Published in IET Information Security
Received on 19th April 2013
Revised on 25th February 2014
Accepted on 1st March 2014
doi: 10.1049/iet-ifs.2013.0159

ISSN 1751-8709

Approaching secure industrial control systems

Rafał Leszczyna

Faculty of Management and Economics, Gdansk University of Technology, Narutowicza 11/12, Gdańsk, Poland
E-mail: rafal.leszczyna@pg.gda.pl

Abstract: This study presents a systematic approach to secure industrial control systems based on establishing a business case followed by the development of a security programme. To support these two fundamental activities the authors propose a new method for security cost estimation and a security assessment scheme. In this study they explain the cost evaluation technique and illustrate with a case study concerning the assessment of the cost of information security assurance activities in a division of a Polish manufacturer of passenger and commercial tyres. They further present the steps of their security assessment scheme and demonstrate how they integrate with the overall approach for protecting industrial control systems.

1 Introduction

In recent years more attention has been paid to industrial control systems. This is due to many reasons, one of them being the fact that these systems have become interconnected with the Internet and a great number of them are utilised in critical infrastructures [1]. The subject has also come under particular scrutiny following the advent of targeted attacks against critical infrastructures such as Stuxnet [2]. Other examples of security incidents in process control system and lessons learned from them are described in [3].

In this context, work on protecting industrial control systems has been intensified. New initiatives have been launched, more stakeholders involved, new security solutions and strategies have been developed etc. Owing to the focused standardisation in the field, systematic, standardised approaches and methodologies for securing industrial control systems have been proposed [1].

There are many challenges facing the protection of industrial control systems (ICS), ranging from technical, such as weak communication protocols (mostly unencrypted) or the long lifetime of these systems, to organisational (e.g. the lack of collaboration and coordination between the involved departments) and governmental ones, for example the lack of a global security policy in critical infrastructure (CI) operators [1].

A very important problem which has been listed among the eight biggest challenges in ICS security is that members of senior management of the enterprises which use ICS are not sufficiently involved in the ICS security. According to experts, senior managers usually consider cyber security as a cost rather than an investment. Moreover, they believe that developing and implementing a complete security programme that incorporates ICS is very costly, and would rather choose temporary and provisional solutions just to avoid this perceived potential cost. Experts agree that defending security costs before senior management constitutes one of the main difficulties in improving ICS security [1].

However, only a few approaches exist which support the process of cost estimation of information security. They include I-CAMP (incident cost analysis and modelling) [4, 5], SQUARE (system quality requirements engineering) [6, 7], some economic metrics [6–10] and simple calculators [11–13] (see Section 4.1). Practically, all of them aim at estimating the cost of a security breach, which means that they focus on the benefit side of the cost–benefit equation. The cost side of the cost–benefit equation that is the question 'how much must I invest?' is addressed by cost calculators, but the precision of their estimations is far from sufficient and they usually use hidden algorithms. With such a limited set of tools and methods it is very difficult or sometimes even impossible to provide costing figures and to defend security costs before senior management in order to persuade them to invest in information security.

On the other hand, detailed information about the costs and resources required to develop, implement and maintain an information security management system is a prerequisite part of any business case included in an information security programme [14].

To address these challenges we developed a new method for the estimation of costs of activities within the cyber security lifecycle. The method is based on activity-based costing (ABC) systems, and uses National Institute of Standards and Technologies (NIST) SP 800-53 as the source of the activities.

In this paper we present this method (Section 4) and its integration with the ICS security programme development approach defined in NIST 800-82 [15] (Section 3). NIST 800-82 is one of the few publications which describe the process of establishing an information security management system (ISMS) or a cyber-security management system (CSMS) in the ICS perimeter (see Section 2). It has gained particular recognition and popularity among the

stakeholders involved in the ICS field (ICS security tools and services providers, ICS software/hardware manufactures and integrators, infrastructure operators, public bodies, standardisation bodies, universities and R&D) [1], most probably because it is so ICS specific and well written. The document provides an overview of ICS and typical system topologies and describes specific security controls for ICS.

After the presentation of our cost evaluation technique (Section 4) we illustrate it with a case study concerning the assessment of the cost of information security assurance activities in a division of a Polish manufacturer of passenger and commercial tyres (Section 4.7).

Our second contribution to the ICS security approach to which we refer in the paper (Section 5) is the proposal of a security assessment scheme for critical networked infrastructures, described in details in [16, 17]. The risk and vulnerability assessment is a part of the development of a cyber-security programme that has a paramount importance for its effectiveness. Our approach is particularly suitable for industrial control systems because it avoids interferences with the evaluated system. These interferences in the case of industrial control systems can be very harmful and can lead to very serious consequences.

