attack signatures and forensics etc.) that would enable domain specific statistical analysis and characterization of attack probabilities and risks.

Unified risk management approaches are critically needed to effectively guide resource allocations, identify best practices on the basis of practical and meaningful benchmarks and demonstrate various regulatory and business compliances for both the control systems and business domains. Such approaches need to provide frameworks which can consider all the interconnected vulnerabilities, different performance
requirements and security priorities of the various data and control flow through the entire information system without adversely impacting various performance requirements and implantation limitations of the smart grid.

II. IMPLICATIONS FOR SECURITY IMPLEMENTATIONS OF ICS AND IT SYSTEMS

A. Overview of IT and ICS Integration

Interconnection of a wide array of traditional and emerging utility business and operation information systems such as Energy Management System (EMS), Distribution Management System (DMS), Supervisory Control and Data Acquisition (SCADA), Market Management System (MMS), Advanced Metering Infrastructure (AMI), Customer Information System (CIS), Outage Management System (OMS) allows the utilities, customers and other service providers not only to monitor energy usage and grid status with higher precision and accuracy but also to analyze and activate distributed energy resources and storage options, construct pricing responses to appropriately reorient consumption patterns to balance available power generation capacity and demand continuously - all in real time. These activities require secure automated information exchange, analysis and intelligent decision making distributed throughout the grid. Adaptive orchestrations of situational awareness, decision intelligence and control activations will ensure that the convergent system operates much more efficiently with much less reserve capacity (spinning reserves) and suffering much lower energy losses over the power network while enhancing reliability and safety. As depicted in Figure 1, various power generation, transmission, distribution, customer energy management and business functionalities interact in such a system with increasing interdependence (sensing, measuring, consuming, processing, controlling), diversity in interconnections (e.g., remote monitoring and testing, synchrophasors, field devices and equipments, asset management, corporate analysis and decision systems) and adaptivity (in the ways control decisions dynamically interact and influence the entire sense-process-decide-control loop) – transforming the power system from a very complicated machine to a complex system.

The term Operations Technology (OT) in Fig. 1 refers to the ICS part of the power grid and in the remainder of the paper these two terms will be used interchangeably.

B. Unified Security for Distinctive Platforms

In the context of the power grid, security refers to the degree of protection accorded to the system from deliberate attacks, equipment failures, inadvertent errors, accidents or natural disaster. This includes both power and cyber system technologies and processes as applied to the enterprise IT and power system operations, governance, risk and compliance.

In view of the integration of the IT and OT information domains, unified and interoperable security solutions are essential to assure communication and information security among varied systems of different media and topologies found in the smart grid. A unified view of risk management is better placed to drive development and deployment of such solutions which will have account for domain specific and common requirements. Even though power operation systems are increasingly being designed and implemented using IT standard hardware and software platforms and network protocols to take advantage of efficiencies such common platforms provide, ICS needs to fulfill very different risks, priorities, performance and reliability requirements. Traditional enterprise IT-focused understanding of cyber security requires ensuring confidentiality, integrity, and availability of the electronic information and communication systems – in that order of priority. In contrast, for the power grid operation systems, priorities of the security objectives are availability first, followed by integrity and confidentiality.

Additionally, distinctions in operating environments for the IT and ICS systems, often preclude the same security implementation to be feasible across both domains. As an example, in most cases power operation systems cannot be easily restarted without adversely affecting power generation or delivery, thereby compromising high availability, reliability and maintainability requirements. Hence use of IT restoration measures like rebooting a component are usually not acceptable owing to such adverse impacts on requirements for the ICS. The following sub-sections and Table 1 describe how some of the special features and specific limitations of processing power, communication protocols safety, and operational environments deployed in the power system operation differ from the ones used in IT systems, thus presenting different implications for security implementations even when faced with common vulnerabilities and threat profiles.

1.) Computer and Communication Resources:

Many substations and distribution communication systems employ slow serial links for SCADA communications with control centers and distribution field equipments to support one of the most critical parts of power system operations – retrieval of status information and transmission of control commands, which are latency sensitive. Communication protocols like Inter Control Center Protocol (ICCP) or DNP3 currently in use do not offer any security protection for
integrity or confidentiality of such critical messages. Cryptographic protocols like Transport Layer Security (TLS) or Internet Protocol Security (IPSec) impose unduly large bandwidth overhead on such constrained communication channels. Neither do such legacy systems have adequate compute power, offload engine or memory to support cryptographic or protocol stack processing. Corporate IT systems, in contrast, are not generally constrained for communication or computing resources making encryption an often used security control to serve integrity and confidentiality requirements. Similar restrictions in power (battery, inactive modes), storage, and tamper possibility limit easy reuse of other security control implementations like key management in ICS.

