Continuous Assurance for Cyber Physical System Security

Chris Codella, Arun Hampapur, Chung-Sheng Li, Dimitrios Pendarakis, and Josyula R. Rao

Abstract—**The security and privacy of cyber-physical systems (CPS) has been the subject of a lot of concern in the recent past especially in the context of the safety of critical infrastructure such as the power grid, transportation, and manufacturing environment. We envision that ensuring the security and privacy of these systems is really part of designing a resilient cyber-physical system. The grand challenge is really to provide continuous assurance of the operating objectives. In order to achieve continuous assurance, we believe fundamental research efforts need to be devoted to the challenges faced by fine-grained isolation, real-world aware, risk-adjusted resource allocation, and closing the loop.**

I. Introduction

Cyber-physical systems (CPS), that is, systems with tight conjoining and coordination between their computational and physical resources, have been identified as one of the eight priority areas in the August 2007 report of the President's Council of Advisors on Science and Technology (PCAST) [1] . Earlier generations of cyber-physical systems can be found in areas as diverse as aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances. Cyber-physical systems of tomorrow are expected to far exceed those of today in terms of adaptability, autonomy, efficiency, functionality, reliability, safety, and usability, such as those envisioned in the IBM Smarter Planet initiatives (Intelligent Utility Networks, Smarter Transportation, Smarter Cities, etc.) [2]. Research advances in cyber-physical systems promise to transform our world by responding more quickly, being more precise, working in dangerous or inaccessible environments, providing large-scale, distributed coordination, being highly efficient, augmenting human capabilities, and enhancing societal wellbeing.

Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements instead of as standalone devices. These systems represent a wide variety of networked information technology systems connected to the physical world. Most industrial control systems have a hierarchical structure. Figure 1 shows the reference architecture of a SCADA (Supervisory Control And Data Acquisition) based CPS system, which has been used in a wide variety of manufacturing, transportation, and power distribution environments [3].

The security and privacy of such CPS systems have been the cause of a lot of concern as their failure can cause irreparable harm to the physical system being controlled and to the people who depend on it. SCADA systems, in particular, perform vital functions for many of the national critical infrastructures, such as the electric power distribution, oil and natural gas distribution, water and wastewater treatment, and transportation systems.

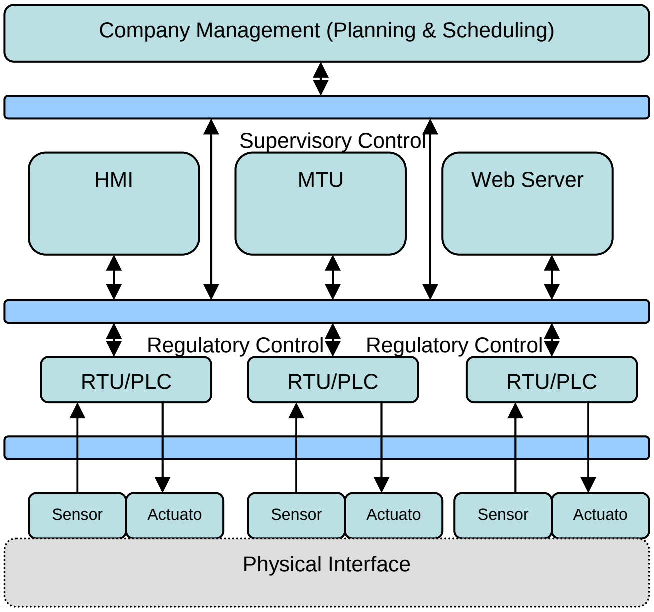

Figure 1: Reference architecture of a SCADA system

A number of recent reports [4-9] have suggested that vulnerabilities exist in many SCADA based systems as more and more of these systems are connected to the Internet:

- **Power Plants:** It is relatively difficult to hack into a nuclear power plant and trigger a meltdown. However, two vulnerabilities related to SCADA power systems have been reported previously (a) during 2003 due to the

C. Codella is with IBM Thomas J. Watson Research Center, P. O. Box 794, Yorktown Heights, NY 10598, email: (914) 945-2218 email: codella@us.ibm.com

A. Hamapur is with IBM Thomas J. Watson Research Center, P. O. Box 794, Yorktown Heights, NY 10598, phone: (914) 784-7440 email: arunh@us.ibm.com

C.-S. Li is with IBM Thomas J. Watson Research Center, P. O. Box 794, Yorktown Heights, NY 10598, phone: (914) 784-6661 email: csli@us.ibm.com

D. Pendarakis is with IBM Thomas J. Watson Research Center, P. O. Box 794, Yorktown Heights, NY 10598, phone: (914) 784-7887 email: dimitris@us.ibm.com

J. R. Rao is with IBM Thomas J. Watson Research Center, P. O. Box 794, Yorktown Heights, NY 10598, phone: (914) 784-6692 email: jrrao@us.ibm.com

Slammer worm at the Davis-Besse nuclear power plant in Ohio and (b) the Blaster worm for causing downtime in a power plant's detection systems. An experiment conducted by DOE in 2007 demonstrated that it is feasible to hack into the SCADA control of a synchronous generator and cause the generator to self-destruct.

