C. Alcaraz, et al., "Adaptive Dispatching of Incidences Based on Reputation for SCADA Systems", *6th International Conference on Trust, Privacy and Security in Digital Business (TrustBus09)*, LNCS, pp. 86-94, 2009.
http://doi.org/10.1007/978-3-642-03748-1_9
NICS Lab. Publications: https://www.nics.uma.es/publications

Adaptive Dispatching of Incidences based on Reputation for SCADA Systems

Cristina Alcaraz, Isaac Agudo, Carmen Fernandez-Gago,
Rodrigo Roman, Gerardo Fernandez, and Javier Lopez

Computer Science Department - University of Malaga,
29071 - Malaga, Spain
{alcaraz,isaac,mcgago,roman,gerardo,jlm}@lcc.uma.es

Abstract. SCADA systems represent a challenging scenario where the management of critical alarms is crucial. Their response to these alarms should be efficient and fast in order to mitigate or contain undesired effects. This work presents a mechanism, the Adaptive Assignment Manager (AAM) that will aid to react to incidences in a more efficient way by dynamically assigning alarms to the most suitable human operator. The mechanism uses various inputs for identifying the operators such as their availability, workload and reputation. In fact, we also define a reputation component that stores the reputation of the human operators and uses feedback from past experiences.

Keywords - *SCADA systems, Critical Control Systems, Reputation*

1 Introduction

Part of our society comprises a set of critical infrastructures most of them belonging to the industrial sector. These critical infrastructures are controlled by specialized and complex control systems known as Supervisory Control and Data Acquisition Systems (SCADA). Through them, the operators could know the state of the infrastructure in real-time, by simply observing those data come from RTUs (*Remote Terminal Units*) and sensors deployed in all the development area. Even though the main requirement of a SCADA system is to ensure the performance and availability of the controlled system, security issues should be taken into consideration since a failure in the controlling process or a threat could mean a harmful cascade effect in the whole system [4]. Hence, SCADA systems are considered critical infrastructures by themselves as well.

During the controlling process, a set of incidences generated and categorized by the type of criticality of their associated alarms can appear. These incidences have to be managed by authorized operators. However,

nowadays, most of them are not always suitable for attending them. The reasons may be several: lack of knowledge/skill, disinterest to take it up, or malicious goals. This paper presents a mechanism based on reputation that allows a SCADA system to identify the best staff to attend an incidence, maximizing reaction time and minimizing future risks.

The paper is organized as follows. In Section 2 we explain the procedures for action control in SCADA systems and highlight our contribution. Section 3 justifies the importance of reputation in SCADA systems and introduces a reputation component that stores human operators' information. In section 4 we detail the mechanism that assigns a certain incidence to an operator and discuss the practicability of using such a mechanism. Section 5 concludes the paper and outlines the future work.

2 Procedures for Action Control in SCADA Systems

SCADA systems are composed of two types of foundation networks: the *control network* and the *corporative network* (see Figure 1). The control network is in charge of receiving measurements or alarms from substations and managing control tasks (e.g open/close a pump). The operations performed by the corporative network are more related to the general supervision of the system. Both networks can make use of different communication infrastructures and specific SCADA communication protocols [8, 9, 16, 17]. Furthermore, Some SCADA systems could offer web and mobile services as well as control operations between critical control systems.

From a security point of view, both networks and all their components can be threatened either by insiders (negligence or malicious acts of the staff) or outsiders (vulnerabilities of the protocols and software components [3]). In fact, Byres et.al. [5] used public databases[14, 15] to infer that the number of external threats are increasing since the SCADA systems are connected to other external networks. Due to all these security problems, experts from different fields [6, 7] are joining their efforts in order to improve the overall security of these critical infrastructures. Special attention should be also paid to the management of human operators since their responsibilities and their influence in the system are very high. Basically, this is currently done by using formal procedures such as security policies, access control policies and auditing mechanisms.