<table>
<thead>
<tr>
<th>Security Characteristics</th>
<th>Control Systems</th>
<th>IT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Security</td>
<td>Less Secure when far flung, unmanned</td>
<td>Secure: Facility, Server room</td>
</tr>
<tr>
<td>Connection Speed</td>
<td>Slow serial link, 1200 baud and dial-up not uncommon</td>
<td>Fast broadband, T1 and above more common</td>
</tr>
<tr>
<td>Latency</td>
<td>Low. Substation IED communication for relays is multicast and &lt; 4 ms</td>
<td>Relatively high</td>
</tr>
<tr>
<td>Compute Power</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Availability</td>
<td>Need timely authorized access 24X7X365</td>
<td>Can tolerate some delay in access and availability</td>
</tr>
<tr>
<td>Integrity</td>
<td>Less assured</td>
<td>Assured</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Less salient</td>
<td>Preservation is critical</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Bona fide data source and provenance critical</td>
<td>Connection and information sharing could be ad hoc</td>
</tr>
<tr>
<td>Encryption key, digital certificate and signature</td>
<td>Server access and local memory limitations</td>
<td>Extensively used</td>
</tr>
<tr>
<td>Message Authentication Control</td>
<td>Resource limitations make it more relevant.</td>
<td>Stronger Authentication available</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Now prevalent for outage records. More prevalent in future with transactive smart grid</td>
<td>More rigorous</td>
</tr>
<tr>
<td>Attack signature</td>
<td>Sparsely available</td>
<td>Well characterized</td>
</tr>
<tr>
<td>Pattern and rules</td>
<td>Limited and useful</td>
<td>Diverse</td>
</tr>
<tr>
<td>Comm. protocols</td>
<td>DNP3, Modbus, IEC 61850, ICCP/TASE.2</td>
<td>TCP/IPv4 or IPv6</td>
</tr>
</tbody>
</table>

Table 1: Differences in security environments

2.) **Performance Requirements**: The time latency associated with information availability in ICS can vary from milliseconds (currently less than 4 milliseconds for protective relaying) through sub-seconds for transmission wide-area situational awareness monitoring to seconds for substation and distribution SCADA data to minutes for monitoring non-critical equipment and some market pricing information to hours for meter reading and longer term market pricing information and finally days/weeks/months for collecting long term data such as power quality information. IT systems, in contrast, are more concerned about high throughput, and they can typically withstand some level of delay and jitter.

3.) **Physical Interaction & Availability**: Power control systems can have complex interactions with physical environment (thermal, wind, sunshine, snowstorm etc.) and their consequences in the control domain can manifest in physical events like power outage or unsafe equipment failures. In a typical IT system, there is no physical interaction with the environment. They can be restarted without any impact to any critical physical process. For this reason, unlike IT systems, exhaustive pre-deployment testing for the security functions integrated into the ICS is essential to validate that they do not compromise normal ICS high availability requirements. Availability constraints like outages often must be planned well in advance for power systems operation; corresponding requirements are less demanding for corporate IT systems.

4.) **Domains of Varied Trust and Security Credentials**: In a unified system, information access often will happen across different organizational and functional domains (e.g., service providers, peers, backup facilities, customer premises gateways, SCADA) with their varied credentials and security levels. Convergence of IT and OT demands optimal coordination for scalable federated identity and trust management across varied environments (secured buildings housing IT systems, limited protection for customer premise meters and field devices).

5.) **Anomaly Detection**: Construction of a normative model of traffic pattern helps in accurate detections of anomalous events. Difference in degrees of “random” (not known a priori) traffic in IT and OT systems would imply that intrusion detection systems and attack signature analytics built with such models will have to take very different approaches.

C. **Leveraging Reliability To Serve Security**

Unified security analysis can offer opportunities to information security implementations by leveraging solutions the power system operations have been using for decades to manage the reliability of the power grid. Existing monitoring and response methods and technologies deployed to protect against inadvertent security problems, such as equipment failures, operational errors, and natural disasters can now be extended to include deliberate cyber attacks and security compromises resulting from the emerging convergence of IT and OT. Benefits flow the other way when additional security monitoring and analytics implemented against possible deliberate attacks can be used to improve safety, minimize
carelessness, and improve the efficiency of equipment maintenance.

III. UNIFIED SECURITY FOR EMERGING CONVERGENCE IN SMART GRID

Although the primary concern of the smart power grid security strategy is protection against deliberate attacks and various failures adversely affecting the grid, it also requires that a response and recovery strategy be developed in the event of a cyber attack on the electric system. Information security services like prevention (access control, authentication and authorization), detection (monitoring, traffic pattern and anomalies) and response (signature forensics, decision analysis, backup or redundancies for service continuity and restoration) could be integrated with existing and upgraded power system applications like fault location, isolation and restoration functionalities, credible contingency analysis methods [11](N-1, N-1-1 and others), grid stability management using SCADA, EMS etc. to address security requirements like availability, integrity, confidentiality, non-repudiation.

