

Position Paper: Cyber-Physical Security Needs in Electrical Energy Systems

Submitted for: National Workshop: Beyond SCADA: Networked Embedded Control for Cyber Physical Systems (HCSS-NEC4CPS)

Submitted by: General Electric Company

Authors: Timothy L. Johnson (*point of contact*) and Michael J. Hartman (GE Global Research),
Kenneth Caird (GE Energy)

As a large diversified international company, GE's business and customer interests include many of the application domains of this workshop, including building and environment, chemical process control, manufacturing systems, electrical energy systems, oil and natural gas, transportation networks, and water distribution systems. The focus of this response is on *electrical energy systems*, as represented by GE Energy Network Reliability Products and Services (http://energy.ge.com/energy_services/nrps/) and GE Global Research (<http://www.ge.com/research/>). GE is a major producer of utility wide area data collection and display equipment, transmission and distribution substation equipment, power island (generator, combined cycle, balance of plant) controls, digital breakers and meters at all power levels. It should be noted that GE Security also produces commercial building (physical) security and fire protection systems. GE has a strong interest in long term improvements in both cyber and physical security of electrical energy systems, and manufactures hardware, networking, software products as well as providing services in this domain. All of the themes cited in this workshop are of interest to GE, but of top interest are "Costs and Barriers to Innovation", "Systems Issues", "Emergent Issues", and "Software Platforms". In view of length limitations, this position paper will focus primarily on these themes.

Costs and other barriers to innovation are a primary concern to GE's customers, and therefore to GE: frequently these are barriers to the adoption of even *existing* products with security enhancements. The perceived cost of enhancing cyber-physical security is high – due to a large amount of installed base (legacy) equipment with non-secure protocols. The *challenge* of identifying compensating advantages – such as reducing operations and/or servicing costs -- of cyber-secure systems must be addressed in order to change customer behaviors. The most important information *technology research needs* include the inexpensive upgrade of hardware and software for existing unsecured legacy power and communications equipment, and invention of low-cost, effective means of detecting cyber-physical threats or intrusions through newer equipment.

Roadmap:

Near (1-3 years): Valuation and prioritization of cyber-physical risks. Intrusion detection methods for distributed systems.

Mid (4-6 years): Retrofit and re-engineering methods; reliable and secure network transition strategies

Long (7-10 years): Integration of new cyber-physical technologies into products; implementation of incentives

Systems Issues are also of high interest to GE. *Challenges* - Traditional decentralized automatic safety protection systems have been demonstrated to be subject to system-level malfunction (e.g., the 1967 Northeast Blackout), even when local protective devices operate correctly. Centralized fault detection and monitoring systems, while improving, still exhibit wide area alarm patterns that are difficult to detect, and introduce un-

acceptable IT and embedded system administration burdens (digital hardware obsolescence, patch installation and testing). The ability to respond deftly to a variety of large network disturbances (i.e., to keep ahead of hackers) is also not well supported by existing systems. *Technology Needs* - Tightly coordinated, digital protection and safety systems (as part of improved “power grid” designs) are needed, as are the ability to anticipate, visualize, and isolate rapidly evolving disaster areas. System safety software technologies (temporal hazard analysis) should be applied to the design of such systems so that they anticipate most threats. Physically diverse networks (e.g., with wireless or satellite-link backup of previously installed wired links) should be employed to improve network robustness to major disruptions. Finally, high confidence software, capable of a layered defense to cyber-threats, is needed.

Roadmap.

Near (1-3 years): Study of utility system cyber-physical operational risks using hazard analysis. Prioritization of risk reduction needs. Study of risks due to coordinated physical and cyber attacks.

Mid (4-6 years): Network backup and software service and maintenance procedures, built-in verification and validation capabilities.

Long (7-10 years): Critical technologies for system level re-design: secure protocols, middle-ware, on-line certification of upgrades, standards for interoperable system simulations

Emergent Issues – Challenges - Adaptive non-deterministic systems or *emergent systems* can be robust to unplanned occurrences in a system. Occasionally the exhibited local behavior is unexpected to human observers. System simulation and human interface tools are needed to understand the global state of the system and predict what the likely future state(s) will be if left undisturbed or if modified by attackers or by external control. *Technology needs* – Given the decentralized nature of many emergent systems they can be effective as a defensive mechanism for cyber attack. One such mechanism could be a variant of a gossip protocol, whereby each node raises its apprehension based on the apprehension of other nodes. The stability of these systems needs to be simulated and approaches for bounding of the behavior of systems need to be created. Emergent systems are robust to the loss of centralized authorities. Trust mechanisms typically work with pre-shared keys or shared certification servers. New methods are needed in cases where a remote node can be compromised and we cannot rely on a central site or new nodes are brought into the system on emergency basis

Roadmap.

Near (1-3 years): Simulation platforms for realistic emergent systems; trust in emergent systems. New algorithms and trust systems

Mid (4-6 years): Human interfaces for emergent systems. External control approaches

Long (7-10 years): Utility system testbeds; certification methods.

