Improving ROI on Big Data through Formal Security and Efficiency Risk Management for interoperating OT and IT systems

Partha Datta Ray, Christopher Reed, Jeff Gray, Atul Agarwal, Suresh Seth

Albeado, Inc.
18640 Casa Blanca Lane, Saratoga, CA 95070
partha.dattaray@albeado.com

Keywords: Smart Grid Systemic Security ROI, Business Risk Management using Utility Big Data, Enterprise Business Process and Information Security, Big Data Risk Intelligence and Compliance

Abstract

A plethora of innovative solutions to combat signature less, camouflaged and evolving attacks are joining the arsenals of existing intrusion and malware protection systems. However, in order to implement the vision of enormous economic and social value creation the smart grid has promised to usher in, robustness, resilience and reliability of the power systems will need to be enhanced while the grid becomes more interconnected and complex. A paradigm shift is needed in the cyber security approaches and architectures to protect the smart grid against complexity induced malfunctions, inadvertent errors, evolving attacks, and more frequent and more severe natural disasters. In order to deliver systemic and holistic grid security and reliability, performance and security properties of Operational Technology (OT) systems where low latency and high availability machine to machine communication predominate, need to interoperate with those of IT systems where privacy and confidentiality of human to machine interactions are higher security priorities.

Given the huge volume, variation and velocity of situational information a Smart Grid decision control system will increasingly need to process, human insights and control actions can play only limited roles in monitoring and control of the grid. Manual analysis and control measures will need to be supplemented by automated correlation and analysis of such diverse and massive amount of information. A Formal Risk Management system will be needed to make the analysis of such Big Data manageable, scalable, and effective by prioritizing inputs to the processes which are found to be more relevant and consequential. Such formal frameworks, as one presented in this paper, will also warrant improved metrics and enhanced measurement precision to formally establish Return-On-Investment (ROI) analysis of different security solutions, provide greater understanding of an enterprise's business process security, safety, and reliability risks and leverages this understanding to optimize business outcome and security.

1. INTRODUCTION

The electric power grid has been one of the most significant forces of social and economic value creation for more than a century now. But a new vision of information driven modernization of the electricity generation and delivery systems is ushering in fundamental changes in ways electricity is consumed, produced, priced and managed. As we start building out one of the most complex networked infrastructure in the world combining a continental-scale power network with an extended network of sensors, controllers, meters, and other field devices, overlaid by an internet like information system network, the Smart Grid is expected to enhance grid reliability, improve business efficiency and increase security of the electric grid [1, 2] through a set of new information monitoring, analysis and control actuation capabilities. Integrated data flow between the power grid and the business IT systems are enabling innovative business cases such as reliable integration of diverse renewable and storage options to the predominantly bulk power grid, market creation for newly imagined electricity trades and consumer services [3], two way customer participation in load management through novel Demand Response (DR) incentives, and enhancement of systemic cyber security risk management [4] of the power systems infrastructure, applications and services. These foundational improvements of services are only the beginning of a growth trajectory for the utility industry which is both challenging in ways that it will warrant different imaginations on business cases and usage models, but also exciting and inspiring in realizing the unprecedented value creation potential this networked system of systems offers.

Such imperatives along with today's competitive business and economic forces are making utilities rely heavily on a

robust business information environment that requires interconnections among the power system control and business domains, the external internet, suppliers and other peer organizations. Integrating operational information like load conditions, equipment and asset status, synchrophasor data, distributed generation and volt-VAR control information with business level information such as consumer preferences, real time load and trend, market prices, asset maintenance schedule, *etc*., allows organizations to improve overall enterprise productivity through higher end to end business and operational efficiency analysis while reducing grid stress and vulnerability.

The power grid OT system as a result is evolving from relatively isolated clusters of computers running stand alone monitoring and control applications on a proprietary platform to a highly interconnected and interdependent system of local and wide area information driven decision intelligence and control systems. Consequently, it is being exposed to new and emergent vulnerabilities and risks which are very different in size, scope, likelihood and frequency of occurrence than what traditional systems of risk analysis would predict.

Current risk management methods are inherently informal, based on subjective perceptions of risk. Security and risk properties of OT and IT systems today are typically assessed through sub-domain specific expertise of individuals. These *ad hoc* decisions are based on personal experience, as well as guidelines and alerts issued by government agencies and third parties. They are unable to consider the numerous complex relationships between all the relevant security and risk concepts in a systemic fashion. The result is a non-holistic and fragmented OT and IT security and risk management approach which becomes less and less effective as system connectivity and complexity increases.

Additionally, increasing flexibility of business processes and rising integration of OT and IT systems require continuous risk assessment which cannot be satisfied by the response time of existing methods. To improve the integrity, repeatability, effectiveness, and timeliness of security and business risk analysis from various sources, reliance on formal and automated methods is required.