As the worlds of utility operations and utility IT gradually merge to promote corporate connectivity, drive down total cost of information system ownership and facilitate remote access capabilities, they both are increasingly adopting common architectural approaches and are being designed and implemented using industry standard hardware, operating systems and network protocols. This trend ensures that the combined system will be able to use a unified risk management framework and consistent risk analysis tools in areas of security and reliability of the overall smart grid, enabling cost-effective resiliency of the power systems in events of various attacks and failures, as well as leveraging traditional power industry restoration measures as described earlier.

Although the overall risk management strategy for the smart power grid needs to examine both domain-specific and common requirements, a unified risk model would benefit from a correlated view of IT security and OT reliability consequences based on unified event detection models that use power system and IT data communication system factors in a cross correlated manner. Such models would need deep contextual understanding of the various operational and business process interdependencies in the smart grid as well as the required information flow, communication protocols and performance imperatives. Wide area security event detection and response systems needed to secure the smart grid end to end will need to share event data across jurisdictional and organizational boundaries securely and interoperably. Reliability and security analytics along with decision intelligence distributed across the grid are expected to analyze such events, predict correlated consequences and provide intelligent, systematic, and coordinated responses on a real-time basis.

A. Information & Decision Coordination across IT and ICS

Figure 2 shows how key components of the smart grid control system interact with one another across several scales and other utility systems through various hierarchical and peer level connections. The convergence of utility OT and IT systems extends such interconnections to corporate and other external information systems as already seen in Fig. 1.

In such coupled systems, advanced sensors and meters would continuously collect energy consumption data, weather data, equipment conditions, thermal, voltage, frequency and phasor data at various points on the grid along with other local and wide area situational awareness. Operating continuously at supervisory and lower levels in the order of minutes to milliseconds (possibly even faster in the future), various control loops shown in Fig. 2 transmit measurement variables from the sensors to the controllers for each relevant change. The controller interprets the information and generates corresponding control signals that it passes on to the actuators. Depending on the types and magnitudes of such changes and the relevant responses, such interactions and co-ordinations can take place among neighborly service points or across the entire grid spanning many substations, control centers and regional systems. The Human Machine Interface (HMI) allows operations engineers to configure set-points, control algorithms and other parameters in the controller as well as provides visualization of status information, including malfunction and event notifications and alarms. With the expected rise in variations and volumes of information exchange among various components of the smart power grid control system including control centers, substations, supervisory controls, HMI, synchrophasors, field equipments, and various business applications, most decisions will need to
be made in almost real time to respond to security, reliability, efficiency and other business and operational exigencies. Automated decision making distributed throughout the grid in the forms of intelligent EMS at customer premises, DMS and EMS at utility locations, and utility enterprise systems like Asset Management (AM), Work management (WM), Customer Information Systems (CIS) would coordinate the consumption patterns and preferences of the consumers with real-time conditions like market prices, intermittencies of various distributed generation and storage resources and grid stress. Customer premise appliances may use the local and grid wide information to interact autonomously with the grid to determine the charging and discharging cycles of various industrial, commercial and residential appliances and electric transports to dynamically balance load and resources, maximize energy delivery efficiency and grid reliability in real time.

B. Self Similarity And Self-Organized Criticality

Interestingly, analysis of the power grid communication and control structures in Fig. 2 reveals it to be self-similar, that is it looks "roughly" the same on any scale – be it at the transmission and distribution level or below the meter customer premise networks. In particular, it can be shown that the “smartness” of the power grid will emerge as the outcome of a number of processes that evolve at various scales like EMS, DMS, Demand Response (DR), EMS at customer locations, Distributed Energy Resources (DER) along with various reliability and security services distributed across the entire grid. A striking consequence of this scale invariance is that the structure of the grid, at least in some segments, is “fractal”—cohesive sub regions displaying the same characteristics as the grid at large. An exploration of this underlying fractal nature will therefore be helpful to designing security services across multiple domains and scales.