Security policies have to define the steps and responsibilities that can be performed by the different elements of the system. For that reason, their foundations should be based on generic security control standards [10–12] being extended to specific requirements of SCADA systems [12,

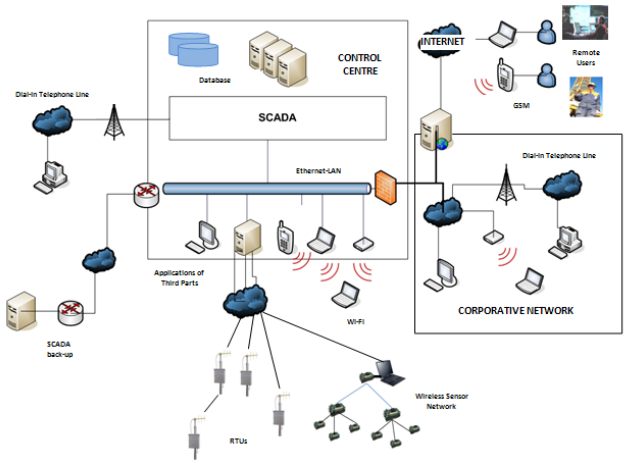

Fig. 1. A SCADA network architecture

13]. In contrast, access control policies must be able to manage and control every user identification and authorization process in all the components of the system.

Finally, auditing mechanisms provide a general overview of the state of the system by inspecting the actual functionality and the responsibilities of all the components and members of an organization. Such inspections must be regulated by formal procedures and standards, e.g. NIST SP 800-53 revision 2 [12].

2.1 Our Contribution

While the policies and mechanisms presented in Section 2 are necessary for securing a SCADA system, it would be also interesting to provide security mechanisms for controlling activities of the human operators. These mechanisms could work in parallel with all the policies and mechanisms mentioned above and can provide a more accurate control. Note that any mechanism of this sort should not interfere with the normal functionality of a SCADA system due to the criticality of its operations.

From a research point of view, this field is still unexplored in SCADA systems. A related work was proposed by Bigham et. al. in 2004. They presented an architecture based on an agent-based system to monitor the system and derive automated trust and privileges re-allocation.

The purpose of this paper is to investigate one of these mechanisms: an automated adaptive response mechanism able to estimate the most

suitable human operator to effectively respond to incidents and alarms in a SCADA system. This will reduce the possibility that an alert could remain untreated. As a primary input, this mechanism will make use of a *Reputation* module where all operators are assigned a certain value according to their behaviour and to their reaction when dealing with incidences. Again, since the adaptive response mechanism is decoupled from the reputation module (i.e. they work in parallel), the impact on the availability of the SCADA system is minimal.

Therefore, the expected results from the mechanism presented in this paper are as follows:

1. Task control and monitoring without reducing the overall performance of the system.
2. Reliability. The mechanism identifies the human operator that is more suitable for performing a certain task.
3. Security. The reputation module manages the behaviour of the elements of the system and it can be used for detecting some malicious activities coming from internal attackers.
4. Availability of the resources of the system. The mechanism works in parallel with the other elements of the system.

3 Reputation Module for a SCADA System

The concept of reputation is defined by the Concise Oxford Dictionary as 'what is generally said or believed about a person's or thing's character or standing'. Reputation can be measured in several ways [1]. According to Resnick [2], a working reputation system must have at least the following three properties:

1. Entities must be long lived, so that with every interaction there is always an expectation of future interactions.
2. Feedback about current interactions is captured and distributed. Such information must be visible in the future.
3. Past feedback guides buyer decisions. People must pay attention to reputations.

Entities in SCADA systems are long lived and there are always expectations for future interactions as in these type of systems there are always incidences or alarms to attend. Also, the information about interactions is something we intend to capture and store. Besides, we believe

that a reputation system is more effective when there are some incentives for maintaining a good reputation level and when it is difficult to get rid of bad ratings. We classify the aims of a user for improving his reputation into the following categories: *Profit*, *Reward*, *Ego* and *Fear*. The reputation system that we propose for SCADA systems fall into the Reward or Fear categories. Operators with a higher reputation could be rewarded with some benefits such as a pay raise or a promotion. On the other hand, if they continuously fail in performing their tasks or they are not performed as well as the system requires they could be given a worse position in the organization or even be fired.