Although IT organizations are responsible for protecting the IT and OT systems, it is difficult for the enterprises to get a clear picture of security and operational postures without a formal risk analysis. While IT staff may be competent in implementing security tools, they often do not have the expertise in business or operational modeling of domains such as power systems, or financial systems and attendant risk management.
Lack of automated processes is hindering wider adoption of enterprise wide security and business risk management, and is exposing the enterprises to disruptive risk events. Automated risk management applied on more frequent collection, collation, and correlation of varied types of data from diverse sources would enable physical and historical statistical analysis, creative correlation methods and other refinements to improve estimated risk and infer effective control measures. They evaluate impact of threats on various assets deployed to support the myriad business processes on which the enterprise business functions are built, and enable mitigation measures such as self healing of the system through dynamic reconfiguration to achieve heightened security, improved efficiency and enhanced compliance.

The following sections describe how a Return On Investment (ROI) guided automated Risk management system can make the processes scalable in the face of the Big data onslaught the utilities are facing as they are integrating their OT and IT systems with different security needs (e.g., availability and integrity in OT, privacy and confidentiality in IT) and performance characteristics (such as low latency machine to machine conversations with real time analysis and control predominant in OT compared to higher throughput and wider accessibility of human to machine interactions in IT).

By prioritizing the Big data inputs for relevance and consequence such system can provide compelling scalability. Yet they can deliver very effective outcome for holistic security because of the business functions, process and systemic data flow context. And best yet, such systems can leverage this monitoring and analysis systems to deliver improvement in efficiency and enhancement of operational compliance at the business function levels of the organization.

Finally, by interoperating existing point, perimeter and defense-in-depth security solutions with actionable insights from such systemic security risk management, the industry can finally deliver a powerful combination of values to customers, thus making a compelling business case for serious consideration for systemic treatment of security risks.

2. SYSTEMIC APPROACH TO SMART GRID CYBER SECURITY RISK: AN OVERVIEW

Businesses invest billions of dollars each year on applications security, firewalls and antivirus software in an attempt to ward off attackers and yet, even “security solutions” vendors and agencies entrusted with implementing national security struggle to protect themselves from intrusion and malware as has been seen time and again. The crux of the problem is that organizations have taken a piecemeal approach to security. Firewalls are used to keep the bad guys out, antivirus

software is deployed to weed out malware but none of these systems communicate with each other in a systemic fashion to gain holistic intelligence. When meaningful patterns of attack do emerge, it's often too late — trade secrets are long gone or customers' confidential data has already been compromised.

As has been seen already, ubiquitous deployment of IT systems, as well as business and regulatory demands on power utilities are driving integration of operational technology (OT) domains with information technology (IT) assets and services. Improved delivery of smart customer services such as outage event intelligence, efficient integration of renewable sources, customer energy consumption analysis and control in real time, increased coordination of business activities in interlinked utility domains - all depend critically on robust and widespread IT systems and services. Increasing interactions among various IT systems within and between enterprises, however, allows new types of risks to emerge and allows risks from one domain to reach others.

These emergent and cross system risks allow adverse impacts to propagate from one system to others, requiring coordination among OT and IT systems to prevent and mitigate such events. In both domains, a malfunction of IT can cause persistent business failure within a very short time. This in turn increases the importance of cyber security and business information risk management for utility enterprises and critical infrastructures which increasingly are being driven by business and regulatory compliance demands.

Without a formal and objective assessment of the economic significance of information security risk of the OT and IT systems, investment decisions for their security management lacks the rigor and transparency of a quantitative ROI analysis, thereby making such investments fragmented, poorly positioned and ultimately inadequate. From a value-oriented perspective, IT and OT risk can be seen as a part of operational risks measuring the unexpected losses that can be quantified by the frequency and extent of losses. In this contribution, we not only examine limitations of current security solutions and outline methods and approaches which enhance systemic security, we also present a formal value based ROI analysis model through prioritization of value at risk.

Organizations need to evaluate implementation cost of security measures against the risk that a business process will have unacceptable adverse impact if a specific vulnerability is exploited by a particular threat. Informed business process security and information security investment decisions however will need analysis of cost, benefit, performance, timeline, risk and other tradeoffs. Decision intelligence models for investment options relating to business process security and information security in an integrated OT and IT system which include web-based, service-oriented environment are explored in later sections, where methods for evaluating operational, economic and performance implications are also considered.

