Security and Survivability of Large Scale Critical Infrastructures

John Bigham

Electronic Engineering
Queen Mary, University of London
John.Bigham@elec.qmul.ac.uk

At the heart of a large complex critical infrastructure (LCCI) such as an electricity distribution or telecommunications network, is a management network consisting of a number of interconnected computers running server, database, monitoring and control software. This management network is vulnerable to attacks because it is often connected to a number of IP networks as well as to the public telephone network, switches, routers and remote terminal units interfacing with sensors. Operator mistakes and malicious insiders can also damage the management network and the system.

Guardians of LCCIs need to monitor and protect the system at a number of different levels. The CEC funded project Safeguard project plans to build agent system components to manage this. Low-level agents will build up models of the normal operation of the software and data in their local environment. These will communicate with higher-level agents with an overview of the system that will build up or use a model of normality within a broader context. Once an abnormality has been detected, a response to protect the network will be carried out. Low-level agents will initiate a fast protective response at a local level, while high-level agents will be responsible for a more sophisticated diagnosis of the problem and a system-wide response.

The objectives of the Safeguard system

What Safeguard will try to do is to construct a unified system architecture (across different LCCIs that can manage the resources so as to robustly provide the services offered. This will consist of) dynamic components that can observe the world and can perform actions that change the allocation of resource or inform third parties. These dynamic components can be at different levels of abstraction and will co-operate with each other. The general architecture of the Safeguards agents is illustrated in the figure 1. Each agent is comprised of several intelligent components with different roles (c.f. striker or defender) and must co-operate to fend off chance circumstances and deliberately hostile acts. Interaction between agents is through the co-ordination layers in the agent. Here the agents are shown located at each control centre, though the architecture is not yet decided. Different components will have different roles and components communicate within the layers of the agent. An aim of the project is to find a solution that fits the requirements of the domains, which is scaleable and is dependable, and not just one that corresponds to an over simplified structure.

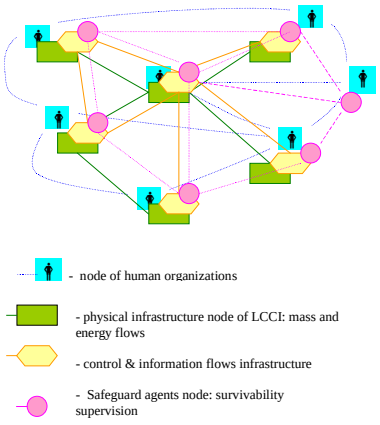

Fig. 1. An illustration of networked layers of a LCCI with the SAFEGUARD agency layer

There are two important kinds of action that can compromise the system and that Safeguards must detect

1. Intrusion attacks and system failures: This includes prevention of intrusion attacks on the software of the controllers and prevention and detection of other malfunctions of the controllers (either by hardware failures in actuators or software bugs in the controlling software) of the system at all layers. This not only includes the controllers in the physical layer of the system, but also attacks on and other mishaps associated with the configuration and reconfiguration management software. In the telecom domain attacks and failures on the latter are considered more likely and potentially more damaging than attacks on individual element control software because of their scope. Also many response mechanisms already exist for failures in the physical layer, though perhaps not yet for those caused by attacks on the element controlling software.
2. Unexpected behaviour due to modifications to the management and control software when service or structure changes: Software in large systems is continually changing and mechanisms to flag errors and to give indicators of unusual conditions are essential

The availability of expert knowledge in the management of attack detection, resource reallocation, failure mitigation etc. is needed. It is not our intention, for example, to replace existing diagnostic mechanisms for the network, but to design and develop a system of agents that can interface with existing (legacy) software, each with different but coordinated roles, that together ensure the survivability of the system. For example, an in house diagnostic system could be wrapped in an agent wrapper so that it also can communicate with the SAFEGUARD agent that has a diagnostic role.