In order to provide a mechanism based on reputation for a critical and complex control system we will design a reputation module for such a systems. This reputation system will monitor all the feedbacks and will compute reputation values for each operator. This information will be gathered later by a specialized component of incidences. Some minimal requirements are though needed. First of all, users (operators in this case) are assigned initial values of reputation. This initial reputation could be the same for all of them assigned accordingly to their experience or knowledge. The values of reputation are increased or decreased depending on how the human operator manages system incidences. The increase or decrease will vary based on how critical the alarm is and what the feedback from an operator with a higher reputation level who takes the role of the 'supervisor' is.

When we require a feedback for a given incidence the system must allocate two available operators. One of them will manage the incidence and the other one will send a feedback to the system informing how satisfactory was the measure taken by the first operator. The feedback system allows supervisors to include some textual description and forces them to rate the incidence management with one of the following values: Bad (1), Neutral (2) and Good (3).

As mentioned above the level of criticality is an input parameter for the management of reputation. This level will be measured ranging from 1 to 5, for example. In order to combine the feedback with this other factor, we can multiply them and obtain a modified feedback: "$Criticality \times Feedback$". We also consider the reputation of the supervisor as a parameter for modifying the feedback. This way, the higher the reputation of the supervisor is, the more relevant the feedback will be. The new feedback value can be computed as "$Criticality \times SupervisorReputation \times Feedback$". Note that other combinations are possible but we have chosen this as an initial approach.

4 Adaptive Assignment of Human Operators for a SCADA System

The reputation module is useful for storing the overall behaviour of the human operators, but it does not hold any decision-making capabilities. Therefore, for developing our automated adaptive response mechanism, we need an "Incidence Manager" component: the *Adaptive Assignment Manager* (AAM) (see Figure 2). This component takes an alarm as an input, and it determines which operator and supervisor are the most appropriate to take it up. The AAM is also in charge of updating the reputation of the operators in the reputation module by using the feedback of the supervisors.

The AAM component does not pretend to completely replace the response and alert management capabilities of human operators and supervisors. Instead, it facilitates their work by selecting, in the first instance, the most skilled staff that could provide an early and effective response to the incidence, offering all the relevant information to supervisors in a way that they can do their job in an assisted manner. In order to determine which operator or supervisor are the most suitable for taking care of an incidence, the AAM considers the following set of parameters:

- ***C*riticality of the alarm**. The alarms are categorized by the type of criticality of an event occurred in the system. Such alarms are received by a SCADA server, which generates the associated incidences.
- ***R*eputation** of the operator and supervisor, obtained from the reputation module.
- ***A*vailability** of the operator and supervisor according to their contracts. They should be authorized in the system and being available in their work place.
- ***L*oad of work** of the operator and supervisor. This parameter is related to the overload of critical incidences that an operator might be dealing with at a certain time. If an operator is attending a number of non very critical incidences he could be still available for taking up a more critical one. However, if the operator is dealing with other critical incidences (even if it is only one) the system should identify another operator who could deal with it. The process is analogous for the supervisor.

Another task of the AAM is to serve as an interface to the values stored inside the reputation module. This way, the managers can determine the knowledge of the operators and even the level or mistakes made by them

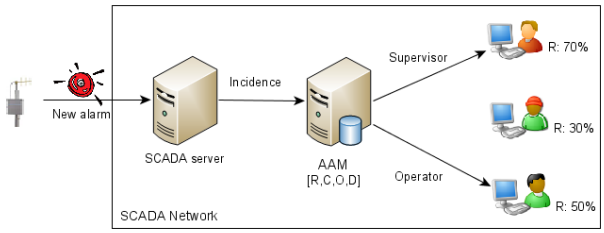

Fig. 2. Functionality of an Adaptative Assignement Manager (AAM)

during the life time of a system. For example, an operator can i) reach the minimal reputation value, or ii) reach the maximal reputation value. In the first case the system should notify it to the responsible managers of the organization owning the SCADA system, thus that they are aware of the situation. However, in the second case the organization should reward these employees in order to maintain this high threshold of reputation.