With the speed and complexity of the threat landscape constantly evolving and the prevalence of combined and persistent threats, organizations need to start being predictive, preventative, and proactive about their security risk management. Rather than drowning in data, Big data based risk analysis, combined with a ROI analysis prioritizing information assets to protect and business processes to analyze for anomaly can achieve significant scalability and effectiveness. With such systemic approaches for creatively containing data deluge, information and business process security functions can gain a comprehensive, in-depth view of risks, both internal and external, and also tap into analytical capabilities such as fraud detection (unauthorized diversion of power, meter tampering, etc.) and customer data correlation (demography, location, weather, historical trend, economic situation, etc.) leading to improved information security and better cyber resilience.

3. INTEROPERABLE AND COMPLIMENTARY: ANALYTICAL CONTEXTS OF OSI AND GWAC STACKS

As Utility Business Information Technology (IT) and Power System Operation Technologies (OT) integrate more, security control solutions are also evolving to address the emerging interconnected vulnerabilities and threats. Unified IT and OT security risk analysis and control systems will need to interoperate with traditional security measures which are often point or perimeter solutions applied to each target system - be they host computers, networks or applications. Currently these methods (e.g., Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), end point device security, firewall protection of LAN) usually lack the systemic awareness needed to analyze events and inputs in a holistic fashion.

Traditional information security controls can take on many forms such as (a) perimeter, host or application security based on passwords and digital certificates for authorization and authentication checks at an entry point (e.g., gateway to a network, port of a computer, remote call to an application) (b) host, storage and application security based on scanning for signatures of known malware (e.g., viruses, worms, etc.) either at the entry point or after the fact scan of various memory and storage elements (c) perimeter security based on filtering out unwanted sources and destinations (d) data security based on cryptographic measures and key

managements. But these point or perimeter solutions applied to host computers, networks or applications often work with little knowledge of each other's functions and capabilities.

Lacking the correlated contexts of domain knowledge such as normative business processes and data flow, situational intelligence often fails to construct a correct cause-consequence trace. This leaves the human operator or the automated analyzer overwhelmed with a deluge of messages without the right context to debug them.

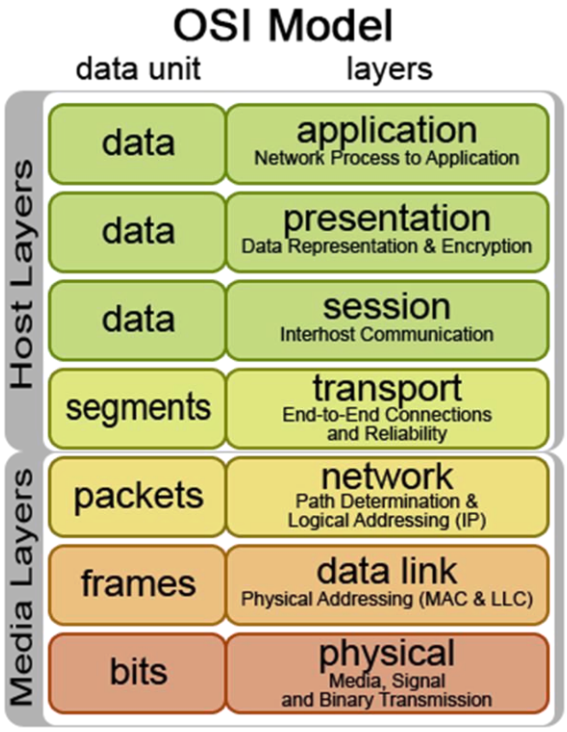
The power grid operation (OT) systems have unique performance and reliability requirements. Retargeting security risk controls commonly effective in the IT domain to the utility OT domain is rendered much more challenging by limited availability of computation and communication capabilities in legacy system platforms. Examples of such limitations include legacy Intelligent Electronic Devices (IED), the slow serial links through which communications among substations, control centers and field equipment take place and clear text communication protocols like Supervisory Control & Data Acquisition (SCADA) over Modbus or Distribution Network Protocol (DNP3).

A successful holistic security risk management system thus will have interoperability as an extremely important design attribute. In addition to being interoperable with diverse structured and unstructured data collected from myriads of devices (e.g., meters, synchrophasors, IEDs, firewalls, field devices etc.), different applications as well as various internal and external sources like social networks, CERTs, third party analytics etc., such systems will have to interoperate with legacy devices and protocols and traditional point and perimeter information security solutions from different vendors.

Currently perimeter, host or application security solutions may operate at layers 1 – 7 of the Open Systems Interconnect (OSI) model depicted in Figure 1. As an example, Secure Socket layer (SSL), one of the most prevalent standards for encrypted communication between network devices in the utility sector, operates at OSI layer 6 – the presentation layer of the OSI model.

The layers of the Grid-Wise Architecture Council (GWAC) model shown in Figure 2 describe the extension of contexts (layers 4 – 8) made by the council to compliment the 7 OSI layers generally corresponding to GWAC layers 1 – 3, which deal with physical and logical connectivity between systems as well as common understandings of data structures in messages exchanged between systems across variety of networks.

