Experiment Based Validation of CIIP

Per Mellstrand and Rune Gustavsson

Blekinge Institute of Technology
per.mellstrand@bth.se, rune.gustavsson@bth.se

Abstract. The connection between critical infrastructure Protection (CIP) and critical information infrastructures protection (CIIP) is a major research area. We describe our view of how a combined experimental approach can be used to build targeted resilient software required for critical infrastructure.

Keywords: Critical Infrastructures, Resilient Software, Vulnerability Assessment.

1 Protection of Critical Information Infrastructures

Critical Infrastructure Protection (CIP and Critical Information Infrastructure Protection (CIIP) are in focus of ongoing R&D efforts worldwide. Among the most important critical infrastructures we find energy system in most listings and investigations. Critical Information Infrastructures is a rather late focus area of R&D. From one point of view this is very natural since critical infrastructures are often connected with, or are embedding of, information infrastructures. In fact, much of the critically (vulnerability) is due to the dependencies between those infrastructures. However, at this point there is no consensus what a CIIP would be. There are several EU project aiming at increasing our understanding in the subject areas in order to identify suitable direction of future R&D [1][2].

In this paper we advocate an experiment-based approach towards identifying and pursuing a principled research agenda towards CIIP. The following Figure 1 illustrates our experimental set up as well as our approach.

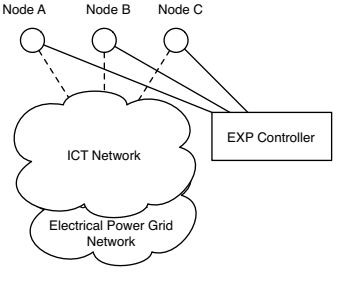

Fig. 1. Experimental Environment with nodes. The network contains both physical and simulated parts.

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 15 – 29, 2006.

Firstly, we believe that it is advantageous to study embedded CII in a CI rather than an isolated CII focus. That kind of investigation might be purposeful when we have a better understanding of the underpinnings of CII. Secondly we will use the figure to pinpoint the goals and contributions of the paper.

1.1 The Anatomy of Critical Information Infrastructures

The purpose of an embedded CII is to drive the corresponding CI in a proper way. In this metaphor the role of information is comparable to that of energy in many CIs. In fact many of our CI are derived and created from the industrial revolution during the last couple of centuries. Understanding of the concept of energy came rather late in that revolution (mid 1850´s) and after the invention and use of energy-based artifacts such as the steam engine. But an understanding of energy allowed us to transform energy in suitable forms and transport it to the point of use as well a enabling new kinds of energybased products and services (Radio, telecommunications and TV). In a sense the industrial revolution led to and was dependant on a proper understanding of energy. That understanding was indeed an emergent property and enabler of the industrial revolution. In fact, the energy metaphor of information was also a basic underpinning of the ongoing efforts on GRID computing [3]. Our point of view is, however, that the energy metaphor of information is oversold and does not guide us in understanding the role of information in the ongoing building up of an information society [4].

Given the embedding of a CII in a CI (energy system) of Figure 1 we can identify the following types of information:

- I_1 Control information interpreted by users. Information from the ICT networks supporting monitoring and user driven system actions of the CI and CII.
- I_2 Intra system information exchange: Information between the two critical infrastructures CI and CII.
- I_3 Information enabling processes: Typical information (code) that enable proper running of software of the systems.

Furthermore, we note that the greatest causes of system complexity and vulnerabilities are in the different interfaces between system components and that the glue of critical systems, of both kinds, is software. Or, to quote from [13]: ‘‘This leaves SCADA/EMS as the vulnerability of greatest concern. Unfortunately, SCADA/EMS components – computers, networks, and software – will remain complex and unreliable for a long time because securing an information system is well known to be problematic. Thus far, it has been impossible to build software that is guaranteed to be bug-free. These software flaws leads to networks becoming disconnected, data being lost, and computers being disabled. As long as software is flawed, there will be faults in industrial control systems such as SCADA and EMS’’. A recent report on infrastructure interdependencies where fault reports from 12 years were analyzed concluded that software faults, including malicious logic and authorization violation, constitues for more than 65% of all faults [14].

From the information security research community we have the following CIA-model of information protection: