Self-Aware Industrial Control Systems through Cloud Based Autonomic Computing

Christopher Rouff*, Ali Tekeoglu*, Joseph Maurio*, Alexander Beall*
*Johns Hopkins University Applied Physics Laboratory, Critical Infrastructure Protection Group
email: {christopher.rouff|ali.tekeoglu|joseph.maurio|alexander.beall}@jhuapl.edu

***Abstract*—Critical infrastructure (CI) is being attacked and needs the ability to identify, protect and recover from attacks automatically. Autonomic Computing can provide self-awareness to critical infrastructure so that it can identify and continue to operate through attacks. In this paper, we propose a cloud-based autonomic computing manager that will give Industrial Control Systems (ICS) self-awareness to detect anomalies in their operation, protect themselves and self-organize with other critical infrastructure to thwart attacks.**

***Keywords*—Self-Aware Computing, Industrial Control Systems, Cloud Computing.**

I. Introduction

Historically, Operational Technology (OT) has run on air-gapped private networks; thus, security was achieved through lack of public network access. With the proliferation of cloud computing resources and the Industrial Internet of Things (IIoT) paradigm, OT networks are now connected to enterprise networks for remote access. The security of the ICS networks is now based on the security of the enterprise networks. This has left the ICS vulnerable to malicious actors who can compromise the enterprise networks, and laterally move to have full access to the ICSs components on the mission critical Supervisory Control and Data Acquisition (SCADA) networks.

Detecting malicious activities is now left to OT operators who must detect anomalies on the networks based on their experience and alarms, which malicious actors often circumvent. The autonomic managers will be able to automatically detect anomalies from learning normal OT network behavior and automatically defend the ICSs against attacks, collectively, at network speed.

There have been a number of high-profile attacks on critical infrastructure, including a water treatment plant and a pipeline [1]. If the water treatment attack had not been detected, many people could have been harmed. Though shutting down the pipeline did not cause direct injury, it did affect the economy by reducing the supply of gasoline and keeping people from getting to work.

If the actors wanted to make a major disruption to the economy, they could have attacked multiple facilities and caused major harm to people and businesses. By making critical infrastructure self-aware, these attacks could be thwarted, and other infrastructure could be informed of the attacks. This would cause OT to go into self-protection mode to prevent an attack on their systems and self-organize to recover.

Autonomic Computing (AC) [2] has as its vision the creation of self-managing systems to address today's concerns of complexity and total cost of ownership while meeting tomorrow's needs for pervasive and ubiquitous computation and communication. Providing security self-awareness to AC-controlled ICSs that can communicate attacks to other AC-controlled ICSs, and collectively defending against these attacks, can provide a higher level of assurance to critical infrastructure.

II. Related Work

This section presents, to the best of our knowledge, closely related work in the recent literature. In [3], authors describe two different approaches that can provide security assurances to cyber-physical systems: (i) Through the use of micro-services that reconfigure the systems dynamically during attacks or failures, researchers embedded ICSs with autonomic properties to allow them to automatically detect and recover from cyber-attacks and other failures. (ii) Resiliency of autonomous unmanned aerial systems are tested through intelligent agents in a modeling and simulation framework. Researchers in [4] investigated the autonomy of individual cyber-physical systems within a larger cyber-physical system-of-systems (CPSoS), and they looked into potentially insecure and unsafe situations as a result of failures in autonomy.

Another study surveyed the methods used for embodied self-aware computing systems, in application of areas of systems-on-chip control systems, health monitoring and condition monitoring in industrial production systems [5]. Embodied self-aware computing systems are compared to traditional embedded systems. They are defined as being significantly more flexible, robust and autonomous such that they can adapt to a wide range of environmental variation and can cope with deterioration and shortcomings of their own performance.

In [6], authors presented a unified framework for integrating Cyber Physical Systems (CPS) in manufacturing. They utilized an adaptive clustering method for interconnected systems and investigated a case study of self-aware machines by CPS integration. Researchers in [7] surveyed potential challenges that are important in the near future to achieve self-aware smart city objectives. They claimed that cyber-physical systems can extract awareness information from the physical world, thus a holistic approach from the physical to cyber-world is necessary for a successful smart city outcome.