- **Oil & Gas Pipelines:** A number of natural-gas companies reported potential vulnerabilities in their SCADA-based gas pipelines as these pipelines could be potentially turned off for the entire northeastern United States as a result of these vulnerabilities. In this scenario, technicians would have to manually re-light thousands of pilot lights before power could be restored, a process that would take months. It is also conceivable that a hacker might also be able to meddle with pipeline pressures and cause an explosion.
- **Transportation**: Trains, subways and traffic lights are all controlled by SCADA systems. That means an electronic intruder could potentially affect train speeds or even cause a collision. It is also conceivable that hackers could attempt to simultaneously turn all the traffic lights in a major city to green to cause major chaos.
- **Dams**: Previously it was reported that Arizona's Roosevelt Dam was hacked. Even though a hacker in control of a major dam is unlikely to destroy the dam or cause a major flood, he could cut off the dam's relatively small supply of hydro-electric power or, more importantly; disrupt the flow of water to the dam’s pumps from deep within reservoirs to cool reactors at other power plants.
- **Manufacturing:** A wide variety of manufacturing plants use SCADA systems, including those in the chemical and pharmaceutical industries. Hackers connecting to these systems via a corporate network could potentially do substantial damage to equipment, for example, by manipulating the temperature controls in a server room to cause servers to overheat and shut down the business's entire IT infrastructure.
- **Water Distribution:** Previously, there was specific incident for a hacker to hack into the control systems of Hunter Watertech, an Australian water-treatment facility from which he'd been laid off. This hacker was found to have gained control of the system 46 times, dumping sewage into parks and rivers so that the company would re-hire him to solve the problem.

II. Resilient Cyber-Physical System

In a typical Cyber physical system, the estimation and control algorithms used within such systems are designed to satisfy certain operational goals, such as,

- closed-loop stability,
- safety,
- liveness, and
- optimization of a performance function.

The security goal for Cyber Physical System is to protect these operational goals from a malicious party attacking. In addition, the security and privacy goals should also include the protection of:

- Physical security of the device as well as the environment where the device is operated within (such as human)
- Security and privacy of the information that was collected within the device.

A **resilient** cyber physical system implies that the cyber physical system can sustain cyber attacks without compromising the operational as well as the security and privacy goals of the system.

III. Grand Challenges: Continuous Assurance

Substantial progress in CPS research is required in order to maximize the resiliency of a cyber-physical system. The required progress includes:

- Early warning and far-field detection of potential anomalies of the operational characteristics (e.g. stability, liveness, and performance) of the cyber-physical system;
- Fine-grained problem determination and containment within a CPS in order to quickly isolate the anomalies once they occur and ensure the problem area will be localized.
- Fast recovery of operational capabilities of a CPS from an incident to minimize the potential sustaining impacts.

In short, the grand challenge for addressing the security and privacy issues of a Cyber Physical System is the ability to implement **Continuous Assurance** of the pre-determined operational, security and privacy objectives, as shown in Fig. 2. This grand challenge can be decomposed into the following four areas:

A. Fine-Grained isolation

A fine-grained approach is the emerging approach addressing the fundamental challenge coming from the dissolution of the traditional perimeter defense. Perimeter defense often relies on securing the perimeter of a network or system through firewalls, intrusion detection and prevention, as well as information leakage detection and prevention. These approaches have become much less effective due to the need to offer remote & pervasive access of the network.

Fine-grained approaches (which includes monitoring, logging, anomaly detection and prevention) will be crucial within a CPS in order to precisely localize the anomaly, prevent the propagation of the anomaly to adjacent areas, and improve the resiliency of the overall CPS. Introducing fine-grained approaches into a CPS could be fundamentally challenging as these approaches may affect the operational characteristics of a control system due to the introduction of additional observation and control points.

Fine grained approaches for the IT network and physical system have been designed independently in the past. Research challenges remain in terms of aligning the fine-grained approaches for CPS, including aligning the control points for cyber security and physical security.

