Chapter 8

ENHANCING THE SAFETY, SECURITY AND RESILIENCE OF ICT AND SCADA SYSTEMS USING ACTION RESEARCH

Stig Johnsen, Torbjorn Skramstad and Janne Hagen

Abstract This paper discusses the results of a questionnaire-based survey used to assess the safety, security and resilience of information and communications technology (ICT) and supervisory control and data acquisition (SCADA) systems used in the Norwegian oil and gas industry. The survey identifies several challenges, including the involvement of professionals with different backgrounds and expertise, lack of common risk perceptions, inadequate testing and integration of ICT and SCADA systems, poor information sharing related to undesirable incidents and lack of resilience in the design of technical systems. Action research is proposed as a process for addressing these challenges in a systematic manner and helping enhance the safety, security and resilience of ICT and SCADA systems used in oil and gas operations.

Keywords: Oil and gas sector, ICT/SCADA systems, action research

1. Introduction

Process management systems used to control oil and gas production incorporate traditional information and communications technology (ICT) systems and supervisory control and data acquisition (SCADA) systems. SCADA systems are often integrated with safety instrumented systems (SISs). Real-time production data is shared between these systems to conduct vital operations at oil and gas facilities.

Process management systems used in oil and gas operations leverage several technologies. The ICT infrastructure consists of networking equipment, production systems (e.g., enterprise resource planning systems), maintenance systems, telephone support systems, radar and video systems (e.g., closed-circuit television and VHF radio systems). Process control systems used in production

include various field devices, including sensors and actuators. SISs are used for emergency shutdowns and to prevent fire and gas emissions.

Over the years, SCADA systems have evolved from proprietary stand-alone systems to commodity networked workstations that are frequently connected to the Internet. The use of personal computing technology and the interconnectivity of production systems and the ICT infrastructure lead to increased vulnerabilities and threats. Meanwhile, dependencies between the various systems and technologies are increasing. The operating environment is also becoming more complex, involving a multitude of highly-specialized professionals from different organizations and located at widely-dispersed sites.

The consequences of an accident at an oil and gas facility can be catastrophic. However, due to the complex infrastructure and operational environment, it may be impossible to foresee what may go wrong [20]. Consequently, ICT and SCADA systems should be resilient in the face of undesirable incidents. Barriers should be established between systems to protect against common failures. Safety guidelines and information security best practices should be implemented to the maximum extent.

ICT and SCADA systems should be safe, secure and resilient. Safety is the "freedom from unacceptable risks" [6]. Information security involves the protection of information assets from unauthorized access, use, disclosure, disruption, modification and destruction by providing high levels of confidentiality, integrity and availability. Resilience is "the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress" [6]. Resilience must be designed into technical systems, the organization and in the workforce.

Two pressing questions in the oil and gas sector are: What is the status of safety, security and resilience of ICT and SCADA systems used in oil and gas operations? How can vulnerabilities be mitigated in order to improve safety, security and resilience?

We conducted a survey of personnel at 46 Norwegian offshore oil and gas installations to assess the levels of safety, security and resilience in ICT and SCADA systems. The survey was mainly based on epidemiological accident models. We assumed that accidents have complex linear dependencies and occur as a result of unsafe acts in combination with weak defenses (i.e., accidents are caused by the lack of barriers or by holes in barriers [6, 15, 16]). The barriers include human factors, technical factors and organizational factors. Defenses and barriers are important aspects of any security model; they reduce the likelihood of undesirable incidents and reduce their consequences. In addition, we attempted to assess system complexity and identify tight couplings based on systemic models (with complex, non-linear relationships). A key objective was to gather data related to "normal accidents" as described by [14], and to identify the likelihood of occurrence and the overall risk in oil and gas facilities.

2. Oil and Gas Industry Survey

Before designing the questionnaire, we conducted a series of workshops and interviews to identify some of the key vulnerabilities introduced by the use of commodity computing and network resources in oil and gas facilities [10]. Some vulnerabilities were identified, including the susceptibility to virus infections and denial-of-service (DoS) attacks. Our earlier work [10] indicated that the key issues to explore were the use of personal computing technology in SCADA systems; the degree of networking between Internet, ICT systems, SCADA systems and SISs; common failures; risk perceptions; and the lack of awareness about vulnerabilities.

The survey questionnaire was designed to identify the types of ICT and SCADA systems used along with their vulnerabilities. The questionnaire covered four areas: (i) general information; (ii) the connections between systems; (iii) the common infrastructure and the possibility of common failures; and (iv) the level of established risk assessments and the barriers to mitigating the risks. The questions could be answered using Yes/No responses. In addition, the respondents were encouraged to provide free-form comments.

Questionnaires were distributed to 46 installations and were mostly completed by operators; typically, individuals responsible for the SCADA systems at the installations and who worked closely with suppliers. All 46 questionnaires were completed. However, only a qualitative assessment of the results can be provided because Yes/No answers were rarely given; in most cases, the respondents provided comments along with qualifying statements.

Additional information was solicited from the respondents after the survey to clarify several issues that arose when analyzing their responses. In retrospect, the questionnaire and terminology could have been more precise. Also, due to differences in the background and expertise of the respondents and the ICT/SCADA infrastructure at their installations, working group meetings and interviews should have been conducted first. The original questionnaire should then have been adjusted based on the respondents' comments, and a more precise questionnaire should have been distributed later.

The survey and the subsequent discussions yielded several key results:

- **Poor Risk Awareness:** Only five of the 46 installations had performed risk analyses related to the integration of ICT and SCADA systems. ICT professionals and SCADA professionals collaborated on risk analysis efforts at only eight of the 46 installations. ICT and SCADA professionals used different standards and procedures to assess risk. In particular, ICT professionals employed standards such as ISO/IEC 27002 while SCADA professionals used safety standards such as IEC 61508.

- **Lack of Consistent Safety/Security Guidelines:** Three installations did not apply safety and/or security guidelines for ICT/SCADA systems. In twenty cases, various guidelines were referenced; however, we were unable to find even one concise guideline that contained all the relevant material.

- **Absence of Systematic Knowledge Sharing:** Information about undesirable incidents had not been shared among the relevant actors. Two installations had no procedures for reporting ICT/SCADA incidents. One organization used three different reporting systems.

- **Poor Scenario Training and Emergency Preparedness:** A set of undesirable incidents that could be explored as the basis for emergency training had not been identified. Emergency preparedness plans to handle ICT/SCADA infrastructure failures had not been developed nor had scenario-based training been performed. Also, systematic awareness training had not been performed.

- **Lack of System Certification:** SCADA systems were not certified as being resistant to DoS attacks involving large volumes of ICT network traffic (e.g., using Achilles from Wurldtech Security or ISA certifications [8]). However, surveillance and testing of network traffic was conducted at seventeen installations.

- **Common Components and Failures:** SCADA systems and SISs often had common power supplies, operator stations and network components, which significantly increased the probability of common failures. Furthermore, SCADA systems and SISs from the same vendor were closely related and had many common components. While no failures of SISs have been reported (e.g., in the Industrial Security Incident Database (ISID) [19]), stress tests have uncovered vulnerabilities that can influence SIS operation. These vulnerabilities have been prioritized for mitigation by vendors.

- **Lack of Network Barriers:** Few barriers existed between SCADA systems and SISs (e.g., using firewalls or network segmentation). Furthermore, network design best practices (e.g., [7]) were not employed. Poor network design can affect resilience; malfunctions and DoS attacks can impact SCADA systems and SISs.

- **Poor Standardization:** Standardization across companies was lacking and different solutions had been established within the same company. This created a more demanding operational environment because remote support was more complex. At the same time, different solutions can enhance resilience because the same vulnerability is not necessarily present in all the solutions. However, most of the installations used Windows platforms with Ethernet (TCP/IP) for communications.

- **Inadequate Deployment of Patches:** Patches should be deployed immediately after they are made available to address vulnerabilities, protect against attacks and enhance resilience. In general, the ICT infrastructure and applications were centrally administered and patched. However, the SCADA systems were administered and patched locally. The deployment

of patches in SCADA systems varied: some SCADA systems were not patched systematically while some systems were not patched at all.

- **Inadequate Review of Firewall Logs:** In general, firewall logs were not reviewed and analyzed. There were several cases where logs were not inspected due to high workload or other factors.

3. Addressing the Challenges

The survey results indicate that several challenges exist related to safety, security and resilience in oil and gas facilities. To address these challenges, we consider four key phases used in resilience engineering [6]:

- **Anticipation:** Knowing what to expect (potential).
- **Attention:** Knowing what to look for (critical).
- **Response:** Knowing what to do (actual).
- **Learning:** Knowing what has happened (factual).

According to resilience engineering, an organization that focuses on anticipation, attention, response and learning can mitigate risks and improve safety and security. In the following, we discuss the notions of anticipation and response in the context of the survey results.

