Contradicting paradigms of control systems security: how fundamental differences cause conflicts

Floris. A. Schoenmakers

Faculty of Technology, Policy and Management, Delft University of Technology & Deloitte NL – Security & Privacy

ARTICLE INFO

Keywords:
Cyber security, Control systems Security, conflicting values, IT/OT integration, shared values.

Date: 8-4-2013

ABSTRACT

During recent years control systems are being integrated with the internet. The integration presents, besides less protection by isolation, more vulnerabilities because of connection to other networks. When IT solutions are imposed upon a group, it causes conflicts due to differences in perspectives between the two groups. To be able to secure the current legacy equipment and to cope with the intensified integration of networks and systems, the values and perceptions on security need to be aligned. Eventually, a shared perspective on security is expected to be vital for the IT/OT, while not underestimating the usefulness of conflicting values. In this article, first the IT/OT integration is explained, secondly literature on IT values and conflict is elaborated and thirdly the future scenarios of control system security are discussed.

1. Introduction

Supervisory Control And Data Acquisition (SCADA) systems became popular around the 1950's due to their ability to facilitate automation (Daneels & Salter, 1999). SCADA systems are the top layer of the network infrastructure. The layer beneath SCADA systems comprise the control systems, such as Programmable Logical Controllers (PLC) and Remote Terminal Units (RTU) (Centre for Development of Advanced Computing, 2012).The bottom layer holds the instrumentation domain. From the 1950's to the 1990's the SCADA systems were isolated and operated on proprietary protocols and operating systems. During the last two decade the industrial automation industry underwent significant changes, especially since 2000 when the internet became a commodity (Mo, 2012). At the same time that the internet became popular, computers also increased rapidly in their

capabilities and user base. The control systems needed to become more 'intelligent', mainly for two reasons:

1. Organizations required more information for daily tasks. They noticed that computer systems enabled them to gather more data about the business, which could provide them with a more solid base for decision making (Kuipers & Fabro, 2006);
2. Innovations in society and governmental regulations required the electricity sector to make adaptations to their infrastructure. Examples of these innovations are: activate demand response at client side; better incorporation of decentralized generation and storage in the electric grid; maintenance or even improvement of the existing high levels of system reliability, quality and security of supply; significantly reduction of the environmental impact of the whole electricity supply system (Collier, 2010).

What currently happens in the control system industry is illustrated by Rod Beckstrom (2012) and his theory on interconnectivity, also referred to as "the connectivity of things" or "the internet of things". He describes three laws regarding the interconnectivity. (World Economic Forum, 2012):

- Law 1: everything that is connected to the internet can be hacked;
- Law 2: everything is being connected to the internet, and
- Law 3: everything else follows from the first two laws.

Beckstrom (2012) tries to indicate that everything which is connected to a network is vulnerable for attacks of hackers. This interconnectivity leads to less isolated, and thus more vulnerable control systems for which three causes can be identified. First, connection of control systems to corporate networks becomes more common and bring them out of their prior isolation. The boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies (Center for Strategic and International Studies, 2011). Second, commodity IT solutions are used. Off-the-shelve IT solutions are implemented to automate control systems such as Windows operating systems and TCP/IP networking (Industrial Defender, 2012). Third, open design protocols are used (Netbeheer Nederland, 2012). Old control systems had unique protocols, the protocols currently used are more accessible and open. In this manner, attackers can gain (or mostly already have) knowledge about the protocols to enable targeted attacks. The three trends result in a more vulnerable environment for control systems. Therefore, the IT integration in control system requires a sharp focus on a crucial aspect of control systems: cyber security.