III. Approach

In this paper, we propose a cloud-based autonomic

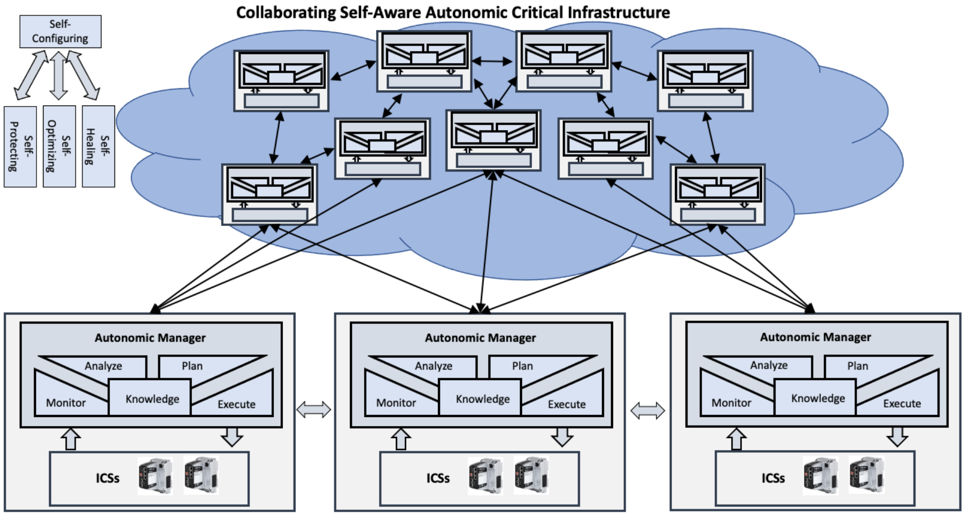

Fig. 1. Cloud Based Self-Aware Autonomic ICS

manager for ICS that will allow them to be self-aware [8] of their operating and computing environment and self-organize with other autonomic managers. Overall system architecture is depicted in Figure 1. Autonomic Computing provides self-awareness properties of self-configuring, self-healing, self-optimizing and self-protecting, among others (referred to as self-CHOP properties) [9].

The proposed design utilizes anomaly detection techniques for ICSs to identify deviations from normal operating conditions. Anomalies will be inputted to a model-base and reasoner in the autonomic manager to identify attacks and failures. Self-CHOP properties will also provide protection and self-healing through reconfiguration and re-optimization. An autonomic MAPE-K (Manage, Analyze, Plan, Execute, Knowledge) architecture will be implemented in the cloud. The cloud will provide the computing resources to store the models and perform the reasoning and computations to implement the self-CHOP properties. The cloud will also provide communications between ICS autonomic managers. This will allow for communication of attacks and provide for self-organization to protect and reconfigure CI components based on the type of attack and the effects on the ICS.

The novelty of the proposed work is the design of autonomic self-aware critical infrastructure that can identify anomalous activity in ICSs, act based on the threat and communicate that threat to other parts of the infrastructure to warn and collaborate with them. Infrastructure that would not be affected by a particular attack would only need to take minimal, or no action. The use of autonomic self-CHOP properties by ICS through cloud resources allows computationally constrained systems to still take advantage of the self-awareness that autonomic computing provides. Cloud-based autonomics prevents overloading an ICS, or needing to upgrade their memory and CPUs to handle the additional load of an autonomic manager.

The model-base and reasoning engine will implement the knowledge component of the autonomic MAPE-K architecture. It will provide the information to detect attacks, protect the ICS, heal, re-configure and re-optimize the ICS. The rest of the MAPE-K components provide the communications to the ICSs, analyze alternatives when attacked, plan and execute changes to the ICSs, communicate and self-organize with other autonomic managers about attacks.

IV. Conclusion and Future Work

In this paper, we proposed a cloud-based autonomic computing manager that will give ICS self-awareness to detect anomalies in their operation, protect themselves and self-organize with other critical infrastructure to thwart attacks. By working together, autonomic computing enhanced industrial control systems can provide the means for critical infrastructure to have security self-awareness and provide the needed robustness against attacks.

References

[1] E. Montalbano, “Florida Water Plant Hack: Leaked Credentials Found in Breach Database,” Feb 2021. [Online]. Available: https://threatpost.com/florida-water-plant-hack-credentials-breach/163919/

[2] R. Sterritt, “Autonomic Computing,” *Innovations in Systems and Software Engineering*, vol. 1, no. 1, pp. 79–88, 2005.

[3] J. Maurio, P. C. Wood, S. A. Zanlongo, J. Silbermann, T. I. Sookoor, A. Lorenzo, R. Sleight, J. Rogers, D. Muller, N. Armiger, C. A. Rouff, and L. A. Watkins, “Agile Services and Analysis Framework for Autonomous and Autonomic Critical Infrastructure,” *Innovations in Systems and Software Engineering*, pp. 1–10, 2021.

[4] M. Gharib, L. Dias da Silva, and A. Ceccarelli, “A Model to Discipline Autonomy in Cyber-Physical Systems-of-Systems and its Application,” *Journal of Software: Evolution and Process*, vol. 33, no. 9, p. e2328, 2021, e2328 smr.2328.

[5] H. Hoffmann, A. Jantsch, and N. D. Dutt, “Embodied Self-Aware Computing Systems,” *Proceedings of the IEEE*, vol. 108, no. 7, pp. 1–20, July 2020.

[6] B. Bagheri, S. Yang, H.-A. Kao, and J. Lee, “Cyber-Physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment,” *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 1622–1627, 2015, 15th IFAC Symposium on Information Control Problems in Manufacturing.

[7] L. Gurgen, O. Gunalp, Y. Benazzouz, and M. Gallissot, “Self-Aware Cyber-Physical Systems and Applications in Smart Buildings and Cities,” in *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2013, pp. 1149–1154.

[8] J. Cámara, K. L. Bellman, J. O. Kephart, M. Autili, N. Bencomo, A. Diaconescu, H. Giese, S. Götz, P. Inverardi, S. Kounev, and M. Tivoli, *Self-aware Computing Systems: Related Concepts and Research Areas*. Cham: Springer International Publishing, 2017, pp. 17–49.

[9] J. Kephart and D. Chess, “The Vision of Autonomic Computing,” *IEEE Computer Society, Computer*, vol. 36, no. 1, pp. 41–50, Jan 2003.