B. Real World Aware

The operational behavior of a cyber-physical system is often captured by the system model of the CPS. The system model relates the state of the controller to the inputs and the feedback from the outputs, as well as between the inputs and the outputs. A typical utility network or a transportation system or a power plant often includes hundreds if not thousands of these inter-dependent cyber-physical systems. Even though the system behavior is often captured by the system model, it is not possible to anticipate all of the possible input combinations from the environment. Consequently, it will be of great importance that the behavior signature of the environment for any given CPS – including the impact of the inputs can be continuously learned autonomously in terms of their impact on the system model and outputs.

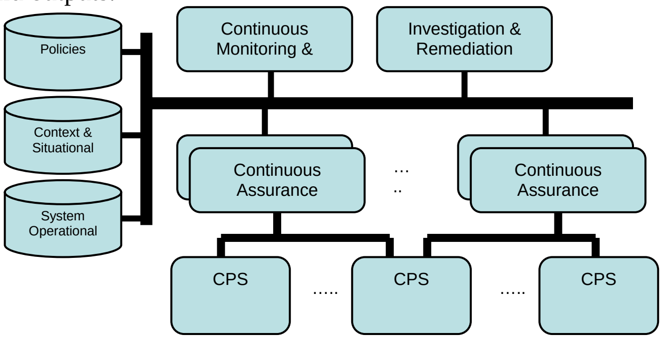

Figure 2: Reference architecture for providing continuous assurance for inter-dependent fine-grained cyber-physical systems

C. Risk Adjusted Resource Allocation

Almost all cyber-physical systems involve some aspects of real-time or near real-time operations. As a result, extracting the behavior during normal operational conditions as well as deciding the best approach when the system is suspected to be under attack needs to be completed within certain time limits. It is expected that the best approach is to use a risk adjusted approach to allocate the resource so that the end objective is to minimize the overall risk of missing the operational objectives even when there are potentially conflicting resource requirements for the individual operational objective.

D. Closing the Loop

Continuous assurance for a CPS or networked CPS requires closing the loop multiple times in order to ensure that the monitoring and logging are not tampered or compromised. The design principle of continuous assurance within a CPS is potentially similar to the auditing of a business system where multiple close-loop audits are required with appropriate separation of duties inserted between those close-loop monitoring and auditing in order to prevent a wide spectrum of both insider attacks and external intrusions.

IV. Conclusion

Security and privacy of cyber-physical systems (CPS) have been the cause of a lot of concern in the recent past, especially in the context of the safety of critical infrastructures such as power grid, transportation, and manufacturing environment. We envision that the ensuring the security and privacy of Cyber-Physical systems is part of designing a resilient cyber-physical system. The grand challenge is really to provide continuous assurance of the operating objectives of CPS at any time and at all times. In order to achieve continuous assurance, we believe fundamental research efforts need to be devoted to the challenges faced by fine-grained isolation, real-world aware, risk-adjusted resource allocation, and closing the loop.

Acknowledgment

The authors would like to acknowledge Dr. Arthur Ciccolo, IBM Research Division, for his careful review and comment of the manuscript.

References

[1] Leadership under challenge: Information technology R&D in a competitive world. An assessment of the federal networking and information technology R&D program. Tech. rep., President's Council of Advisors on Science and Technology, August 2007.

[2] http://www.ibm.com/SmarterPlanet

[3] A. A. Cardenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," Cyber Physical System Security Workshop 2008, Irvine, CA.

[4] DOE. Smart Grid. Department of Energy, http://www.oe.energy.gov/smartgrid.htm, Accessed July 14 2008.

[5] EISENHAUER, J., DONNELLY, P., ELLIS, M., AND O'BRIEN, M. Roadmap to Secure Control Systems in the Energy Sector. Energetics Incorporated. Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, January 2006.

[6] GAO. Critical infrastructure protection. Multiple efforts to secure control systems are under way, but challenges remain. Tech. Rep. GAO-07-1036, Report to Congressional Requesters, September 2007.

[7] GAO. Information security. TVA needs to address weaknesses in control systems and networks. Tech. Rep. GAO-08-526, Report to Congressional Requesters, May 2008

[8] GREENBERG, A. America's Hackable Backbone. Forbes, http://www.forbes.com/logistics/2007/08/22/scada-hackersinfrastructure-tech-security-cx ag 0822hack.html, August 2007.

[9] GREENBERG, A. Hackers cut cities' power. In Forbes (Jaunuary 2008).