Large scale power grid outages like the August 2003 North East blackout [8] or the November 2006 European blackout display many of the characteristic properties of complex systems which exhibit adherence to a power law distribution in their failure probability versus event size. Part of this behavior arises out of different parts of the systems interacting in both space and time [9]. Each service point in Fig. 2 following its own processes, procedures and terminology could potentially achieve uncoordinated local optimization, potentially bringing about grid-wide cascading events. Steadily increasing load and economics of utility business often compels organizations to run the electric power transmission networks near their operational limits. When distributed generation and storage resources of various capacities and intermittencies are interconnected with such systems, prevalent practices of operating these diverse and interconnected systems much closer to their maximum capacity might lead to magnified effects of random, unavoidable perturbations due to deliberate attacks, operational mistakes or weather events. This power law behavior suggests that conventional risk analysis does not apply to these systems.

IV. RISK MANAGEMENT

A. Risk & Vulnerabilities

In view of the evolving and emergent nature of the vulnerabilities and risks facing the smart power grid operations and IT systems, appropriate risk management frameworks and security blueprints need to be implemented to secure the overall power grid system against deliberate attacks, equipment failures, inadvertent errors or natural disasters. Risk management provides organizations the ability to correlate resource and information value to security and safety need, record business and engineering assumptions and dependencies, analyze technological and other uncertainty. Objective risk assessment methodologies are predicated upon quantification of security management by modeling assets to be protected and their damage scenarios, the threat (attack) agents of concern and their attack scenarios and the risk mitigation countermeasures.

To control the risks of developing and operating an IT or an OT system, organizations need to know the vulnerabilities of the system and the threats that may exploit them. Adequate knowledge of the threat environment allows the security personnel to implement the most cost-effective security measures. In some cases, managers may find it more cost-effective to simply tolerate the expected losses. Such decisions should be based on the results of a prudent risk analysis.

In order to provide a reliable way of estimating risk to decide how much security is needed at any location on the smart grid, a risk assessment methodology which can systematically evaluate the likelihood of an adverse effect arising from security exposure has to be constructed and refined on an ongoing basis to assess risks at that point of time for various types of assets, services, critical functionalities with appropriate considerations to their interactions and needed performance. Security properties of control and IT systems today are typically assessed through individual expertise based human evaluation. In order to improve the integrity, repeatability and timeliness of security measurements, it can be argued that we need to reduce reliance on such human elements and eliminate the inherent subjectivity they bring.

B. Risk Management Process Framework

A risk management framework for Critical Infrastructure/Key Resources (CI/KR) as described by NIPP [10] has been combined with a typical enterprise business risk management framework in Fig. 3, presenting a unified framework for physical, cyber, human and organizational aspects in both IT and OT domains. This combined framework demands interactive, step-wise refinements on an ongoing basis to reduce the overall smart grid informational risks. Such unified risk management approach calls for a coordinated assessment of cyber and power grid risks keeping the overall smart grid security goals in mind.

The management process comprises of the steps shown in Fig 3 and enumerated below.

- Risk Identification including threat characterization;
- Risk Analysis including vulnerability analysis;
• Risk Planning including level of risk acceptance while allowing for uncertainties;
• Risk Prioritization based on business goals and objectives, both short-term and long-term;
• Risk Tracking by periodically checking how well we are doing on a given risk item;
• Risk Control & Monitoring including deployment/enforcement of countermeasures and application of abatement and mitigation strategies for each identified risk event on a periodic basis;
• Risk Communication dealing with risk event communication to the top management, the external stakeholders and internal organization. Utilities have established specialist departments for media communication that also take the onus of communication of risk events when risks mature.
• Risk Documentation usually records risk events, and risk responses deployed.

Traditionally, risks are identified in IT domain using nomenclatures like software development risk taxonomy from SEI [12]. Similar identification, analysis and prioritization methodologies could be followed for other IT & OT systems, although the risks there would involve different vulnerabilities, consequences and solutions.

Interconnections of domains warrants considerations of rich variety of dynamic and structural interactions in terms of realizable vulnerabilities and threat likelihoods associated with each part. This is due to emergence of newer and hitherto unknown vulnerabilities through such interactions. Attack paths to known but dormant vulnerabilities in one domain may become realizable attack paths as shown in the risk assessment subsection below.

Furthermore, a unified risk analysis and assessment model is much more complex than the separate models for the traditional risk analysis and risk assessment of IT and OT systems respectively. Unified risk planning and risk prioritization calls for adopting efficient risk strategies while balancing the respective goals of the IT and OT systems as well as the bigger goals of the organization and the grid itself. During the unified risk planning phase, organizations need to determine their level of risk acceptance while allowing for enough resources for contingencies. Unified risk prioritization techniques should help to plan and prioritize for both short term and long term risks for the IT system or OT system risks or a combination of these. Unified risk monitoring & control needs greater collaboration, coordination and cooperation among the neighboring entities involved. Unified risk communication becomes more complicated due to language and terminology issues across the grid, more so when end customer is a stakeholder. Unified risk management calls for a common but federated risk repository where all risks, encountered or perceived, by utilities and customers are stored to help them in reassessment of existing risks, better choice of risk strategies and planning for contingencies.

