

# Chapter 33

## Autonomic Computing Architecture for SCADA Cyber Security

**Sajid Nazir**

*Firstco Ltd., London, UK*

**Shushma Patel**

*Faculty of Business, London South Bank University, London, UK*

**Dilip Patel**

*Faculty of Business, London South Bank University, London, UK*

### ABSTRACT

*Autonomic computing paradigm is based on intelligent computing systems that can autonomously take actions under given conditions. These technologies have been successfully applied to many problem domains requiring autonomous operation. One such area of national interest is SCADA systems that monitor critical infrastructures such as transportation networks, large manufacturing, business and health facilities, power generation, and distribution networks. The SCADA systems have evolved into a complex, highly connected system requiring high availability. On the other hand, cyber threats to these infrastructures have increasingly become more sophisticated, extensive and numerous. This highlights the need for newer measures that can proactively and autonomously react to an impending threat. This article proposes a SCADA system framework to leverage autonomic computing elements in the architecture for coping with the current challenges and threats of cyber security.*

### 1. INTRODUCTION

Cognitive computing relates to intelligent computing platforms that are based on the disciplines of artificial intelligence, machine learning, and other innovative technologies. These technologies can be used to design systems that mimic the human brain to learn about their environment and can autono-

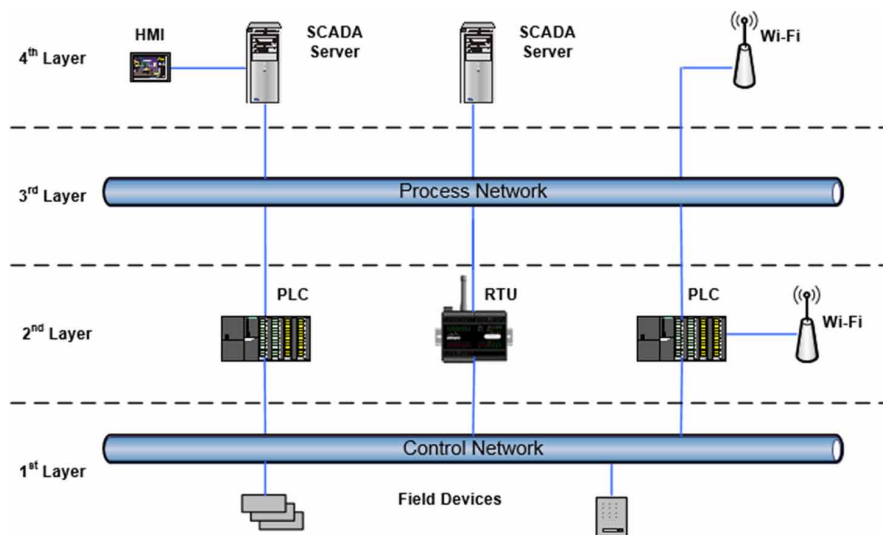
DOI: 10.4018/978-1-7998-2466-4.ch033

mously predict an impending anomalous situation. IBM first used the term ‘Autonomic Computing’ in 2001 to combat the looming complexity crisis (Ganek and Corbi, 2003). The concept has been inspired by the human biological autonomic system. An autonomic system is self-healing, self-regulating, self-optimising and self-protecting (Ganek and Corbi, 2003). Therefore, the system should be able to protect itself against both malicious attacks and unintended mistakes by the operator.

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control complex infrastructures of national importance such as transportation networks, power generation and manufacturing plants. SCADA systems can be visualised as a layered architecture, as shown in Figure 1. The field devices (sensors, etc.) at the lowest layer interact with the physical processes. At layer 2, the Programmable Logic Controllers (PLC), and Remote Terminal Units (RTUs) aggregate data values from the lower layer and communicate the commands and their responses through the communications network to the SCADA server and Human Machine Interface (HMI). The generation of commands at the top layer and collection of responses from the lowest layer results in the monitoring and control of the process. The applicability of SCADA systems has become widespread due to industrial automation, cost reduction and growth in global economies (Nazir et al., 2017).

Traditionally, SCADA systems were developed as closed systems with security being the overriding factor, and no Internet connectivity. However, to leverage efficiency and gain a competitive advantage, the systems are increasingly becoming connected to the Internet and cloud technologies. SCADA system security vulnerabilities were first highlighted by the Stuxnet attack (Karnouskos, 2011). Subsequently, there has been an increase in the frequency and sophistication, of the attacks as evidenced by Constantin (2014).

*Figure 1. Layered architecture of a SCADA system*



Isolation and obscurity as a mechanism for protection is no longer an option for critical infrastructures (Mahoney and Gandhi, 2011). At the same time systems are getting so complex that it is difficult to develop effective defence strategies, as there is a lack of understanding of the complex interactions

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/autonomic-computing-architecture-for-scada-cyber-security/251448](http://www.igi-global.com/chapter/autonomic-computing-architecture-for-scada-cyber-security/251448)

## Related Content

---

### Mitigating Cyber-Attacks in Cloud Environments: Hardware-Supported Multi-Point Conceptual Framework

Jitendra Singh (2021). *International Journal of Cyber Warfare and Terrorism* (pp. 43-57).

[www.irma-international.org/article/mitigating-cyber-attacks-in-cloud-environments/289385](http://www.irma-international.org/article/mitigating-cyber-attacks-in-cloud-environments/289385)

### The Threat of Cyber Warfare in the SADC Region: The Case of Zimbabwe

Jeffrey Kurebwaand Kundai Lillian Matenga (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1485-1505).

[www.irma-international.org/chapter/the-threat-of-cyber-warfare-in-the-sadc-region/251505](http://www.irma-international.org/chapter/the-threat-of-cyber-warfare-in-the-sadc-region/251505)

### Commissioning Development to Externals: Addressing Infosec Risks Upfront

Yasir Gokce (2021). *International Journal of Cyber Warfare and Terrorism* (pp. 30-40).

[www.irma-international.org/article/commissioning-development-to-externals/281631](http://www.irma-international.org/article/commissioning-development-to-externals/281631)

### Evaluating the Strategic Consequences of Cyber Targeting Strategies on Road Transport Networks: A Case Study of Washington DC

Skanda Vivekand Charles Harry (2022). *International Journal of Cyber Warfare and Terrorism* (pp. 1-14).

[www.irma-international.org/article/evaluating-the-strategic-consequences-of-cyber-targeting-strategies-on-road-transport-networks/314942](http://www.irma-international.org/article/evaluating-the-strategic-consequences-of-cyber-targeting-strategies-on-road-transport-networks/314942)

### Security Integration in DDoS Attack Mitigation Using Access Control Lists

Sumit Kumar Yadav, Kavita Sharmaand Arushi Arora (2021). *Research Anthology on Combating Denial-of-Service Attacks* (pp. 207-229).

[www.irma-international.org/chapter/security-integration-in-ddos-attack-mitigation-using-access-control-lists/261979](http://www.irma-international.org/chapter/security-integration-in-ddos-attack-mitigation-using-access-control-lists/261979)