The unprecedented success of the Internet can in part be attributed to the remarkable interoperability the Internet Engineering Task Force (IETF) engendered around the Network layer (layer 3) of the OSI model. A wide set of physical media (copper, fiber, wireless, etc.) and logical addressing (Ethernet, Fiber Channel, etc.) could interoperate around a common network protocol of IP in this model.



OSI Stack Source: Wikimedia Commons/Dino.korah

Fig. 1 OSI layers – traditional contexts for security solutions

The same interoperability benefit can be extended to the smart grid communications technology, enabling innovation and evolution around a common network protocol.

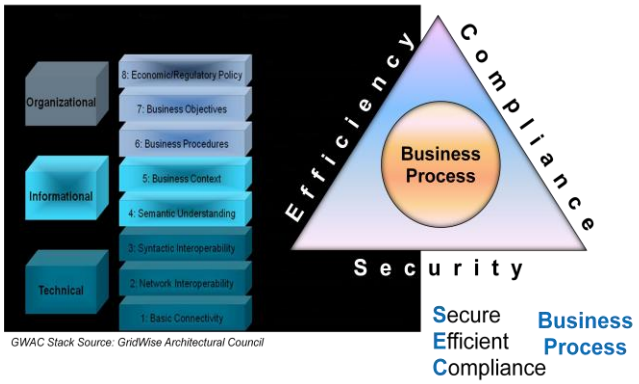


Fig. 2 GWAC stack: Context of Business Function Security

A similar opportunity of exceptional interoperability success can be built around the GWAC informational layers of

Business Context and *Message Semantics* (layers 4-5) which deal with the business knowledge related to specific interactions among the utility systems and the semantics of the messages being exchanged. These layers offer very compelling and context rich systemic view valuable for security, efficiency, compliance (SEC) as well as reliability and stability correlations.

Most importantly, such layered implementations enable evolutionary development of all levels of abstraction in the technical, informational and organizational layers around the interoperability layers, yet protecting the investments made in all other layers. As an example, smart meter (AMR) interval readings in MultiSpeak [13] can be correlated against metered energy dispatch reading at a substation, which could be in CIM [14] to analyze any mismatch if the analysis engine can interoperate across the semantic specifications of both the MultiSpeak and the CIM meter reading payloads. The mismatch may potentially be traced to deliberate attacks such as meter reading spoofing, meter tampering or unauthorized diversion of energy (non-technical loss).

Plethora of security solutions exist for layers 1 – 7 of OSI model and all end to end Smart Grid (SG) security frameworks will need to be flexibly built on them. The focus of this paper is technologies necessary for improving cyber security at higher levels (OSI layers 5-7 or GWAC levels 4-8). Evolving cyber security solutions will also need to leverage mature risk management approaches, including automated risk analysis by correlating situational and domain contexts (processed at GWAC layers 4 and above). Risk governance artifacts like security blueprint, security policies, security processes and security rules could be used to determine appropriate risk mitigation and security postures. Thus the higher layer GWAC information and procedures will work with monitored inputs to generate the security controls.

Conceptually such framework could encompass data centers and IEDs as well as emergent infrastructure and processes. They could also address integration of legacy systems using robust security wrappers.

4. SECURITY, EFFICIENCY, AND COMPLIANCE (SEC): CONTEXTS FOR RISK MODEL

Security, Efficiency, and Compliance (SEC) is pervasive to the architecture of an automated risk model and the general solution needs to address SEC to be effective. A formal approach, which incorporates the SEC (Security, Efficiency, and Compliance) paradigm, is also essential in the risk calculation component when transitioning from the existing ad-hoc non-automated processes to an automated provable computational process.

- Security – Any automated system must detect the existing security state and then improve on the state.
- Efficiency – The system must be efficient since the amount of information and the number of combinations in the Smart Grid is increasingly large.
- Compliance – The system must have a formal compliance process to consistently and accurately determine compliance

The increasing interdependency of OT and IT within the Smart Grid significantly increases the number of risks to the different business organizations comprising the Smart Grid. The threat and vulnerability analysis in a classic risk model where Business Functions are correlated to threats via a formal process has substantially increased in complexity due to the increasing combinations of interactions between systems. This is especially true with the emerging Smart Grid. Traditional OT systems have operated in isolation and there had been limited interaction with IT enabling ROI to be clearly discerned. In the emerging Smart Grid, many different systems are being connected thereby increasing the combinatorial multi-dimension array of interactions between disparate systems. The systems in the Smart Grid interact dynamically in a multi-dimensional space where output from one control/change may influence other threat parameters. This dynamic and multi-dimensional aspect of the data requires a formal computational solution.

