Introduction

The process control of utility infrastructures is based on the SCADA (Supervisory Control and Data Acquisition) systems which yield the operational ability to acquire data, supervise and control whatever is the business in question (electricity, water, gas, telecom). However, they also have interconnections to the standard corporate intranets, and hence indirectly to the Internet (e.g., remote access via dedicated or public networks). The aforementioned SCADA systems were classically not designed to be widely distributed and remotely accessed, let alone be open. They grew-up standalone, closed, not having security in mind. Today, widely distributed monitoring, protection and control systems, implementing special protection schemes over the power transmission network, are emerging whose architecture is based on open communication infrastructures. This opening that we observe nowadays is an afterthought in the line of the generic trend of any informatics system. Whilst it seems non-controversial that such a status quo brings a certain level of threat, namely but not only through interference, we know of no work that has tried to equate the problem by defining a generic model of “utilities distributed systems architecture”.

In fact, the above-mentioned hazardous evolution led to the inevitable: access to operational networks such as remote SCADA maneuvering, ended up entangled with access to corporate intranets and public Internet, without there being computational and resilience models that understand (represent) this situation and deal with the resulting interference. The damage perspectives that may result from this exposure are overwhelming. They range from wrong maneuvering, to malicious actions coming from terminals located outside, somewhere in the Internet. The potential targets of these actions are computer control units, embedded components and systems, that is, devices connected to operational hardware (e.g., water pumps and filters, electrical power generators and power protections, dam gates, etc.).

In the electrical power provision these situations have already been experienced by citizens in various parts of the world. One particularly nasty failure is the cascading failure: as highlighted in the analysis report of a major failure in 2003 [2], it was the failure of various information systems that thwarted the utility workers’ ability to contain the blackout before it cascaded out of control, leading to an escalating failure, characteristic of interdependent critical infrastructures. This type of failure will be a first-order citizen in our research agenda.

Background and Research Challenges

The main challenge for the European CRUTIAL project is to make power control resilient in spite of threats to their information and communication infrastructures. Considering the crucial role of control systems in governing the quality and the stability of the electric power service, it is considered of great importance for the utilities operating the infrastructures to dispose of tools for analyzing threat impacts and of technologies for avoiding, or limiting, most serious consequences. In what follows, we present a brief overview of the state of the art on the major topics involved, and the basic research challenges that the CRUTIAL consortium has identified.

Countries and industrial associations have been attentive to the problem, having produced analyses, studies and recommendations, such as interdependency analyses and models, assessment of cyber risk to power control systems, studies of electronic security in manufacturing and control systems environments, or establishment of process control security requirements [3,6]. Research initiatives and activities related to the protection of critical infrastructures and security of information and SCADA in electric power systems were launched in the USA and Europe [4,5]. On the practical side, real test beds for the simulation of attack scenarios to power control and management systems have been built [7].

A large body of research exists on the dependability analysis and evaluation of computer based infrastructures [14]. As regards malicious threats, new approaches have been proposed recently for the quantitative evaluation of security based on probabilistic modelling [8], and to the study of interdependencies and their impact on critical outages [9]. Some pioneering work addressing this problem [15] must now be complemented by the definition of a comprehensive framework for the modeling and evaluation of resilience taking into account malicious faults as well as accidental faults. An additional relevant issue is the problem of modeling interdependencies in a context
characterized by different operation phases and regimes, which can be handled by stochastic models for multi-phased systems [13].

Regarding resilient distributed real-time architectures, there is a reasonable body of research, both in the fields of fault tolerance, and of security. A unifying approach has slowly emerged during the past decade, and gained impressive momentum recently: intrusion tolerance. In short, instead of trying to prevent every single intrusion or fault, these are allowed, but tolerated: the system has the means to automatically trigger mechanisms that prevent the intrusion from generating a system failure. A number of isolated works, mainly on protocols, took place that can be put under the IT umbrella, but only recently did the area develop significantly, with two main projects OASIS and MAFTIA [10], respectively in the US and the EU, doing structured work on concepts, mechanisms and architectures. Some recent results on protocols resilient to malicious faults and on architecting and programming with trusted components open interesting prospects on how to simultaneously tolerate faults and intrusions on critical utility infrastructures [11].

Research Agenda

The project focuses on the electrical power infrastructure and the information infrastructures, by considering different topology realms and different kinds of risks:

- distinguishing the backbone from the specific information networks and from the control and monitoring infrastructures, as they usually have different levels of protection requirements;
- distinguishing faults of different kinds and severities, such as electric power outages and cyber attacks;
- handling all faults (accidental and intentional malicious) under common approaches and mechanisms.

In order to master the complex mechanisms of global failures particular focus should be put on the study and modeling of the types of failures that are characteristic of interdependent critical infrastructures. Although the modeling of such failures has received increasing interest in the last years [12] after the large blackouts of electric power transmission systems in 1996 and 2003, this problem is still open and further developments are needed:

- cascading failures that occur when a disruption in one infrastructure causes a failure in a second one;
- escalating failures that occur when an existing failure in one infrastructure exacerbates an independent disruption in another infrastructure, increasing its severity or the time for recovery and restoration;
- common cause failures that occur when two or more infrastructures are affected simultaneously by some common cause.

On the other hand, in order to effectively withstand the above-mentioned combinations of faults and intrusions, and handle them in an automated way, the study of resilient architectures devoted to the critical utilities infrastructure problems are included in our research agenda:

- architectural configurations that induce prevention of the more severe interaction faults, and of attack and vulnerability combinations;
- middleware devices that achieve tolerance of the remaining faults/intrusions (architectural blocks, protocols);
- sophisticated system monitoring mechanisms.

References