With regard to cyber security, there is a cause for concern regarding the differences in perspective between groups of persons that are active on the industrial control systems. IT systems are inherently exposed to malicious entities. In order to have an effective security policy, to some extent there needs

to be a shared perspective on security. Two important groups are identified. The operational technology (OT) specialists, who are active on the operational domain, and the Information Technology (IT) specialists, who are active on computer and network security, are bound to work closely together. Based on literature, we expect that (ENISA, 2012):

> *The conflicts in cultural values and the consequent difference in (cultural) perspective cause conflicts that lead to security issues in control systems.*

A shared perspective on security is likely to increase cyber resilience; attention and commitment to security should increase security (World Economic Forum, 2012). Yet, it has to be recognized that differences in perspective could have a positive contribution to security. The central question in this article is: *to what extent are differences in perspective functional and when do they become dysfunctional?*

The formulated proposition and research question are analyzed with an analytical lens that is constructed on two papers on cultural conflicts. First, with Von Meier's paper on the causes of cultural conflicts and second. Second, with Leidner & Kayworth's paper focusing on the implications of cultural conflicts. In the last section a figure is drawn of the relations from issues to implications. Hereby creating the ability to anticipate on the positive and negative implications of conflicting values and/or shared values.

2. Conflicting values in the control system domain

This paper focuses on two conflicting perspectives in control systems domain: the IT specialist and the Operational Technology (OT) specialist. The IT specialist has two commonly used synonyms: (cyber) security specialist and control system security specialist. Also the OT specialist has two synonyms: (operational) engineer and control system specialist. In this paper the terms IT specialist and OT specialist are used to distinguish between the two groups. In the literature significant differences are found regarding technical requirements and aspects when comparing the 'business IT' – generally the domain of IT specialists - and the 'industrial IT' – generally the domain of OT specialists -. The corporate network is considered as the business IT domain, where in many cases administrative and supportive services are carried out, services like sales, billing, taxing and orders (Ernst & Young, 2011). The industrial IT is considered to be part of the operational network. This network primarily comprises SCADA systems and is usually the operational center of the control system network that actually controls production.

In theory, the people working on these different systems have different (group) values, depending on the subgroup they belong to (Byres, Carter, Elramly, & Hoffman, 2003). OT specialists are involved

in the design and operation of systems that have a high physical interaction: the production systems that are controlled interact directly with the physical world. Requirements as safety, reliability and availability (SRA) are valued as the most important design criteria (Stapelberg, 2008). A particular system must be available, with for example an uptime of 99,9%. Also, due to the high physical interaction, safety is important and must be guaranteed. This mostly refers to the (physical) safety of the people who are involved and in contact with this system. The IT specialists are involved in securing system and networks. In general, the IT specialist has a different set of requirements than the OT specialist. In literature confidentiality, integrity and availability (CIA) are the criteria that are valued the most for IT specialists (Wu, 2009). These criteria are reoccurring and seem to be dominant in securing the systems and networks.

To gain more insight in what the possible consequences of contradicting values between groups can are, relevant literature on conflicting cultures will be discussed. The literature of Von Meier explains how certain values are inherent to specific subgroups. Consequently problem perception, problem definition and possible solutions are difficult to decouple from the specific subgroup, because in respect to their own values their arguments and perspectives make sense.

Contradicting values between groups could cause and/or contribute a great deal to difficulties in securing control systems. The issues with the difference in perspectives occur are at the bottom of the organization, where people influence the organization with practical actions and decisions. Management can decide to invest heavily in security, but in the end the people who work with the security implications have to understand, agree and accept these decisions. Not only understanding is necessary, but also shared values on security might be preferred. A shared perspective could contribute in the decreasing conflicts caused by different perceptions on security.

3. Conflicting cultures

Von Meier (1999) focusses on cultures as the decisive factor on conflicts in technological innovation. Suppose a technological innovation is available and ready for an organization to implement in their systems. It is argued that there is a difference of interest between two groups. Von Meier illustrates this with an example: the engineer finds the efficiency and reliability of the system of significant importance. While the operator predominately wants to ensure safety. These ‘conflicts of interest’ are believed to be the root cause of failures to adopt new innovations. The conflict of interest impedes to some extent the cooperation between the groups. The most important conclusion of Von Meier was the following: “conflicting values and judgments can arise not only from conflicting interests, but from differences of interpretation” (von Meier, 1999, p. 101).

Von Meier (1999) argues that there are two misunderstandings when it comes to conflicting cultures. First, "evaluations of technology are determined only by facts" (von Meier, 1999, p. 109). When this statement is assumed to be true, then there would be a relatively simple solution: educate both sub groups so the 'optimal' decision can be made. Von Meier argues this is impossible due to the fact that important perceptual differences will always remain: "the root of the difference lies not in fact but in representation" (von Meier, 1999, p. 109). This is inherent to the differences in group culture, i.e. an engineer is adapted to analytical reasoning, while an operator uses mainly experience for his reasoning. Consequently, the two subgroups will have different opinions, even if they would agree on the facts.

The second misunderstanding regards bias: "Cultural groups have inherently subjective or irrational biases" (von Meier, 1999, p. 109). Von Meier illustrates this misunderstanding by the help of an example: an opinion can be that operators are generally old-fashioned, afraid of the unknown, and prejudiced against computers. This would obstruct actual innovation to be implemented. She continues in her argument that cultural differences can also be understood in a constructive way that unifies the picture, while granting each perspective its own validity. Therefore implicating that they are both right in their own manner. The difference in perspective could be a complementary aspect for the organization, as it offers a critical perspective on problems and solutions. The acknowledgement of the possible usefulness of conflicting perspectives is an important aspect to remember.

With the paper of Von Meier more insight to causes of the underlying aspects of conflicting cultural perspectives is gained. Leidner and Kayworth (2006) wrote a paper, relevant to the IT integration in industrial control systems. Their paper focus more on the issues resulting from cultural conflicts described by Von Meier. Leidner and Kayworth argue that culture is often partially blamed when organizations experience failure, moreover: information technology is often implicated in failure to successfully adopt innovations. While IT is often seen as a possible resort to reduce errors or cut costs, yet the introduction of IT is often met with cultural resistance (Leidner & Kayworth, 2006). Leidner and Kayworth introduce six propositions, based on their research. Several of these propositions are relevant to reflect on the IT/OT integration. Every proposition states that a difference in values between groups results in negative consequences for security:

> The first proposition regards cultural distance and conflict. The greater the cultural distance between the group responsible for championing the IT and the group adopting the IT, the greater the system conflict experienced by the group adopting the IT. (Leidner & Kayworth, 2006, p. 379)
>
> The second proposition explains how an apparent cultural conflict indicates the likeliness of adoption. The greater the system conflict experienced by a group, the less likely the group is to be a forerunner in the adoption of the system. (Leidner & Kayworth, 2006, p. 376)

> The third proposition focuses on the adaptation and changes made to systems to fit to the existing values. The third proposition concerns the altering of an IT solution by responsible entities (managers or employees) in such a way that it suits the requirements and values of their company or group. The greater the systemic conflict experienced by a group, the greater the modification of use to support the group's values. (Leidner & Kayworth, 2006, p. 376)
>
> The last proposition is a logical but important finding of Leidner and Kayworth: Managers can reduce all forms of conflict by promoting shared values. (Leidner & Kayworth, 2006, p. 380)

From the propositions it can concluded that conflicting values can impede control system security. Possible consequences of conflicts range from increasing vulnerabilities for control systems to obstruction to move forward with the available technology.

4. Future scenarios

From the latter three paragraphs, we can conclude three things. First, there is an ongoing (r)evolution in the control system domain, where the control systems are increasingly interconnected with other networks. Second, the interconnectivity requires a conjunction of IT and OT specialists. However, the two groups have values that do not necessarily fully correspond with each other. Third, different or even conflicting and contradicting values – or cultural distances – could frustrate cooperation between the groups, which for control system security would result in and increased chance of vulnerabilities and impediments of progress in efforts to increase security. While security of control systems is also dependent on a variety of other variables - as security by design, investments in security, etc. -, minimizing contradicting values between groups is a relevant variable.