3.1 Anticipation

The results of the survey indicate that there is a lack of anticipation about what can go wrong and a lack of attention when something unexpected happens. This is because there is poor risk awareness, no systematic risk assessment and no systematic sharing of information about incidents. Since most organizations do not have safety and/or security guidelines in place, it is difficult to establish anticipation and attention based on formal procedures. Also, the relative absence of formal certification and qualification procedures for ICT/SCADA systems implies that the organizations are uncertain about system resilience and the ability of the systems to handle unanticipated loads and DoS attacks. System tests [11] and actual incidents such as the one at the Browns Ferry nuclear plant [13] demonstrate that ICT/SCADA systems have significant vulnerabilities and are susceptible to DoS attacks.

Common components lead to common failures; however, because risk analyses were not performed at the oil and gas facilities that participated in the survey, there was limited awareness about this issue. Also, networks were not systematically segmented, which can lead to unanticipated problems. Poor standardization often leads to unanticipated results. However, the lack of standardization may, in fact, increase resilience – with different technical solutions at the 46 installations, it would be practically impossible to have a common failure at all the installations. Some of the systems were complex and had tight

couplings, which increase the likelihood of "normal accidents." The evaluation of the connections between complex, tightly-coupled systems and incidents is an important topic that deserves further investigation.

3.2 Response

Learning from incidents is perceived to be a challenge because of the lack of systematic information sharing about incidents. The resilience of individual installations with respect to ICT/SCADA incidents is also expected to be poor. Due to the robustness of SISs, an incident would likely result in a production shutdown, but this can be very costly – around $1 million per stoppage. In the event of a health, safety and environmental incident, an SIS would be expected to shut down the system or, at the very least, move it to a safe state. However, the SIS itself can fail (albeit with very low probability), but the consequences are major [20]. Implementing the correct response to such an incident is a definite challenge because of inadequate scenario training and emergency preparedness. Clearly, it is extremely important to enhance the resilience of ICT/SCADA systems through increased awareness, training and organization.

3.3 Mitigation Actions

Anticipation, attention, response and learning are key to enhancing resilience. The anticipation of undesirable incidents by ICT and SCADA professionals can be improved by having them participate in risk assessment studies where potential scenarios are identified and explored; this helps create common awareness and anticipation. ICT and SCADA personnel should gain a common understanding of risks and mitigating actions and, ideally, have ownership of the mitigating actions.

To improve the ability of personnel to learn from and to respond to incidents, it is important that relevant scenarios are discussed and explored. ICT and SCADA professionals have different knowledge, experience and perspectives. By collaborating on learning and scenario analysis, they can obtain better assessments of the risk and identify appropriate risk reduction measures from a combined ICT and SCADA perspective.

Several other actions should be performed after a risk assessment is completed. These include conducting scenario training and establishing emergency response plans; performing systematic qualification and certification processes on key systems; and implementing barriers between process control systems and SISs using firewalls and network segmentation. Also, systems should be systematically hardened based on the results of the risk assessment (e.g., by installing operating system and application upgrades, security patches and anti-malware updates). Furthermore, firewall logs should be analyzed carefully to increase the understanding of incidents and the awareness of possible threats.

Our analysis indicates that professionals in different units have different expertise and levels of risk awareness; thus, there is a great need to increase risk

communication. In particular, all four resilience engineering phases – anticipation, attention, response and learning – must be improved. Participation, communication, action and ownership can improve operational safety and security. These issues suggest the need for a participatory process based on action research. Action research has been used to improve safety and security in complex organizations. Smith, *et al.* [18] describe how an action research program conducted across the entire New South Wales (Australia) Government contributed to better compliance, increased understanding and knowledge, improved policies, and effective business continuity plans. Similar results have been obtained in the Australian health care industry [3, 9].

4. Action Research

Action research is an established method for implementing changes based on reflection and participatory problem solving in team settings. Action research varies in form, but it usually involves technological, organizational and human issues in a change process. The underlying philosophy is that complex changes can be best understood and influenced by action [4].

Our hypothesis is that action research improves safety, security and resilience. The argument is that the process of action research together with the involved actors, sometimes called the "community of practice," identify relevant issues in design and operations, and also identify mitigating actions. The involvement of a community that includes management, ICT and SCADA professionals and workforce members increases the likelihood that the mitigating actions will be implemented successfully. Action research is especially useful in complex settings such as when multiple entities collaborate on safety-critical oil and gas operations.

Westrum [22] suggests that an organization whose workforce is aligned, aware and empowered is better at rooting out underlying problems. Action research can assist this endeavor by enabling "hidden" problems to be identified and highlighted. At the same time, action research can involve different stakeholders (or communities of practice) in a meaningful and positive dialog, fostering understanding and lasting collaboration. All this can ensure that issues related to safety, security and resilience are handled in a sensible matter. Although the work processes are fragmented, the "entire picture" can be analyzed due to the involvement of all the relevant participants.

Our survey of the action research literature reveals that it contributes to safety improvements. Our survey findings are based on a limited data set and, therefore, may be somewhat biased. The key issue is to identify causal relationships between the change process used in action research and the development of safety, security and resilience. We are especially interested in identifying action research activities that influence safety, security and resilience, the involved stakeholders and the application domains.

Van Eynde and Bledsoe [21] describe action research as the "touchstone of most good organizational development practices." The iterative method of action research has been formalized by Davidson, *et al.* [4] as an iterative

process model with five canonical action research principles: (i) researcher-client agreement; (ii) cyclical process model; (iii) theory; (iv) change through action; and (v) learning through reflection.

The involvement of stakeholders and the commitment from the "client" are important in relation to ownership, process, results, learning and reflection. Action research is an approach that is well-suited to complex problems. The relevant actors should be involved in the process because development and improvement may involve many stakeholders outside the organization (e.g., suppliers and service providers).

Alteren, *et al.* [1] have documented the improvements in safety and productivity from an action research project conducted at an offshore oil rig. The number of injuries at the rig decreased and the productivity (drill meters per day) increased. Moreover, the number of incidents involving injuries dropped to one-third of the previous number.

Alteren and colleagues highlighted some key issues: building on communities of practice by involving people who formed working communities at the platform, regardless of the company for which they worked; and implementing a "bottom-up" process involving first-line workers to ensure ownership by all the relevant employees regardless of line position. Other key issues include the need to focus on issues and challenges that the involved personnel deem to be most important, and using search conferences [5] as a tool to create understanding and participation among the workforce.

Antonsen, *et al.* [2] have documented similar improvements in safety (and efficiency) related to the use of service vessels in the oil and gas industry. The initiative realized dramatic reductions in injuries and collisions. Injuries on service vessels (per million working hours) were reduced from 13.8 in 2001 to 2.6 in 2006. Service vessel collisions were reduced from twelve in 2000 to an average of one per year from 2001 through 2005.

The key issues highlighted by Antonsen and co-workers include building on communities of practice whose safety is at stake (e.g., crews on service vessels and offshore installations); developing a unified approach to safety in the logistic chain; focusing on an interpretive bottom-up process in addition to "top-down" support of activities and mitigating actions; increasing worker understanding and ownership of challenges and solutions; basing the work on practical experience from the workforce; and implementing safety improvements without having to wait for an accident, which contributes to mitigating actions being perceived as more legitimate by workers. Other issues include using workgroup meetings (search conferences) as a tool for fostering workforce understanding and participation; generating enthusiasm; shifting from a "blame-oriented" to a "learning-oriented" culture with regard to incidents; and focusing on dialog and reflection (i.e., "two-way" communication).

Richter [17] notes that action research on accident prevention caused accident rates at two Danish enterprises to drop to about 25% of the average of the preceding five years. He observed that safety can be improved by building on communities of practice; focusing on an interpretive bottom-up process in

addition to top-down support of activities and mitigating actions; increasing worker understanding and ownership of challenges and solutions; and using search conferences as a tool to create understanding and participation by the workforce.

Richter's results could be a manifestation of the so-called "Hawthorne effect" [12], where increased attention to the principal issues is the real reason for safety and productivity improvements. However, the results appear to have a prolonged effect, lasting more than six months. The thesis that "structured" attention has a positive influence on safety and productivity clearly deserves further investigation.

5. Conclusions

Our survey of technical personnel at oil and gas installations has identified several challenges related to the safety, security and resilience of ICT and SCADA systems used in oil and gas production. The organizations and systems are complex and interdependent, and incidents can be potentially catastrophic. It is, therefore, critical to enhance the resilience of systems, organizations and human actors.