2 Standards, good practices, guidelines and policies

Currently the set of guidelines, standards and regulations for ICS security comprises more than 50 publications, a quarter of which are standards. The majority of these publications are not ICS specific and treat the security of ICS from a general perspective. However, there are also many documents which are dedicated specifically to the energy sector (oil, gas and electricity), where the library of documents aiming at the electricity sector is particularly extensive. At the same time, other sectors, for example transportation, water supply or agriculture are not very well addressed. Many of the documents are already in their final versions. In other cases, such as IEC 62443 which adapt ANSI/ISA 99 or some NIST standards, the documents are still being developed [1].

The standards address various aspects of security of industrial controls systems: data and communication security, security requirements and controls, risk management, security programmes and other issues.

For instance, IEC 62351 and IEEE 1711 focus on data and communication security. IEC 62351 introduces security measures to protocols used in the energy sector, such as IEC 60870-5 (DNP3, IEC101, IEC104) or IEC 60870 (TASSE.2/ICCP). IEEE 1711 defines a cryptographic protocol to provide integrity and optional confidentiality for cyber security of serial links [1].

There is a very useful set of publications in which security requirements and controls are defined. Security requirements and controls are essential for building a security framework in a system as they explicitly define security measures (objects and actions) which must be present in the system in order to assure its protection. Examples of standards used by the industry include the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), the Department of Homeland Security (DHS) Catalogue of Control Systems Security, NIST SP 800-53, ISO/IEC 27001 or ISA/IEC 62443 [1].

Definitions of controls and requirements allow operators to request specific security functions from vendors in the products they offer, as well as to consider appropriate criteria when making purchasing decisions. For instance, IEEE 1686-2007 defines the functions and features to be provided in substation intelligent electronic devices (IEDs) to accommodate CIP programmes. Another example is the 'WIB Security Requirements for Vendors' mandate, which specifies the requirements and provides recommendations for IT security to be fulfilled by vendors of process control and automation systems [1].

There are also guidelines which set out the good practices in industrial security for relevant issues specific to ICS. For example, the CPNI Good Practice Guide series on process control and supervisory control and data acquisition (SCADA) security focuses on aspects like cyber-security assessments of ICS, configuring and managing remote access for ICS, or firewall deployment for SCADA and process control networks [1].

Another group of publications is devoted to risk-management-related concepts and methodologies, and includes, for example, ISA-62443-3-2, or NISTIR 7628, which is based on NIST SP 800-39, NIST SP 800-30, FIPS 200, FIPS 199, NERC vulnerability and risk assessment and other documents.

For an enterprise, a very important aspect of cyber security is to establish a ISMS. There are very few documents which advise operators on how to incorporate industrial control systems into their ISMS. One of them is IEC 62443-2-1, which adapts the relevant content of ANSI/ISA 99, defines the elements necessary to establish a CSMS for ICS and provides guidance on how to develop those elements. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organisation.

Other documents that help operators develop such an ISMS system are API 1164 or a combination of the famous ISO/IEC 27000 framework with NIST SP 800-82. API 1164 provides pipeline SCADA operators with a description of industry practices in SCADA security, and a framework needed to develop sound security practices within the operator's individual companies.

ISO/IEC 27000 framework is composed of information security standards which provide recommendations on information security management, risks and controls within the context of an overall ISMS. The series is broad in scope and non-ICS specific, aiming at organisations of all structures and sizes. For this reason it is necessary to use it in conjunction with other, more specific publication(s), for example NIST SP 800-82.

NIST SP 800-82 provides guidance on securing ICS, including SCADA systems, distributed control systems (DCS) and other systems performing control functions. The document gives an overview of ICS and typical system topologies, identifies common threats and vulnerabilities to these systems and provides recommended security countermeasures to mitigate the associated risks. It also addresses specific security controls for ICS, provides enhancements to classic ones and a supplemental guidance for the controls which can be applied in a practically straightforward manner. In addition, there are some other guidelines focusing on specific controls for ICS operators, which could be used as a reference for incorporating ICS in the enterprise's ISMS. NIST 800-82 has gained particular recognition and popularity among the stakeholders involved in the ICS field (ICS security tools and services providers, ICS software/hardware manufactures and integrators, infrastructure operators, public bodies, standardisation bodies, academia and R&D) [1].

doi: 10.1049/iet-ifs.2013.0159

3 Developing the ICS security programme

From the available publications we chose the approach for developing a security programme for ICS which is described in NIST SP 800-82 [15]. The publication was chosen from the few standards which address the subject: NIST 800-82, API 1164, IEC 62443-2-1 and ISO/IEC 27000 family (see Section 2). Our choice was based on the fact that NIST 800-82 is actually a widely followed standard, implemented by the ICS operators not only in the US but also globally [1]. It is freely available in the electronic form via the Internet, and describes the phases of the development in a very straightforward and clear form.