It is expected that companies are rational and are driven to make a tradeoff between risks and investment. Also rationality is expected when it comes to decreasing vulnerabilities that can endanger the continuity of the organization. One way for organizations to decrease conflicts between groups related to security is by education and communication. Communication is reckoned to be of vital importance when it concerns overcoming the issues related to contradicting values. The IT/OT integration in control systems and the subsequent security issues can develop into three different future scenarios:

1. **Separate values and minimal communication**. Decision makers in the IT and OT domains do not see the need or ignore the need for intensive communications between experts. Logically, minimal communications ensure that shared values are not likely to arise;

2. **Separate values and intensive communications**. There is a general consensus that communications and increased understanding of each other's values is of importance. Intensive communications comprise (awareness)training and education;
3. **Shared values**. When both groups understand, agree and adopt the same set of values, the relevant groups in an organization has shared values.

When recognizing the possible future scenarios, the ability to steer towards a desired end state becomes an option. For this, one vital question has to be answered: when does the tension between contradicting values become dysfunctional? Based on the previous sections, it can be argued that a shared perspective is – to a certain extent - desirable. When values significantly differ, the security of control systems is expected to suffer. Somewhere on the spectrum from 'contradicting values' to 'shared values', there is an area that utilizes the tradeoff for a company between investment and risks. The previous writings can be combined into one graph that consecutively shows the relevant insights (figure 1). The implications of technical differences are outside the scope.

