Chapter 71
Safety and Security in SCADA Systems Must be Improved through Resilience Based Risk Management

Stig O. Johnsen
The Norwegian University of Science and Technology, Norway

ABSTRACT

This chapter describes vulnerabilities related to safety and security in distributed process control systems integrated with information and communication technology (ICT). The author describe key vulnerabilities and how to mitigate these vulnerabilities by current best practices, which have worked in an industrial setting in Norway. Distributed process control systems are denoted as SCADA systems, i.e. supervisory control and data acquisition systems. Increased networking and increased use of ICT impacts the complexity and vulnerability of the SCADA systems. To improve safety and security, there must be a focus on systematic knowledge generation between ICT and process experts and a focus on exploring resilience as a strategy to manage risks and support continuity of operations (resilience seen as the ability to bounce back and sustain operations). Best practices in risk management in this area are to establish policies, improve risk awareness, perform risk assessment in collaboration between ICT and SCADA professionals, focus on segregation of networks, focus on active protection against malicious software, improve reporting and sharing of incidents, and establish and explore disaster/recovery plans. In addition, there should be focus on certification and testing of components in ICT and SCADA systems and improvement of resilience to mitigate uncertainty and complexity.

DOI: 10.4018/978-1-4666-4707-7.ch071

INTRODUCTION: SAFETY AND SECURITY MUST BE IMPROVED

This chapter consists of the following five parts:

- This introduction, where we have argued that integration of SCADA systems with ICT systems creates new vulnerabilities and uncertainties that must be mitigated through improved risk assessment and improved risk governance.
- Description of a general framework and best practice guidelines that have been implemented in the Norwegian Oil and Gas sector to support risk governance of integration of SCADA and ICT.
- Description of how to assess the use of the framework and the guidelines.
- Documentation of the actual use of the guidelines and how safety and security have been impacted.
- Discussion of the impact of the guidelines and suggested improvements in the future.

Distributed process control systems are a key part of industrial production. In the following we are focusing on process control systems used in the oil and gas industry. SCADA (i.e. supervisory control and data acquisition systems), is used when we describe distributed process control systems, that is systems that monitor and control industrial processes, including safety instrumented systems used to perform emergency shut down or emergency disconnect. Safety and security are key issues in SCADA systems. In the following commentary safety is defined as *the degree to which accidental harm is prevented, reduced and properly reacted to* and security is defined as *the degree to which malicious harm is prevented, reduced and properly reacted to* (both definitions are taken from Firesmith (2003)). Thus the avoidance of harm is dependent on both safety and security.

Initially, SCADA systems were independent and based on specialized hardware and software. Hardware consisted of networks with remote terminal units (RTU) or by programmable logic controllers (PLC). However, SCADA systems are no longer independent and based on specialized technology, but are increasingly connected to local and public networks and are often based on standardized commercial "off the shelf" technology (COTS). The SCADA systems are increasingly communicating with other ICT systems in real time and communicating with distributed users connected to the different networks. The SCADA systems are consisting of many interrelated systems and interrelated users. It seems that complexity and connectivity is increasing, defining complexity as a system *consisting of many interrelated parts*, from Perrow (1999).

Increased connectivity has exposed the SCADA systems to a wide range of security issues, as described by Igure, Laughter and Williams (2006) and Stouffer, Falco and Kent (2008). Key challenges and security issues mentioned by these papers are access controls, monitoring of activities and management policies. If these challenges are not managed, incidents may happen. In a SCADA environment the incidents may impact safety, since the SCADA systems are controlling key industrial processes. A study by the National Transportation Safety Board in 2005, NTSB (2005), scrutinized 13 pipeline mishaps from 1992 to 2004. The study found key issues from the mishaps related to the SCADA systems. In 10 of these accidents, some aspect of the SCADA system contributed to the severity of the accident. However, NTSB didn't perform systematic exploration of the role of SCADA systems in gas line accidents earlier. They started to perform systematic exploration from 2010. Thus there is a need for increased focus on SCADA systems and their role in accidents and support of safety in operations.

Examples of serious incidents from operation of SCADA systems can be found in Stouffer, Falco and Kent (2008). One example mentioned is the Maroochy Shire Sewage Spill, where a disgruntled employee broke into the controls of a