2.3 Policy-Governed Secure Collaboration

2.3.1 Analytics for Cyber-Physical System Cybersecurity

Collaborators: Choucri (Lead), Amin

Problem Description Smart grid technology – increasingly-ubiquitous in power systems – represents a highly complex CPS. Mounting concerns about safety and security have re-sulted in an intricate ecosystem system of guidelines, compliance measures, directives and policy reports for cybersecurity of all critical infrastructure. By definition, such guidelines and policies are written in linear sequential text form that makes them difficult to integrate, or to understand the policy-technology-security interactions, thus limiting their relevance for science of security. Missing are analytics for smart grid cybersecurity and risk assessment. We propose to develop text-to-analytics methods and tools, applied initially to Cybersecurity Framework [59] and NIST Guidelines for Smart Grid Cybersecurity [68].

Policy directives and guidelines texts for cybersecurity carry their own constraints. It is not clear if the dilemma lies in design and substance of the policies, the paucity of metrics, or in the absence of informative analytics. RAND concluded that "...the policies governing cybersecurity are better suited to simple, stable, and predictable environments, leading to significant gaps in cybersecurity management." [81]. More important, they are not based on any precepts we would consider as bearing on a science of security.

Technical Barriers Several technical barriers impede full understanding of the cyber-physical properties of a smart grid enterprise: (a) locating policy relevant decision points, (b) identifying vulnerabilities embedded in organizational process and technical operations (c) differentiating intents of threat actor vs. vulnerability of system, (d) tracking dam-ages and diffusion effects, (e) characterizing potential unknown-unknowns, or (e) metricizing functional relationships – to note the most obvious.

Previous Related Work In our previous work, we reviewed the new trends, contribu-tions, and identifiable limitations in cybersecurity research. We argue that these limitations are due largely to the lack of interdisciplinary cooperation required to address a problem that is clearly multifaceted. We have also provided recommendations for terminology use when writing papers on cybersecurity and lay the ground work for interaction between tech-nical and nontechnical stakeholders [71]. The vision and the objectives of our research and a solution strategy for analytics for smart grid cybersecurity are described in [18].

Research Approach We propose a multi-method modular approach applied to a generic system in a controlled environment. The "raw data" consists of texts of National Institute for Standard and Technology (NIST) guidelines for cybersecurity of power systems [68],

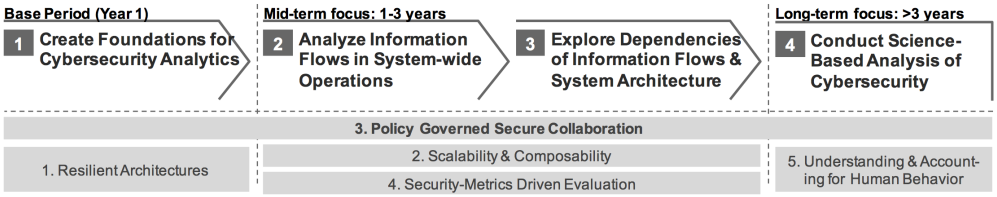
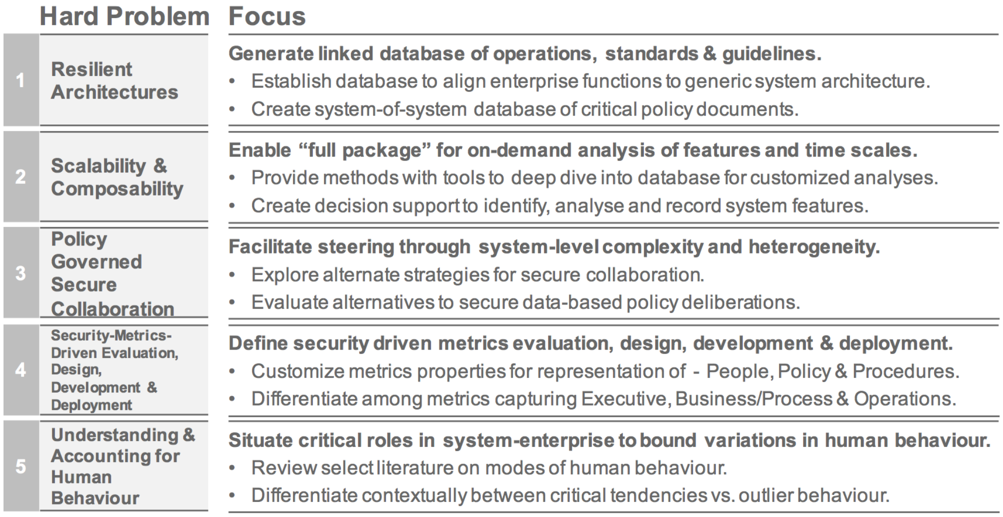

Base Period (Year 1)
1 Create Foundations for Cybersecurity Analytics
Mid-term focus: 1-3 years
2 Analyze Information Flows in System-wide Operations
3 Explore Dependencies of Information Flows & System Architecture
Long-term focus: >3 years
4 Conduct Science-Based Analysis of Cybersecurity
3. Policy Governed Secure Collaboration
1. Resilient Architectures
2. Scalability & Composability
4. Security-Metrics Driven Evaluation
5. Understanding & Accounting for Human Behavior

Figure 3: Near-, mid- and long- term project goals and hard problem addressed.