Traditionally, the high level risk analysis was carried out by a group of domain experts using standard tracking tools such as spreadsheets and databases; however the increased complexity is exceeding the human capacity for complex system risk analysis. A formal and provable computational approach to risk analysis is now required to properly guide organizations on threat mitigation. Typically an organization performs risk analysis on the assets of the Business Functions of their organization based on a financial ranking without understanding the interdependencies of the assets. In the emerging Smart Grid the complexity is now exceeding our human capacity to track and analyze threats using the traditional methodologies.

There are several significant weaknesses with the historical approach.

- Formal Ranking Engine: Historically organizations have had ad-hoc and non formal methodologies for ascertaining the relative priority of threats. The ranking has been correlated to perceived financial loss, however generally no formal methodology with qualifying feedback loops has been utilized.
- Formal Prioritization Methodology: Prioritization has been tightly coupled with the ranking methodology. Feedback loops are generally absent.
- Dynamic Ranking and Prioritization: Ranking and prioritization have been performed with ad-hoc methodologies and dynamic real-time feedback loops have been absent.
- Large Data: The amount of data is rapidly increasing and has surpassed the ability of traditional relational and scan/sort systems to process the data.

There are two main strategies within risk management, *viz*., asset-based and threat- and vulnerability-based risk management [7]. To evaluate risks in a large enterprise one has to employ a systematic methodology to cover all assets of the enterprise. Methodologies of course could combine both the approaches where the asset-based risk management focuses on identifying the most valuable aspects of the organization assets like information, equipments, process and data flow etc. and then assesses how they may be protected from threats and risks. Threat- and vulnerability-based risk management aims to identify the threats and vulnerabilities of a system first, and then look at the risk they pose in a top-down manner. Such methodology will include the following steps to start with, followed by appropriate iterative refinements and adaptive feedbacks to respond to dynamic and evolving threat landscape.

- Identify all assets that are important to the business goals of the enterprise
- Assess vulnerabilities of each asset
- Analyze all potential threats that can exploit the identified vulnerabilities
- Identify appropriate control mechanisms to mitigate each threat
- Determine optimum security postures for each asset

These steps provide a framework as input into a formal risk model. The formal risk model should be a provable computational engine capable of evaluating large volumes of data/input from multiple disparate sources. The model should have the following capabilities:

- Perform dynamic analysis in feedback loops to continuously update the threat matrix.
- Provide independent ranking and prioritization values based on the real-time and dynamic analysis.
- Have the capability to handle large data.

A model which incorporates these steps and adheres to the SEC paradigm will allow for a provable computational model to replace the existing *ad-hoc* non-computational systems in place so that the Smart Grid organizations may effectively evaluate and operate on security, efficiency and compliance (SEC) risks to their assets which have significant negative financial impact on the overall businesses.

5. ROI ANALYSIS AND METRICS

Historically in the electric utility industry there have been ad-hoc and informal framework for calculating Return on Investment (ROI) analysis for mitigations and remedies applied to threats to the enterprise. Most of the security investments are headline driven, *ad-hoc* and ultimately provide questionable protection. These same systems have generally failed to provide adequate protection for the most technology savvy corporations as well as military and even security agencies.

Because there is no accepted formal methodology applied across the industry, the ROI for control postures applied to existing perceived risks is difficult to calculate. The well known perceived risks have well defined solutions and all industries apply these remedies. The ROI in these cases is assumed. It is also well understood that these solutions work for existing known issues, however new threats keep

emerging requiring further *ad-hoc* remedies and subsequent integration back into the static solutions.

To effectively understand the ROI for applying control postures against risks the organization needs clarity about what is at risk. Assets like equipment, services, data, processes, personnel need to be part of the assessment. In addition to the asset analysis, a formal ranking system is required to help properly prioritize the threats based on relevance and impact. This analysis and ranking should be performed by a real-time dynamic model which is continuously updated with both internal and external feedback data.

A Threat and Vulnerability model should perform a systematic analysis of which postures and countermeasures are more effective. The effectiveness should be measured in a standardized model so that the ROI may be determined when compared to comparable industries.

There are several methodologies in use for Risk Analysis (OCTAVE, CRAMM, FRAP) [11]. Each specifies a life-cycle for risk treatment (countermeasure) for given assets. The ROI follows from a follow-up analysis of a treatment and the cost of the treatment compared to the cost of the threat occurring for an asset for a given frequency. If the cost of the threat occurrence multiplied by the frequency is greater than the treatment, then there will be a positive ROI for the given treatment. The ROI calculation is dependent on estimates and predictions and therefore it is generally impossible to deterministically prove a specific ROI. The ROI is generally expressed as a probability and is positive or negative depending on the actual occurrences and therefore absolute ROI may never be known. However probabilistic models may be constructed to result in accurate ROI estimates.

A formal methodology for estimated versus actual cost of threat and remedy is required to quantify the ROI for control postures versus impact of threat. The following spreadsheet illuminates a matrix of potential real-world threats and a sample subset of information which is useful in calculating ROI for specific control postures.

In the example of Fig. 3, an organization has the five threats and they need a formal methodology to evaluate the ROI.

The following additional information is known about these threats:

- Energy Theft – Intentional theft of electricity by overriding or bypassing metering
    - Dependency Impact: None
- Denial of Service – A malicious entity floods the network with artificial meter messages with the intent of disrupting both service and billing.
    - Dependency Impact: Grid Network Failure: A message flood could bring down a network and disrupt important actions like meter connect as well as cause financial damage.

Threat	Estimated Financial Loss	Actual Financial Loss	Estimated Posture Cost	Actual Posture Cost	Freq.
Electric Theft	Estimate	Derive	Estimate	Derive	N
Denial of Service	Estimate	Derive	Estimate	Derive	N
Meter Tamper	Estimate	Derive	Estimate	Derive	N
Water Leak	Estimate	Derive	Estimate	Derive	N
Gas Leak	Estimate	Derive	Estimate	Derive	N

Fig.3: ROI (Return on Investment) Example Use Case

- Meter Tamper – A malicious entity tampers with meters by sending shutoff messages and other unauthorized commands
    - Dependency Impact: Critical Infrastructure: If disconnect messages are sent to hospitals or homes with life-support, it can lead to loss of life. Loss of revenue is the impact with less than actual meter readings.
- Water Leak – There is a water leak either at a premise or between a supply line and a premise
    - Dependency Impact: Drought Mitigation: Loss of revenue, resource and possible damage of equipments.
- Gas Leak – There is a gas leak at a premise or between a supply line and the premise
    - Dependency Impact: Gas Explosion: Can lead to gas explosions which can kill people and destroy property (safety).

In this model the predicted financial loss minus the cost of the control will be compared to the actual financial loss and the actual cost of the control. The cost of controls is generally well understood and should not deviate significantly. The actual cost of the threat depends on frequency.

This is a simple example; however it exemplifies the major requirements of a well behaved ROI model. In this example there are only 5 threats, however in the real-world the number of potential threats will be much larger.

- The ROI model needs to be computational and provable to handle the combinations of a system with a large number of threats, which could interact among themselves to make the impact even larger. The ROI model needs a formal ranking algorithm to prioritize the threats so that an organization can focus on the significant threats.
- The ROI model needs to include dynamic and real-time exogenous and domain information to dynamically prioritize and rank the threats. In the case of the water leak, weather related drought information may add to the impact of the water leak. In the case of a gas leak, the system can determine the nature of the leak. The impact of a potential explosion can then be added to the potential cost of the threat.
- The ROI model needs to process large data and to perform machine learning against the large data to correlate dynamic information with situational domain awareness to effectively adapt to the rapidly emerging and dynamic Smart Grid.

In the emerging Smart Grid an effective ROI model is essential to the business organizations. The plethora of data, the increasing combinations of systems, the increasing number of risks and the changing value of assets require that the ROI model uses a provable model in a computational environment capable of handling large data.

6. SECURITY, EFFICIENCY, RISK (SEC) RISK PROCESSING: A SIMPLE SCHEMATIC

A schematic architecture of a unified OT and IT domain aware adaptive security system is illustrated through Figures 4 and 5. Exogenous and endogenous sources of intelligence and asynchronous and real time operational interactions among its various components are shown in Figure 4. It also depicts how the security control posture changes in near real time (order of milliseconds to hours) in response to changes in the power and/or information system state changes due to security, reliability, stability related incidents or events. The IED (Intelligent Electronic Devices) and the RTU (Remote Terminal Unit) represents the aggregate information, telemetry and control systems embedded in the field equipments at substations and central power stations as well as transmission lines and distribution feeders.