Organizations like NERC and US-CERT maintain federated repositories of risk events and security incidents needs to facilitate on-demand interfaces with new automated unified risk tools so that utilities using such new risk tools will benefit from the lessons learned out of the risk events or incidents archived in such repositories. On an ongoing basis, utilities also need to report to these organizations on risk events and security incidents through bidirectional information exchange with various oversight agencies (FERC, NERC, US-CERT, NIPPP), thereby enriching these federated repositories.

Methods & tools have been developed to manage various aspects (steps) of risk management. These include Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA), Failure Mode, Effect & Criticality Analysis (FMECA), etc. Some traditional tools that have helped in risk management practice are risk charts, risk matrices, risk maps, risk forms & templates, risk registers and databases. Automated tools to manage all aspects (steps) of risk management are critically needed.

Risk management process must facilitate sound decision making. The level of security impact or equivalently the level of acceptable risk is a policy decision. Since threats cannot be eliminated altogether, the process must focus on vulnerabilities and countermeasures. Vulnerabilities are design and operational issues that are better addressed during the System Development and Operations Life Cycle (SDOLC) phases presented in later sections.

C. Unified Risk Management & Risk Strategies

As we have already seen for the utility IT systems, data exchanges among applications dealing with market, partner, customer and enterprise information are the primary security concerns, making confidentiality and integrity of such data as security priorities. For the utility control system however, fault tolerance, resiliency to prevent loss of mission critical services, regulatory compliance, loss of equipment, lost or damaged products are the priorities, implying protection against unauthorized denial of timely information access or unauthorized information modification are the concerns. As a result, while confidentiality, integrity and availability are the order of priority for the business IT system, availability, integrity and confidentiality are generally the prioritization order for a control system. A unified risk management approach lets organizations evaluate risks and protection measures across both domains (which often can be highly correlated) for all its assets using a common principle.

“Keeping the lights on”, implying continuous availability of electric power is the primary goal for the power sector. In view of increasing reliance of the power system operations on the information infrastructure, there is a need to better integrate the cyber and power system views, particularly in regards to...
intrusion detection, unauthorized access, and incorrect configurations. It is also quite important to anticipate impacts of cyber and power system security incidents and formulating an appropriate and systematic response.

Countermeasures or risk response actions are less characteristic of systems than of their environments and the ways in which they are used. Typically, to make any asset less vulnerable raises its cost, not just in the design and development phase but also due to more extensive validation and testing to ensure the functionality and utility of security features, and in the application of countermeasures during the operation and maintenance phase as well.

Risk strategies help only when a risk is timely identified. These strategies work efficiently for a risk from whatever little is known to surmounting the unknown and uncertain elements that make the entire risk.

Risk strategies are effective when used properly and are applicable either separately for OT system risk management or IT risk management or in the unified risk management scenario. More than one risk strategy may be applicable in a given situation. The security analyst must observe and execute the risk strategy that best fits the purpose and situation the most and in a timely manner. Any single strategy may turn out to be inadequate. For instance, passive acceptance may bring in more consequences than originally expected. Over time, risks have the capability to grow and become the biggest risk on hand. If risks are not dealt with on a timely basis, risk strategies will become ineffective. Table 2 shows some risk strategies that are effective when used in a carefully selected combination.

<table>
<thead>
<tr>
<th>Risk Strategies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Avoidance</td>
<td>Take an alternative approach and re-assess risk, document &amp; communicate to stakeholders</td>
</tr>
<tr>
<td>Risk Acceptance</td>
<td>Accept the risk. Passive: Accept consequences. Active: Prepare Contingency Plan and re-assess risk, document &amp; communicate to stakeholders</td>
</tr>
<tr>
<td>Risk Mitigation</td>
<td>Apply countermeasures to reduce the risk while monitoring and re-assessing the risk on an ongoing basis. Document &amp; communicate to stakeholders</td>
</tr>
<tr>
<td>Risk Transference</td>
<td>Transfer the risk with a deliberate intent. Re-assess risk, document &amp; communicate to stakeholders</td>
</tr>
<tr>
<td>Contingency Plans &amp; Workarounds</td>
<td>Workaround are short-term risk response actions. These are wish-list items for long-term solutions. Contingency plans are planned risk responses for short term or long term.</td>
</tr>
</tbody>
</table>

Table 2: Effective Risk Strategies

D. Security Blueprint

The security foundation component of the security blueprint shown in Fig 3, presents a unified context for threat & vulnerability management, identity management, application integrity management, systems and network infrastructure, physical and environmental security, risk metrics formulation and measurement, Information assets management, infrastructure blueprint, business continuity planning, logging, monitoring & reporting.

