

Autonomic Renewable Energy Management of Biosphere 2 Smart Grid

by Don Cox, Malaz Mallouhi, Youssif Al-Nashif, and Salim Hariri

As energy critical infrastructures (power, water, gas and oil) starting to modernize their industrial control systems to build what is referred to as “Smart Grid” that uses advanced computing and communications technologies to bring knowledge to power grid so it can operate far more efficiently. The widespread use of Supervisory Control and Data Acquisition (SCADA) systems in critical energy infrastructures (gas, oil, and electrical power) makes them vulnerable to both internal and external attacks. To make the matter even worse, SCADA systems were never designed with security in mind and securing them is a challenging research problem. Consequently, SCADA networks become a prime target for cyber attacks due to the profound and catastrophic impacts they can inject to our economy and all aspects of our life. For example, the largest blackout in North American history, which is occurred in August 2003, covered 9,300-square-mile area and affected around 50 million people could have been triggered by a national cyber terrorism act. Furthermore, a CIA analysts reported that hackers controlled foreign utilities and control lights in several cities.

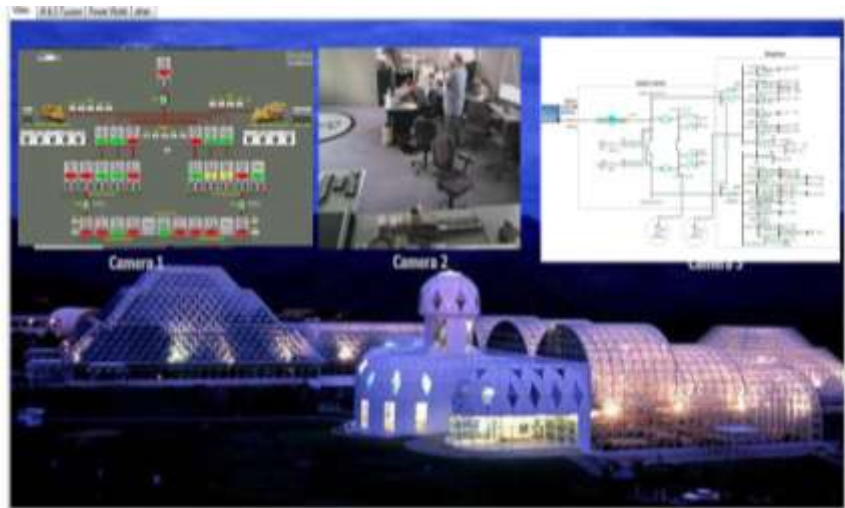
With the explosive increase in the number, complexity and the speed of malicious attacks it becomes no longer feasible to identify all types of attacks and build defenses against them. Current security techniques that are signature

base and manual intensive will not be able to provide the required security and protection for our critical energy infrastructures that are controlled and managed by SCADA systems.

The UA NSF CAC researchers are collaborating with our industrial members Raytheon and AVIRTEK to develop autonomic management testbed for protecting and managing renewable energy resources at the UA Biosphere 2 (see Figure 1). Our implementation approach utilizes autonomic agents, online monitoring, feature selection based on information theory, multi-level behavior analysis of SCADA systems and networks, decision fusions based on statistical and data mining techniques, automated/semi-automated protection actions, visualization and adaptive learning.

The topology of the smart renewable energy testbed that is currently implemented by Raytheon, AVIRTEK, and University of Arizona at the Biosphere 2 (B2) is shown in Figure 2. The main goal of the testbed is to experiment with and evaluate the integration of Raytheon ATaRS™ and AVIRTEK AND and Autonomic agents to achieve the following objectives: 1) Autonomic control and management of different power generation technologies; 2) Integrate Raytheon Autonomic Tracking and Respond System (ATaRS™) with AVIRTEK AND system and Autonomic agents to secure and protect B2 smart grid resources and services; 3) Evaluate the autonomic protection strategies against cyber and physical attacks. The testbed will be an invaluable resource to develop, experiment with and evaluate the proposed A-IPS functions and services.

The Raytheon ATaRS™ is an information system that provides near real-time actionable intelligence on asset location, environment and status. It provides mobile or stationary asset monitoring with minimal infrastructure required to establish usage of ATaRS™ in a mobile or stationary setting. It forms a mesh network system



that consists of controllers and nodes to provide a persistent network in ATaRS™ autonomously self-organize their communication paths which allow data to move from any controller to any node and vice versa. The nodes regularly exchange information about relative location and signal strength between themselves and use that information to restructure the network to minimize power consumption and maintain communication paths when devices move, go out-of-range, or fail – a self-healing capability.

The ATaRS system will be used to instrument portions of the B2 electrical micro-grid. These sensors have been modified to interface directly to the existing B2 commercial off the shelf monitoring and control equipment. ATaRS sensors are also being placed in the Tropical Rain Forest Biome to provide environmental data for use by B2 scientists. The collected data is stored in computer servers featuring an Oracle Database Management System providing standardized retrieval of the data by B2 scientist.

In what follows, we briefly describe how the testbed can be used to experiment with and evaluate the A-IPS important security capabilities.

The ATaRS™ sensors (video surveillance, cameras, motion sensors, electronic access control) and secure communications will keep the intruders off the premises. The 24 by 7 continuous monitoring will significantly reduce the amount of time it takes facilities personnel and operations teams to respond to incidents across the grid.

The observer and controller modules of A-IPS will play a critical role in the overall security strategy. Access to the systems, be it local or remote, should be granted only who are authorized to access these resources. By continuous monitoring who is accessing the system resources and verifying their access rights, we will be able detect any unauthorized access or malicious activities.

The continuous monitoring and analysis of the configurations of the routers, firewalls and servers, we can automatically change their configurations, security policies, and update their firmwares to make them more secure and remove any vulnerabilities that can be exploited by new types of cyber attacks.

The multilevel behavior analysis to be performed by the A-IPS observers will implement an effective layered detection and consequently defense through the controller actions against Denial of Service (DoS) attacks, Control Application Attacks, Network based attacks, and Host based Attacks. The AND system developed by UA

researchers and AVIRTEK has successfully been used to protect against all cyber attacks known or unknown with high detection rates and low false alarms.

The A-IPS provide a very secure and encrypted communication services that will be critical to secure the data storage and transmission. In addition, the A-IPS observer and controller will enforce multi-level in-depth defense to secure the access to the data; intruders will need to break into many layers of defense mechanisms before they can access the data. Our multi-level anomaly behavior analysis will provide us with effective mechanisms to detect any sophisticated malicious attack on the data.