In this section we briefly present the ICS cyber security programme development approach described in NIST 800-82 and indicate where it was complemented by our new contributions, namely the method for the estimation of costs of activities within the cyber security lifecycle and the security evaluation approach for critical infrastructures. More detailed descriptions of these contributions are presented in the Sections 4 and 5.

According to NIST 800-82, the first step in developing a cyber-security programme for ICS should be establishing a business case which presents the unique characteristics of a particular company. The role of this business case is to provide the business impact and financial justification for developing an integrated cyber-security programme [15]. It should include detailed information about:

- the benefits of creating the integrated security programme,
- prioritised potential costs and damage scenarios for cases where no cyber security programme is implemented,
- overview of the processes involved in the cyber security programme lifecycle (implementation, operation, monitoring, review, maintenance and improving),
- costs and resources required for these processes.

There are four main elements of the business case: prioritised threats, prioritised business consequences, prioritised business benefits and estimated annual business impact.

The process of developing a security programme consists of multiple steps and starts with obtaining the acceptance of enterprise's senior management for performing cyber-security-related activities. The key components of the process for developing a security programme are presented in Fig. 1, which also show where the new method for cost estimation and the security evaluation scheme described in Sections 4 and 5 should be integrated.

The senior management acceptance is a prerequisite without which it is impossible to commence any security assurance activities. The big challenge for security officers, information system operators and any other players involved in the security of industrial control systems is the less than favourable attitude taken by the senior management of the enterprises which use these systems [1]. This is often caused by their incorrect (exaggerated) estimation of security assurance costs, so they perceive the security only from the angle of excessive costs, not seeing the benefits and added value from protecting their crucial systems [1]. That is why it is very important to prepare a convincing (but of course – realistic) business case, and to provide a faithful estimations of these costs. However, there are very few techniques which help in performing this step, either addressing the subject from a different perspective or exposing certain limitations (Section 4.1). In this paper we describe a new method which addresses these issues, described in Section 4.

Once the approval of the senior management is obtained (which some experts believe is 50% of the success of the whole security assurance endeavour) we can start with the security assurance activities. First, we need to build a cyber-security team, consisting at least of a member of the organisation's IT staff, a control engineer, a control system

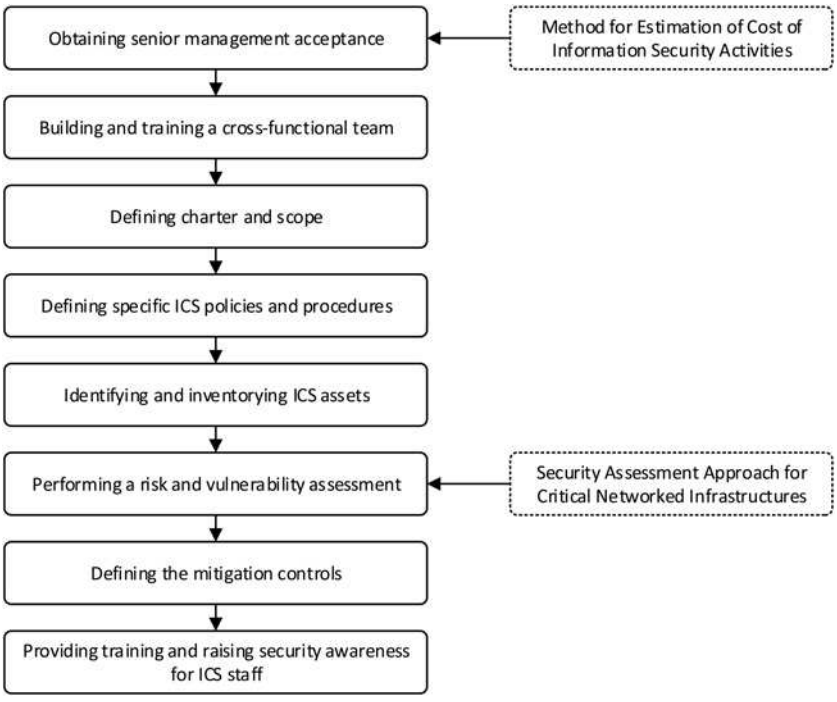

Fig. 1 *Integration of the NIST 800-82 security programme development process with the method for estimation of the cost of information security activities and the security assessment approach for critical networked infrastructures*

operator, security experts and a member of the management team. It is important that they should have properly assigned roles and responsibilities, and that they share knowledge between each other as well as complying with reporting schemes.