4.1 Discussions

The implications of using the Adaptive Assignment Manager (AAM) presented previously in a real environment need to be carefully analyzed. First, it is necessary to consider in which order we should process the four parameters (C, R, A, L). Next, we should check the different situations that can be found in the management of an incidence by an operator assigned by the AAM system.

At first, the order of processing the four parameters employed by the AAM system could be crucial for quickly reducing the set of candidates to be chosen as operators and supervisors. This is a key point when critical alarms need to be dispatched as soon as possible. Availability (A) seems to be the first parameter to be processed from the set of the four parameters presented in Section 4. It can reduce the group of operators to be evaluated in a speedy way as it puts aside those employees that are not actually at work. The rest of variables can be sorted in different ways depending on each scenario but a logical sequence that can be used is to take into account criticality (C) of alarms. This can be used in a third step to select those personnel that are less busy (L), and from them the one with a higher reputation (R).

As for incidence management, after selecting a human operator to manage an incidence received by the AAM system, a supervisor is chosen for monitoring the way it is going to be resolved by him/her. The

operator must confirm the acceptance of the assignment before a defined time (*Tcon*). At that moment the resolution of the incidence starts. The supervisor is informed of the assignment done by the AAM system and a time counter (*Tres*) for determining how long it has been spent for resolving the incidence is started. This counter will warn the supervisor when an incidence remains unresolved for longer than it should. Thus, this counter could also help to calculate the efficiency of the operator in the resolution of incidences. Finally, a third counter must be used (*Tsup*) to check that the maximum time spent by a supervisor for managing an incidence not resolved by an operator is reached. These three counters are shown in Figure 3.

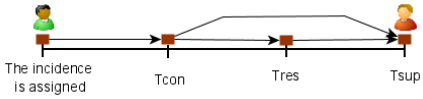

Fig. 3. Counter to be used in this schema

At this point, three situations can happen (see Figure 4).

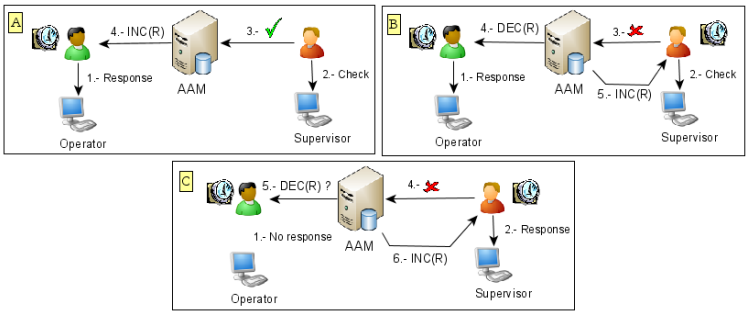

Fig. 4. Three main situations in the management of an incidence in a SCADA system

- The incidence is successfully resolved by the operator assigned before *Tres* is reached. Nonetheless, the supervisor checks his/her resulting action after this counter is reached. The operator's reputation must be increased. (Figure 4-A).
- The incidence is not successfully resolved by the operator and *Tres* is reached. The supervisor checks the operator's action to be in charge

of resolving it again. Finally, the operator and supervisor's reputation are changed (Figure 4-B).
- The operator could not confirm the acceptance of the assignment done by the AAM system. This situation is detected because *Tcon* is reached. The supervisor will be in charge of the incidence if this counter is overtaken increasing his final reputation. (Figure 4-C).