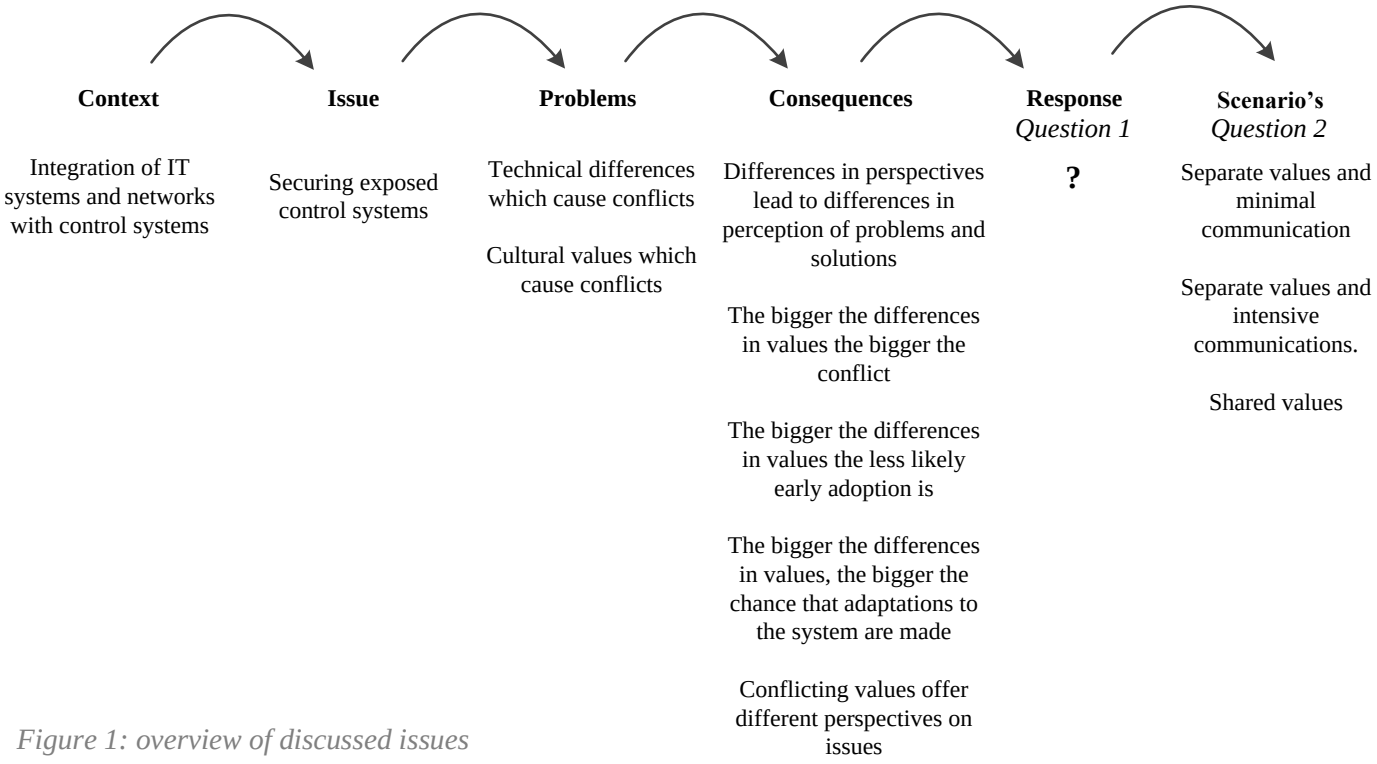

Figure 1: overview of discussed issues

The 'response' section of figure 1 needs some additional explanation. The question mark is added there because response is dependent on the preferred scenario. Organizations could choose to work towards a scenario but also could intentionally or unintentionally ignore planning towards one of

these scenarios. A relevant question related to response - *Question 1* - reads: What is the desired scenario for the organization and to what extent can a response to the problems influence to which scenario an organization moves? When it would be possible to work towards a desired scenario, *Question 2* is relevant: when does the tension between contradicting values become dysfunctional? Both questions are relevant for organizations that are aware of different perspectives on security in their organization. Based on the relevance, these questions deserve further research.

5. Conclusion

Differences in perspectives between IT and OT specialists can cause security issues for control systems. It is important for organizations to keep in mind that different values between groups can influence the perception of issues and solutions. In the literature there is a wide range of negative consequences related to conflicting values which would influence the control system security in a negative manner. Yet, as Von Meier indicated, differences in perspective can also offer a keen eye, and strengthen rational decisions related to security. To be able to move forward, the two questions from paragraph four are for organizations open to answer: which of the three scenario's is the desired scenario for the organization and how does an organization keep balance between functional and dysfunctional differences in value?

Concerning security in control systems, we argue that it is best to fall in – or close to - the third category 'shared values'. Security-wise, it seems best to have a shared understanding and agreement on a set of values. Yet, never underestimate the keen and critical eye which can ask the right questions.

References

Byres, E., Carter, J., Elramly, A., & Hoffman, D. (2003). *Worlds in Collision - Ethernet and the Factory Floor* . Burnaby: BCIT Internet Engineering Lab .

Center for Strategic and International Studies. (2011). *Twenty Critical Security Controls for Effective Cyber Defense.* SANS.

Centre for Development of Advanced Computing. (2012, 2 10). *SCADA Security Awareness.* Retrieved 12 10, 2012, from Forum of load despatchers: http://www.forumofld.in/Data/Meeting/6th%20fold%20meeting/Awareness%20-%2010Feb2012-Ver2.0.pdf

Collier, S. (2010). Ten Steps to a Smarter Grid. *Industry Applications Magazine, IEEE*, 62 - 68.

Daneels, A., & Salter, W. (1999). What is SCADA. *International Conference on Accelerator and Large Experimental Physics Control Systems*, (pp. 339 - 343). Trieste.

Ernst & Young. (2011). *Attacking the smart grid.* London: Ernst & Young.

Industrial Defender. (2012, 10 24). *Industrial Defender*. Retrieved 10 24, 2012, from ICS Challenges: http://www.industrialdefender.com/asm_solutions/security.php

Kuipers, D., & Fabro, M. (2006). *Control Systems Cyber Security: Defense in Depth Strategies.* Idaho: Idaho National Laboratory.

Leidner, E., & Kayworth, T. (2006). A review of culture in information systems. *MIS Quarterly Vol. 30 No. 2*, 357-399.

Mo. (2012). Cyber–Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEE. Vol. 100, No. 1, January*, 195 - 209.

Netbeheer Nederland. (2012). *The road to a sustainable and efficient energy supply: Smart Grid Roadmap.* Netbeheer Nederland.

Stapelberg, R. (2008). *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design.* Springer.

von Meier, A. (1999). Occupational Cultures as a Challenge to Technological Innovation. *IEEE Transaction on engineering management*, 101 - 112.

World Economic Forum. (2012). *Risk and responsibility in a hyperconnected word: pathways to golbab cyber resilience.* Geneva: World Economic Forum.

Wu, A. (2009). *Security Architecture for Sensitive Information Systems.* Faculty of Information Technology Monash University.