Strategic drivers like risk management and legal and regulatory requirements influence the security foundation on an ongoing basis along with process and business enablement functions. As newer methods and technologies emerge the strategic drivers and security foundations dynamically realign the organization to combat newer and hitherto unknown (zero-day) threats and vulnerabilities.

E. Risk Assessment

In order to provide a reliable way of estimating risk to decide how much security control is needed to adequately and adaptively protect any smart grid system, a risk assessment methodology has to be constructed and refined on an ongoing basis to assess risks at different points of time for various types of assets, services and critical functionalities at needed performance. Also, increasing integration of the utility operational control and enterprise business information requires that the risk assessment methodologies consider the overall risk of the entire information system.

The process of risk assessment describes and qualifies the risks associated with structural and interactive vulnerabilities, threat profiles, and control measures and refers to the systematic evaluation of the likelihood of an adverse impact on the business. Interconnections of domains are likely to create new vulnerabilities combining weaknesses which were innocuous when unconnected. Protocol vulnerabilities in plaintext SCADA messages were “secured” through isolation and obscurity of the power operation system technologies.
Vulnerabilities in IT and external systems communication channels and protocols now offer threats like Man-in-the-middle (MITM) attack a realizable path to this SCADA vulnerability, potentially spoofing the control center with false grid state information and ultimately leading to large-scale grid failure.

1.) Qualitative & Quantitative Approaches:
Qualitative risk assessment is performed when the organization requires a risk assessment to be performed in a relatively short time, meet a small budget, when significant quantity of relevant data is not available, or the agents performing the assessment don’t have the sophisticated mathematical and risk assessment expertise required.

Quantitative approaches use mathematical calculations based on security metrics on the asset (system or application), thus ensuring consistent evaluations of parameters like threats, vulnerabilities, consequences of incidences to assets and effectiveness of countermeasures and their interrelations.

Risk is defined as the probability of a threat agent exploiting a vulnerability to cause harm to a computer, network, system, or organization, and the resulting operational and business consequences. As explained in the following subsection on threat and vulnerability modeling, vulnerabilities arise from defects or exploitable weaknesses introduced during design and operation life cycle of the IT and OT assets, their operating environments and usage models. Quantification of attack probabilities from different threat agents is a difficult task especially in view of absence of large scale data correlating prior attacks from them and vulnerability paths (static and dynamic) exploited by them. Similarly, quantifying the role of a particular threat, or an identified vulnerability in a threat model, defining the form of the attack, as well as their interactions in a given scenario in the overall risk assessment of the IT and OT systems is also extremely challenging.

The following equations attempt to characterize and correlate different elements of the risk in both IT and OT domains. Risk is a function evaluating consequences of threats exploiting vulnerabilities against assets and traditionally expressed as

\[
Risk = \sum_{\text{threat profile}} Pr_{\text{attack}} \cdot C
\]

where \( Pr_{\text{attack}} \) is the likelihood of attack resulting in consequence \( C \) of loss of assets being protected. Analysis of loss consequence shows a single large event with large loss is perceived to be of greater consequence than numerous small events creating the same loss, meriting a refinement to equation (1) as follows, where \( \gamma \) is >1 accounting for this non-linearity.

\[
Risk = \sum_{\text{threat profile}} Pr_{\text{attack}} \cdot C^\gamma
\]

Deploying security countermeasures, the residual risk can generally be brought down as expressed by equation (3)

\[
R = (1 - SC_{\text{Effectiveness}}) \cdot \sum_{\text{attack types}} Pr_{\text{attack}} \cdot C^\gamma
\]

Where \( R \) is the risk, \( Pr_{\text{attack}} \) is the likelihood of adversary attack, \( SC_{\text{Effectiveness}} \) is security control effectiveness and 1 - \( SC_{\text{Effectiveness}} \) measures lack of security mitigation and hence adversary success, \( C \) is consequence of loss of the asset. The consequence \( C \) depends on the value of the target attacked. Security countermeasures abate the danger and as equation (3) shows, greater the countermeasures lesser the risk. Resource allocation to risk abatement and mitigation, therefore, depends on the consequence [1].