	Hard Problem	Focus
1	Resilient Architectures	**Generate linked database of operations, standards & guidelines.** • Establish database to align enterprise functions to generic system architecture. • Create system-of-system database of critical policy documents.
2	Scalability & Composability	**Enable "full package" for on-demand analysis of features and time scales.** • Provide methods with tools to deep dive into database for customized analyses. • Create decision support to identify, analyse and record system features.
3	Policy Governed Secure Collaboration	**Facilitate steering through system-level complexity and heterogeneity.** • Explore alternate strategies for secure collaboration. • Evaluate alternatives to secure data-based policy deliberations.
4	Security-Metrics-Driven Evaluation, Design, Development & Deployment	**Define security driven metrics evaluation, design, development & deployment.** • Customize metrics properties for representation of - People, Policy & Procedures. • Differentiate among metrics capturing Executive, Business/Process & Operations.
5	Understanding & Accounting for Human Behaviour	**Situate critical roles in system-enterprise to bound variations in human behaviour.** • Review select literature on modes of human behaviour. • Differentiate contextually between critical tendencies vs. outlier behaviour.

Figure 4: Focus area of research goals and their connections to the hard problems.

augmented by exploration of on user-specific customizations and generalizations. Figure 3 provides the near-, mid- and long- term project goals (described in more detail below), with "Policy Governed Secure Collaboration" as the primary hard problem. The others four are situated in the Figure 3 and details are in Figure 4.

This work directly addresses the hard problem of policy-governed secure collaboration at the enterprise level (for Smart Grid). It is especially relevant to the Science of Security program because the design is based on a structured system model derived from critical texts to (a) identify major system-wide parameters, (b) situate vulnerabilities, (c) map security requirements to security objectives, and (d) advance research work on how multiple system features interact with multiple security requirements and affect the cybersecurity of such important cyber physical enterprises.

Research Goals and Tasks *Task 1. Create Foundations for Cybersecurity Analytics:* During *Year 1*, we will focus on the required foundations for cybersecurity analytics that include: (1) Identify the policy relevant ecosystem; (2) Formalize rules for extracting data from text; (3) Identify missing pieces for implementation of cybersecurity measures; (4) Construct internally consistent structure to organize, metricize, and manage critical information.

Task 2. Analyze Information Flows in System-wide Operations: Our objective in *Year 2-3* is to analyze information flows in system-wide operations. We will review rules and methods for extracting data from key documents. We will also create a dependency structure matrix of of physical cyber system by identifying first level information dependencies. The dependency matrix will be transformed into clusters and partitions of structure and process, and will be used to explore properties that reveal "hidden features".

Task 3. Examine Dependencies of Information Flows and Technical Architecture: Our next task in *Year 2-3* is to examine the dependencies of information flows and technical architecture. We will generate visual representations of information flows using graph theory and network methods. These representations will be used for identifying critical nodal or control points, distinguishing between human/management vs. technical operations and connections, and identifying modalities of interface or integration of human and technical systems.

Task 4. Conduct Science-Based Analysis of Cybersecurity: The long-term goal (*Year 4-5*) of the project is to conduct science-based analysis of cybersecurity. We will formalize enterprise-wide system dependencies and we will use a three-fold Live-Virtual-Constructive environment for evaluation and validation: (1) Live: a simulation involving real people using/operating the real system; (2) Virtual: a simulation involving real people using/operating the simulated system; and (3) Constructive: a simulation involving simulated humans and the simulated system. Finally, we will formalize properties of system disturbances (vulnerabilities and risks) in order to assess potential system impacts of disturbances.

Strategy for evaluation and validation include (i) completing, validating, and implementing analytics derived from NIST smart grid “conceptual” model, and (ii) undertaking contingency analysis of security threats, in terms of “what...if...”

Tasks 1-4 summarize an operational method for replicating it in other systems. For example, it supports four focus areas of US DoD CIO (2013) by establishing foundations of a resilient cyber defense posture (focus area 1); buttressing the transformation of cyber defense operations for greater emphasis on adversary activities and intent (focus area 2); enhancing cyber situational awareness (focus area 3); and supporting capabilities to identify and transcend highly-sophisticated cyber-attacks (focus area 4).

Integrative Research The proposed project is complementary to the other research efforts in the lablet. While this project focuses on cybersecurity issues of a cyber-physical infrastructure at a conceptual level, other projects focus on system aspects, and this cross-disciplinary research is necessary to address the cybersecurity challenges in real CPS. Further, the SURE platform can provide the simulation environment for evaluation and validation of the research as well as dissemination of tools and methods.