When a supervisor is in charge of managing the incidence, the AAM system must offer him all the information generated for the assignment. Thus, the supervisor can use this report in order to evaluate the reason why the incidence was not successfully resolved in such a way that he can deal with it in a more accurate way. Besides this, the supervisor must make a decision about how to proceed with the resolution of the incidence before *Tsup* is reached, otherwise his reputation must be modified by the AAM system conveniently.

Finally, an AAM system could not find any operator with enough reputation and the load of work needed to be selected for the assignment of an incidence. Also, supervisors could have a parameter showing their load of work that could drive to a similar situation. These states must be evaluated for each scenario as in some cases it could be solved by re-sorting actual incidences and the staff assigned to them. Some other times these incidences can be queued waiting for an operator and a supervisor to deal with them.

5 Conclusions and Future Work

This paper presents an approach based on reputation that intends to improve the incidence management in a SCADA system. Basically, reputation will allow the system to identify which human operator is more suitable to attend it and those supervisors to check the resulting action. Such identification is made by an incidence manager (AAM) which will identify not only the best candidates but also will manage their final reputation level. To this end, a reputation module and a set of input parameters has been defined as well as some important situations (discussed in Section 4.1).

Any data associated to the reputation and the human operator's operations must be registered for future analysis processes. Basically, these will allow managers or staff in charge of a critical and complex system to be able to determine the operators' knowledge level in real time and/or even the presence of suspicious actions. Moreover, these registers will improve the response processes, the control procedures and the development

of new and interesting tools such as auditing and maintenance of the system.

In order to show the validity of this approach this work is being currently formalized through a mathematical model. Besides, we are working on extending it and thus to take into account web and mobile services as well as remote control from other control systems.

6 Acknowledgments

This work has been funded by MEC I+D and MICT of Spain under the research projects: CRISIS (TIN2006-09242), ARES (CSP2007-00004) and PROTECT-IC (TSI-020302-2008-46).

References

1. A. Jøsang, R. Ismail, C. Boyd, *A Survey of Trust and Reputation Systems for Online Service Provision*, Decision Support Systems, 43(2):618–644, 2007.
2. P. Resnick, R. Zeckhauser, E. Friedman, K. Kuwabara, *Reputation Systems*, Communications of ACM, 43(12):45–48, 2000.
3. A. Cardenas, S. Amin, S. Sastry, *Research Challenges for the Security of Control Systems*, HotSec'08, 2008.
4. J. P. Peerenboom, R. E. Fisher, *Analyzing Cross-Sector Interdependencies*, IEEE Computer Society, HICSS '07, IEEE Computer Society, pp. 112–119, 2007.
5. E. Byres, J. Lowe, *The myths and facts behind cyber security risks for industrial control systems*, 'VDE Congress, VDE Association For Electrical, Electronic Information Technologies, British Columbia Institute of Technology and PA Consulting Group, 2004.
6. Department of Energy Office of Energy Assurance, *Steps to Improve Cyber Security of SCADA Networks*, white paper, 2002.
7. NISCC, National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, BCIT, 2005.
8. IEC 60870-5-104, *International Electrotechnical Commission*, 2006.
9. IEC 60870-6, ICCP/TASE2, *International Electrotechnical Commission*, 2008.
10. ISACA, *Control Objectives for Information and related Technology*, rev 4.1, 2007.
11. ISO/IEC 17799:2005, *Code of Practice for Information Security Management*, 2005.
12. NIST Special Publication 800-53 revision 2, *Recommended Security Controls for Federal Information Systems*, 2007.
13. NIST Special Publication 800-82, *DRAFT - Guide to Industrial Control Systems (ICS) Security*, 2007.
14. BCIT, *British Columbia Institute of Technology*, http://www.bcit.ca/, 2008.
15. CERT, *Carnegie Mellon Software Engineering Institute*, http://www.cert.org/stats/vulnerability_remediation.html, CERT/CC Statistics 1988-2008.
16. DNP3, *DNP Users Group*, http://www.dnp.org, 2008.
17. Modbus-IDA, *The Architecture for Distributed Automation*, http://www.modbus.org/, 2005.