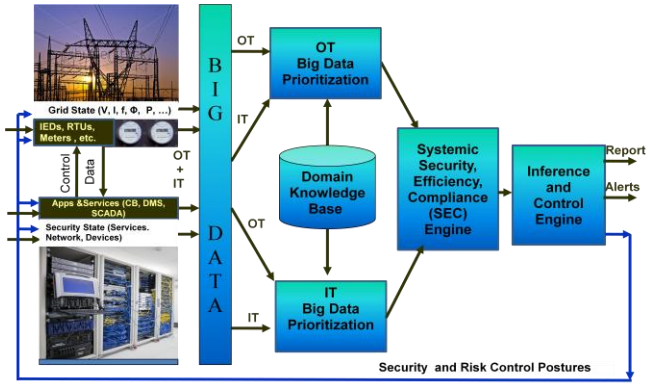


Fig. 4: Big Data and OT, IT Systemic Risk Management

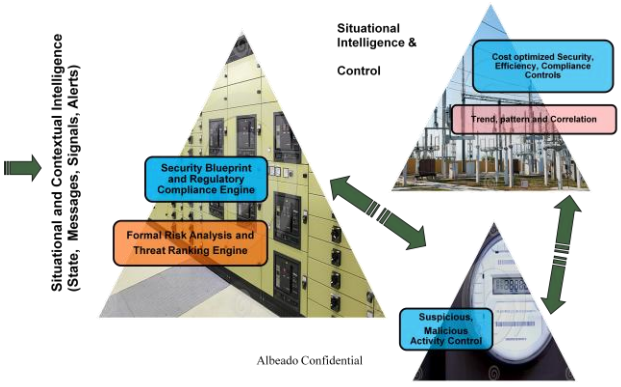


Fig. 5: Coordinated SEC Risk Analysis and Management

The objectives of adaptation include:

- Increasing or decreasing the security levels associated with various grid components and IT system components according to the threat environment inferred from various grid and information system states and other Big Data inputs
- Right sizing security by balancing costs against benefits varying the encryption strength. In the real-time context, this involves the allocation of available IT resources for processing security related functions versus business related functions. For example, when the power system is undergoing certain changes, the volume and variety of grid information related transactions may increase and if necessary, some of the low priority security related transactions may have to be curtailed. In the maintenance/upgrade mode, "right sizing" involves balancing the life-cycle costs of security against the grid-related benefits.
- Manage scalability, performance and effectiveness of the process of examining large volume of data of variety of types from diverse sources (Big data) which uncovers hidden patterns of systemic anomaly, reveals unknown correlations and offer various insights to better understand and manage business process risk and security in unified OT and IT domains.

7. CONCLUSIONS

Smart grid business and security risk management requires secure automated information exchange among all domains of the enterprise to support analysis and intelligent decision making distributed throughout the enterprise. Orchestrated correlation of situational awareness, domain knowledge including physical, behavioral, operational and security intelligence of the OT and IT systems are the key elements of the real time predictive data analysis process. An appropriate risk management engine from the perspective of relevance and consequence of the various inputs ensures that the analyses is scalable and yet remain effective in the face of the huge volume, diverse sources and types and the varied speed of the incoming data. The ROI analysis aspect of the risk management system can guide the inference engines and decision control systems to recommend and actuate control activations ensuring that the entire enterprise operates much more efficiently while enhancing end-to-end security and mitigating business efficiency and compliance risk.

As the OT and IT domains of the smart grid integrates more, a unified risk model can take advantage of a correlated view of IT security and OT reliability consequences, based on unified event monitoring and analysis models and deep contextual understanding of the various operational and business process interdependencies in the enterprise. Such approaches will enable analysis of significant events, prediction of correlated consequences, and provision of intelligent, systematic, and coordinated responses on a real-time basis. Such integrated risk management will also need to rely on consistent ROI and Risk management metrics and objective risk analysis processes, along with historical vulnerability and threat data, *e.g.* anomaly in traffic, attack signatures, information forensics, *etc*., that would enable domain specific statistical analysis and characterization of attack probabilities and risks.

In conclusion, diverse data collection sources, various analysis programs correlating them with other power system and customer data, decision control elements from possibly different vendors will need to interactively coordinate to provide functionally pervasive yet business process context aware security risk analysis and control systems. Interoperability among them is a critical requirement that will ensure that innovation and competition offer customers a sustainable ecosystem for integrated security and risk mitigation solutions. The ROI guided automated Risk management system described here captures the architecture and approaches to make the system scalable in the face of the Big data onslaught the utilities are facing, yet provide effective outcome by prioritizing the inputs for the systemic security, operational efficiency and business process compliance context of the industry and the organization.

References

[1] U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability, "Smart Grid Research & Development: **Multi-Year Program Plan (MYPP)** 2010-2014", March, 2010

[2] Annual Energy Review 2009, August 2010, U.S. Energy Information Administration, Office of Energy Markets and End Use, U.S. Department of Energy, Washington, DC 20585

[3] Ranjit Kumar, Partha Datta Ray, Chris Reed, "Smart Grid: An Electricity Market Perspective", IEEE Innovative Smart Grid Technology Conference, January, 2011

[4] Partha Datta Ray et. al, "Smart Power Grid Security: A Unified Risk Management Approach", Proceedings for the 44th IEEE International Carnahan Conference on Security Technology (ICCST),San Jose, CA, October 5th – 8th, 2010.

[5] Partha Datta Ray, "The Smart Grid's Singular Security Challenge", POWERGRID INTERNATIONAL, vol.16, No.05, pp 58-60, May 2011.