Both \( SC_{\text{Effectiveness}} \) and \( Pr_{\text{attack}} \) are dimensionless. Risk \( R \) and consequence \( C \) have same dimensions – often expressed in monetary terms like dollar value. It is interesting to note that in equation 1 above, \( R \) is expressing residual risk and if \( SC_{\text{Effectiveness}} \) is set to 0, indicating absence of effective security measures, equation 1 reduces to classical linear risk equation expressing total risk. Because of evolving nature of threats and complexities of the control and IT systems, not only \( SC_{\text{Effectiveness}} \) is always expected to be in the range [0, 1), neither numerator nor denominator will ever become constant in the following equation clearly defining \( SC_{\text{Effectiveness}} \).

\[
SC_{\text{Effective}} = \frac{R_{\text{mitigated}}}{R_{\text{total}}}
\]

Notionally, a non-linear function \( g_1 \) could be constructed to capture the quantification of interrelationship between vulnerability \( V1 \) and threat \( T1 \) for different use cases, and systems. However, vulnerabilities without threats to eventuate them are not considered to be contributing to risk. The same goes for threats with no known vulnerabilities to exploit them. In both cases, the \( g_1 \) term and consequently the risks due to such threats reduce to zero. Equations (5) and (6) are not strict mathematical formulae but can be used as a schematic for considering the factors that enter into risk management and their interactions in a given situation.

\[
Risk \ R_i = f_1(g_1(V1, T1), C_1)
\]

Extending the notion to compose overall risks for larger and unified systems, we could construct a non-linear composition function which would capture two component risks, their weighted contributions (\( \alpha, \beta \)) and power indices (\( \gamma, \mu \))

\[
\text{Unified Risk}, \quad R_{\text{unified}} = F(\alpha R_1^\gamma, \beta R_2^\mu)
\]

F. Threat and Vulnerability modeling

It follows that a threat model, defining the form of the attacks of concern, is necessary for the concept of security to be operationally useful. Analysis of the threat environment, which really is the entire operational environment of the system, assumes not only accurate knowledge of the power grid structure and system interactions or the topology and communication between the interconnected operational and business information but also the physical, regulatory and external environments with which the system interacts. Absence of formal system description of perturbation profiles of the coupled systems and lack of historical data on distribution, duration and magnitude of such threats for the grid operational information systems make such analysis very challenging and complicated. However, threat models express our understanding of the threat environment and enable the development of countermeasures.
It is assumed that the target of attack is an asset (equipment, functionality, service, reputation etc.) associated with the power or information system and which the system is responsible for protecting (possibly in collaboration with other systems). The required degree of protection is determined by the assets to be protected, the damage and recovery costs associated with successful attacks on them and the risk tolerance of the stakeholders. In many cases, the system will have some other primary purpose and security is a constraint that may have to be traded with other performances. In case of the power system, security and safety properties are somewhat coupled – a security breach may compromise system safety.

The capability and motivation factors of threat agents like capital and technology access, cultural background, financial situation, education level, susceptibility to dogma, etc along with the catalysts that enhance capability and motivation factors determine eventuation of potential vulnerabilities.

### Table 3 Threat Profile

<table>
<thead>
<tr>
<th>Threat (STRIDE Model)</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>A person or program masquerades as another thereby gaining undue and illegitimate advantage.</td>
</tr>
<tr>
<td>Tampering</td>
<td>Intentional modification of the product so as to cause harm to the user or organization or community.</td>
</tr>
<tr>
<td>Repudiation</td>
<td>To refute the validity of a statement or contract or service level agreement.</td>
</tr>
<tr>
<td>Information Disclosure (Privacy breach or data leak)</td>
<td>Intentionally or otherwise disclosing the information to those who should not know that information.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>An attempt to make the resource unavailable to the intended users.</td>
</tr>
<tr>
<td>Elevation of Authority or Privilege</td>
<td>The scope of threat increases for a higher role user access/privileges.</td>
</tr>
</tbody>
</table>

Fig 4 Security Threat & Vulnerability Modeling

The capability and motivation factors of threat agents like capital and technology access, cultural background, financial situation, education level, susceptibility to dogma, etc along with the catalysts that enhance capability and motivation factors determine eventuation of potential vulnerabilities.

### Table 4 Vulnerability Classification

<table>
<thead>
<tr>
<th>Vulnerability Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage potential</td>
<td>The potential damage vulnerability may cause to the system (e.g., a software bug is a vulnerability. Depending on its criticality, severity and degree of participation, its damage potential may vary.</td>
</tr>
<tr>
<td>Reproducibility</td>
<td>Vulnerability may be classified as either reproducible or non-reproducible.</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Exploitability refers to how much effort is needed to launch the attack using the vulnerability.</td>
</tr>
<tr>
<td>Affected Community</td>
<td>Size and scope of the affected community.</td>
</tr>
<tr>
<td>Discoverability</td>
<td>Ease of discovering the threats associated with the vulnerability.</td>
</tr>
</tbody>
</table>