Software Platforms Priorities: Heterogeneous, legacy platforms and patch management are costly *challenges* in cyber security. The cost of full replacement of equipment is a large barrier to the security updates needed. Partial replacement and gateways are possible but it is difficult to understand efficient architectures and performance requirements for these overlay systems. *Technology needs* - Methods for abstraction of the actual system through publish/subscribe and other approaches will need to be explored in the context of real-time feedback control behaviors. High confidence systems require reliable and trusted communications. Low cost wireless sensors and wireless

field communications have unique authentication requirements including combined physical and cyber access and physical control of communicating devices. Additionally adaptive behavior based intrusion detection is needed.

Roadmap.

Near (1-3 years) : Wireless comm. security for sensors, field and control systems. Simulation platforms for realistic overlay heterogeneous systems.

Mid (4-6 years): Optimization algorithms for architecting legacy security & control overlays to networks.

Long (7-10 years): Utility system test beds.

GE Energy Network Reliability Products and Services (NRPS) and the GE Company, represented by its corporate component GE Global Research (GEGR), look forward to the opportunity to present and publicly discuss issues in Cyber-Physical Security at the forthcoming HCSS-NEC4CPS workshop on November 8-9 in Pittsburgh.

Following is the requested biographical information for each author:

Timothy L. Johnson, Ph.D. [*Primary Point of Contact*]

Project Manager, Computing & Decision Sciences

GE Global Research, Bldg. K-1, Room 5C30A

One Research Cir.

Niskayuna, NY 12309

e-mail: johnsontl@research.ge.com

Phone: (518) 387-5096

Capsule Biography:

Dr. Johnson received a Ph.D. in Electrical Engineering and Computer Science from MIT in 1972. He then joined the MIT faculty, performing research in the area of control of systems governed by partial differential equations, biomedical engineering, and hybrid controls. In 1980, he joined Bolt Beranek and Newman (BBN) as a Senior Scientist and pursued applied research in man-machine systems, robotics, and automated systems. In 1984, Dr. Johnson joined GE Corporate Research and Development (now GE Global Research) where he has subsequently held several technical and management positions. Most recently, he has been involved in the development of automated system verification, knowledge management and diagnostics technologies in support of GE's Industrial and Medical businesses. Dr. Johnson has held several professional society positions, including Vice President of Technical Activities of the IEEE Control Systems Society, member of the Board of Governors, General Chair of the 1991 American Control Conference, and Finance Chair of the 1996 IFAC Congress. He was recognized as a Distinguished Member of the IEEE Control Systems Society in 1995 and as an IEEE Fellow in 2003. He has authored or co-authored over 100 publications and has been awarded several patents.

Michael J. Hartman,

GE Global Research, Bldg. KWC

One Research Cir.

Niskayuna, NY 12309
e-mail: hartman@crd.ge.com
Phone: (518) 387-6933

Capsule Biography:

Michael Hartman is a technical staff member and project manager at General Electric's Global Research Center, in the Computer and Decisioning Science Technology Organization. He joined GE GRC in 1982.

In 1986 he received his MS in Electrical and Computer Systems Engineering from RPU. While at GE GRC he has been engaged in the research and development of distributed systems, electronic circuits and information networks. His recent activities have been focused on mesh and wireless network technologies to enable distributed systems for a range of applications & businesses needs including industrial networks, satellite communication, field service, network management, medical information systems, media distribution and mobile ad hoc networks for rapid deployment and defense applications. He holds more than 10 patents in the areas of silicon compilers, expert systems for fault analysis, industrial/ consumer networking, ad hoc mobile network protocols & radio control, and sensor networks. He has written over 15 publications.

Kenneth Caird

Chief Engineer, GE Energy, Network Reliability Products & Services
2728 Hopewell Place NE
Calgary, Alberta T1Y 7J7
CANADA
e-mail: ken.caird@ge.com
Phone: (403) 214-4572

Capsule Biography:

Ken Caird received the Bachelor of Science in Electrical Engineering, University of Saskatchewan, 1973. As a Senior Design Engineer at Sask Power (a utility) after 1973, Ken designed and installed Energy Management Systems (EMS), Remote Terminal Units (RTUs) and communication systems for the automation and control of the high voltage grid. In 1988, Ken joined a start-up firm, Westronics, as Manager of Research and Development. Westronics became a leading international supplier of RTU's and Substation Automation Systems. Westronics was acquired by Harris Control Systems, where Ken became Director of R&D. In 1997, Harris was acquired by General Electric (GE), building the division into a global supplier of EMS, Distribution Management Systems (DMS), Geographical Information Systems (GIS), Outage Management Systems (OMS), Substation Automation Systems, Substation Monitoring and Diagnostic Equipment, Test Equipment and Meters where Ken now serves as Chief Engineer. He received the Alberta Science and Technology Award in 1993, and has authored one US patent. He is the author of the recent review article "Integrating Substation Automation" in IEEE Spectrum (Volume 34, Issue 8, Aug. 1997 Page(s):64 – 69).