An action research program can help address these challenges. In particular, action research should focus on building communities of practice involving ICT and SCADA personnel in addition to members of the workforce whose safety is at stake; using search conferences as a tool to create understanding and participation among the various actors; using bottom-up and top-down processes; increasing worker understanding and ownership of challenges and solutions; exploring actual incidents and establishing best practices proactively rather than reactively; sharing experiences in an open manner to create awareness and understanding; and implementing a learning-oriented approach to accidents and incidents that incorporates dialog and reflection.

Risk assessment should be performed in a group setting involving professionals from the operating entity as well as from service providers. Actual and potential undesirable incidents should be discussed and explored in an open manner in order to create understanding and awareness of what has happened and what can happen. These incidents should be used to establish scenario training and emergency response plans. Systematic certification of critical equipment should be performed. Systems should be resilient because of their complexity, tight couplings and the possibility of common failures and other vulnerabilities. Therefore, a resilience engineering perspective should be incorporated when performing risk assessments of these systems.

The implementation of mitigating actions should be measured and evaluated. The overall level of resilience should be examined. Finally, key actors should be surveyed periodically to understand the relationship between risk anticipation, risk attention and responses during successful interventions as well as during accidents and undesirable incidents.

References

[1] B. Alteren, J. Sveen, G. Guttormsen, B. Madsen, R. Klev and O. Helgesen, Smarter together in offshore drilling – A successful action research project? *Proceedings of the Seventh International Conference on Probabilistic Safety Assessment and Management*, pp. 1302–1308, 2004.

[2] S. Antonsen, L. Ramstad and T. Kongsvik, Unlocking the organization: Action research as a means of improving organizational safety, *Safety Science Monitor*, vol. 11(1), 2007.

[3] H. Armstrong, Managing information security in healthcare – An action research experience, in *Information Security for Global Information Infrastructures*, S. Qing and J. Eloff (Eds.), Kluwer, Boston, Massachusetts, pp. 19–28, 2000.

[4] R. Davison, M. Martinsons and N. Kock, Principles of canonical action research, *Information Systems Journal*, vol. 14(1), pp. 65–86, 2004.

[5] D. Greenwood and M. Levin, *Introduction to Action Research: Social Research for Social Change*, Sage Publications, Thousand Oaks, California, 2007.

[6] E. Hollnagel, D. Woods and N. Leveson, *Resilience Engineering*, Ashgate, Aldershot, United Kingdom, 2006.

[7] International Society for Automation, ISA Security Compliance Institute, Research Triangle Park, North Carolina (www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISCI/ISCI.htm).

[8] International Society for Automation, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, ANSI/ISA-99.02.01-2009, Research Triangle Park, North Carolina, 2009.

[9] H. James, Managing information systems security: A soft approach, *Proceedings of the Information Systems Conference of New Zealand*, pp. 10–20, 1996.

[10] S. Johnsen, R. Ask and R. Roisli, Reducing risk in oil and gas production operations, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 83–95, 2007.

[11] S. Luders, CERN tests reveal security flaws with industrial networked devices, *The Industrial Ethernet Book*, GGH Marketing Communications, Titchfield, United Kingdom, pp. 12–23, November 2006.

[12] E. Mayo, *The Human Problems of an Industrial Civilization*, Macmillan, New York, 1933.

[13] Nuclear Regulatory Commission, The effects of Ethernet-based, non-safety-related controls on the safe and continued operation of nuclear power stations, NRC Information Notice 2007-15, Washington, DC (www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf), 2007.

[14] C. Perrow, *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, Princeton, New Jersey, 1999.

[15] J. Reason, Too little and too late: A commentary on accident and incident reporting systems, in *Near Miss Reporting as a Safety Tool*, T. van der Schaaf, D. Lucas and A. Hale (Eds.), Butterworth-Heinemann, Oxford, United Kingdom, pp. 9–26, 1991.

[16] J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate, Aldershot, United Kingdom, 1997.

[17] A. Richter, New ways of managing prevention: A cultural and participative approach, *Safety Science Monitor*, vol. 7(1), 2003.

[18] S. Smith, R. Jamieson and D. Winchester, An action research program to improve information systems security compliance across government agencies, *Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences*, p. 99, 2007.

[19] K. Stouffer, J. Falco and K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST Special Publication 800-82, Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[20] N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, Random House, New York, 2007.

[21] D. van Eynde and J. Bledsoe, The changing practice of organizational development, *Leadership and Organizational Development Journal*, vol. 11(2), pp. 25–30, 1990.

[22] R. Westrum, Removing latent pathogens, presented at the *Sixth International Australian Aviation Psychology Conference*, 2003.