[6] Jeff Katz, "Smart Grid Security and Architectural Thinking", White Paper, http://www.ibm.com/smarterplanet/global/files/us__en_us__energy__smartgridsecurity_and_architecturalthinking_katz.pdf

[7] *Risk and Reliability - An Introductory Text*, 5th ed: Risk & Reliability Associates (R2A), 2005.

[8] Wayne Jansen, "Directions in Security Metrics Research", NISTIR 7564, April 2009

[9] "The CIS Security Metrics: Consensus Metric Definitions V1.0.0", Center for Internet Security, May 2009

[10] K. Moslehi, R. Kumar, "A Reliability Perspective of the Smart Grid", IEEE Transactions on Smart Grid, Vol1, Issue 1, pp.57-64, , June 2010.

[11] Ida Hogganvik, "A Graphical Approach to Security Risk Analysis", "A Reliability Perspective of the Smart Grid", Doctoral Dissertation by Ida Hogganvik, pp.1 - 46, October 2007.

[12] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", NISTIR Special Publication 800-30, pp.37-41, July 2002

[13] http://www.multispeak.org/about/Specification/Pages/default.aspx

[14] http://cimug.ucaiug.org/default.aspx

Biographies

Partha Datta Ray has 27 years of industry experience and served in multiple business and technology management roles including Vice President at GDA Technology (acquired by Larsen and Toubro) handling engineering and strategic marketing, TeraBlaze (a networking start up acquired by Agere), LSI Logic, Telerate (acquired by Dow Jones), Silicon Compiler (acquired by Mentor Graphics) and AT&T Bell Laboratories.

He currently leads the Information Security Work Group for the IEEE P2030 Smart Grid Standards Committee. He held the chairmanship of the RapidIO BFM Working Group, an interconnect standard widely deployed in wireless communications and is a senior member of the IEEE Communication Society. In the past, he led or served on various industrial and trade groups on Communications Protocols, Simulation, and Modeling.

Partha holds a BSEE and MSCS from Rutgers and conducted advanced post graduate research work at leading academic and research institutes.

He holds multiple patents in areas of circuit and network optimization and has multiple pending patents in areas of cyber security control and automated risk management. He has been invited keynote speaker at CIO Utilities Summit and most recently has presented at IEEE International Security Conference, IEEE Innovative Smart Grid Technology Summit and many other industry events.

Christopher Reed has served in senior leadership roles in service organizations at companies ranging from startups to Fortune 500 including Nokia, Borland and Intellisync. Chris has built and lead teams distributed around the globe that provided integration and development services, custom engineering and educational support. He currently leads the Enterprise Solution Engineering and Services at Albeado.

Chris attended University of California, Santa Cruz & earned his BSEE at San Jose State University and is currently leading the Information Modeling Subgroup for IEEE P2030 standards committee. He actively participates in other industry consortiums like MultiSpeak, CIM & others. He earned his JD degree from Monterey College of Law.

Atul P. Agarwal has 24 years of experience in building complex software systems both in technology and enterprise business domains. He currently heads a team of about 10 engineers building a Java/J2EE framework for easily and securely integrating applications based on various Smart Grid standards like MultiSpeak, CIM and others. Atul has earlier founded and successfully grown Apt Software a software product and services company in India which provides software development and product engineering services to organizations around the world in diverse areas like energy exploration and operation, mobile platforms and applications for commerce and entertainment, semiconductor design and services. He has worked with many technology startups in the Silicon Valley and is currently heading the Albeado India Design Center.

Jeff Gray has 25 years of experience designing, developing and architecting software products for companies like Texas Instruments, Bell Northern Research, and Nokia. Since moving to Silicon Valley in 1995, Jeff has designed, developed and patented software products for several successful startups (e.g. Netscape, Starfish/Motorola, LightSurf/Verisign and eMeter/Siemens). While at Starfish/Motorola, Jeff designed, patented and developed the first Calendar Internet synchronization product which was successfully integrated into the Yahoo! server backend to create the first highly scalable Internet synchronization offering. Jeff earned a Bachelor of Science degree in Mathematics and then studied Artificial Intelligence through MIT. For the last 10 years he has developed and deployed highly scalable Java/J2EE client-server installations for carriers like AT&T and Verizon.

Suresh Seth For the past 26 years, Suresh has been developing and applying software technologies to improve operational efficiency for diverse enterprises. He started his career in AT&T Bell Labs in Murray Hill, NJ following a Ph.D in Operations Research and Masters in Computer Science from Virginia Tech. After his stint in Bell Labs, he was the Vice-President for Servers Business at Starfish. There his team developed the synchronization server software which is still being used by a variety of vendors including AT&T. Starfish was acquired by Motorola. He has also served in a variety of roles – from sales engineering, solutions architect and technical product manager in companies like Intellisync, Nokia, Navisite, Power Assure and RingCentral before joining Albeado.