G. System Development & Operation Life-Cycle (SDOLC)

As explained before, threat analysis will determine or even improve the organizational security policy that in turn establishes the security system development and operational strategy. Security must be incorporated into the design right from the initiation phase of system development/sourcing lifecycle. NIST standard recommends that a sensitivity assessment is done during this phase. A sensitivity assessment looks at both the importance of the data to the system processes and the system itself and expresses the result in terms of the Integrity, Availability and Confidentiality aspects. During the development/sourcing phases, the security requirements are determined & documented in the requirements specifications document and known risks are assessed. The identified security controls are implemented through either a buy or build decision while considering other related security aspects associated with the decision. During the development and implementation phases, the security controls are developed in such a way that these can be calibrated adaptively as needed so that extensive security testing can be done with varying degrees of security measures controlling the core functionality and performance of the system. Once the security testing is completed in varying operating environments the system is certified as security are inhibitors (providing counter-incentives) and amplifiers (enabling attacks). Fig. 4 shows an interaction model of the security threats, vulnerabilities and risk mitigations in the context of the smart grid operating environment.

Defects introduced during the system development or testing phase contributes to potential vulnerabilities. Hence improving the general quality of product development contributes to improved security. Similarly defects in operating environments of the power system give rise to reliability and safety vulnerabilities. Security risks arise from a combination of the presence of an attacker, an attack goal, vulnerability in the system and the consequence of a successful attack. Formal risk management processes enable prioritization of defects from a system security perspective. Table 3 and Table 4 below present some common security threats and system vulnerabilities respectively.
compliant. Systems need to be configured for appropriate security enablement before deployment.

Once the system is operational, ongoing risk assessments may determine newer vulnerabilities requiring new security controls, in turn warranting a fresh round of security testing and certification. For such reasons, throughout the system development and operational lifecycle a “live” security plan must be maintained and strictly adhered to [7].

V. CONCLUSIONS

Business imperatives are driving interconnection of power grid IT & ICS systems. Unified methodologies for automated risk management will comprehensively enhance the security and reliability aspects of the convergent smart grid information exchange system. Increasing dynamism from sources like distributed generation intermittencies and demand response is expected to transform the smart grid operational behavior. Since threats and vulnerabilities to existing and emergent smart grid functionalities are continuously evolving, automated and adaptive methodologies and tools with adequate configurability and extensibility to accommodate such changes are better placed to make such frameworks robust. Such tools generally ensure access to decision support artifacts offered by automated systems and can enormously improve the integrity of the risk management system by reducing the subjective human interpretations that still exist.

In addition to extended investigations of the quantitative approaches and associated schema discussed in this paper, further research is needed to develop tools based on unified models, methods, and technologies for risk and security that provide a correlated view of power system and cyber impacts. These tools would:

a.) Provide for newer grid simulation tools and techniques that incorporate device communication and modeling for transmission and distribution segments and improve upon the existing grid simulations so as to integrate cyber components and study their interactions.

b.) Enhance response & containment strategies

c.) Interoperate and securely share data across an organization as well as other utility enterprise organizations while allowing for intelligent, real-time systematic and coordinated responses

d.) Unify intrusion detection/prevention systems and provide deeper contextual understanding of the smart grid and its interdependencies

e.) Include security and reliability analytics providing for event and impact prediction and infrastructure resiliency improvement.

VI. ACKNOWLEDGEMENT

The authors wish to acknowledge the various sources of information, suggestions and guidance that came from the power grid and security community. If any reference has not been adequately acknowledged, the oversight is unintended. Finally the authors would like to thank the members of the IEEE P2030 information technology task force for providing their valuable feedback to this paper.

VII. REFERENCES


VIII. VITA

Partha Datta Ray (M ‘89) is Chief Technology Officer of Albeado Inc. He has served in multiple technology executive roles in the past including Vice President of Engineering at GDA Technologies, Terablane (acquired by Agere/LSI), LSI Logic, Silicon Compiler/Mentor Graphics and at AT&T Bell Labs (communications research). He holds a BSEE and MSCS from Rutgers and has conducted advanced research works at leading institutes. He currently leads the Information Security Sub Group of IEEE P2030 Standards Committee and has led other trade and standards groups in the past.

Rajgopal Harnoor (M ’98) is a PMP certified Project Manager with ABB Inc focusing on MMS and OS. He has Masters Degree in Software Engineering and Masters Degree in Computer Applications. He is a member of the Security Sub Group of IEEE P2030 Standards Committee.

Mariana Hentea is currently authoring a book on information security and her research focus is computer and network security including control system security. She has worked at AT&T, Lucent in various R&D and systems engineering capacity where she worked with VoIP and wireless telecommunications. She received her MS and PhD in computer science from Illinois Institute of Technology and is a certified CISSP from ISC. She is a member of the Security Sub Group of IEEE P2030 Standards Committee.