The appointed team should devise and document the corporate policy, where roles, responsibilities and accountabilities of system owners and users are defined, together with the objectives of the security programme. It should also indicate the business organisations affected, information assets involved, the budget and resources required, and the division of responsibilities.

The development of the corporate policy should be followed by the definition and communication of the security policy. Policies and procedures are very important for achieving a successful security programme. They should be integrated with existing operational/management policies and be as transparent as possible because the degree of their implementation depends on their clarity.

In the next stage all assets which form the industrial control systems, such as computer systems, networks and applications, should be thoroughly identified and documented. NIST 800-82 recommends that the inventorying should be focused on systems rather than just devices, and should include programmable logic controllers, DCS, SCADA and instrument-based systems that use a monitoring device such as a human–machine interface.

When all the ICS assets are inventoried the cyber-security team can commence the risk and vulnerability assessment process. This part is the most important part according to many experts, because if done correctly, it will lead to a position where the appropriate system assets are properly protected, and the system is secure at the agreed level. On the other hand, when performed superficially, it may create a situation where irrelevant system components are being guarded, whereas the sensitive ones are left without protection. Of course, this also suggests that the financial resources were spent improperly. In view of the recognised importance of this stage of information security programme development, many standards, guidelines and recommendations have been proposed which address this area, such as ISO/IEC 27005 [18], NIST SP 800-30 [19], AIRMIC resources [20], risk management information hub by ENISA [21], CPNI guidelines [22] and many more.

The key component of performing an effective risk and vulnerability assessment is the identification of the vulnerabilities, threats and risks. The approach which is particularly suitable for industrial control systems is based on attack simulation (as opposed to penetration testing) of attacks against the evaluated systems [16, 17]. In Section 5 we briefly explain our approach to vulnerability and security evaluation which we developed and have been using for years. Detailed descriptions of the approach can be found in [16, 17].

Once the risks, information assets and threats are prioritised, the team begins selecting and applying security solutions which will reduce the risks to an acceptable level. These controls can be at the technical, operational or management level and include, for example, access control, awareness and training, contingency planning, personnel security and more [23]. Many guidelines exist here as well.

The final step in the development of the information security programme is based on designing effective training and awareness programmes and communication mediums to help employees understand the need for introducing new access and control methods into their daily work life, the ways they can use in order to reduce cyber security risk, and the impact on the organisation if control methods are not incorporated. Training programmes also demonstrate the management's commitment to the cyber security programme.

More details regarding these steps can be found in [15, 24].

4 Method for estimation of cost of information security activities

As mentioned in the previous section, the business case required for developing a security programme should include detailed information about the costs and resources required to develop, implement and maintain the programme. According to our research, the set of tools which could support the estimation of these costs is very limited and practically consists of one method (see the next subsection). In order to address this lack of support tools, we have developed a new method, designed to facilitate estimation of the cost of activities involved in the cyber-security lifecycle. The method was developed in the following steps:

- selection and adaptation of a costing system,
- preparation of the list of activities,
- assignment of cost centres and activity cost drivers,
- specification of input data,
- output data.

The overview of these steps is presented in the following sections, after the discussion of available alternative approaches.

4.1 Related work

Annual loss expectancy (ALE) is quoted [8] as one of the earliest methods for computer incident cost analysis in the computer industry. It was published in 1979 by the NIST in the FIPS 65 guideline, which described a quantitative method for performing risk analysis. From that time cost–benefit analysis techniques and tools have been applied to this domain. The methods or models described in the literature are [The literature also mentions CICA (cyber incident cost assessment), but its documentation is unavailable.]:

- I-CAMP and its follower I-CAMP II developed by Big Ten universities [8],
- SQUARE [25].

In fact, ALE is not a method for cost estimations but a risk estimator which takes into account the costs of a security breach. The documentation of ALE recommended using the 'order of magnitude approach' for approximating the values required for calculating the estimator. This recommendation was often misunderstood by users and lead to incorrect interpretations of the results obtained [9].

I-CAMP project, funded in 1997 by the chief information officers of the CIC (CIC – Committee for Institutional Cooperation/Big Ten. The Big Ten universities include The University of Michigan, Pennsylvania State University, Purdue University and Indiana University.) universities, proposes an estimate of the actual costs of particular IT incidents, where the total cost is obtained by adding the costs on the resolution side of the incident, the costs on the user side of the incident and other cost factors that include

doi: 10.1049/iet-ifs.2013.0159

new purchases necessitated by software and hardware failures. The method was refined in 1997 with the release of I-CAMP II [4, 5]. The difficulty in using the method is that it requires continuous data gathering and incident logging. It is also very difficult to assess the costs on the users' side. According to [8] the I-CAMP model is appropriate for the situations where the related usage losses are in fact close to nil.

SQUARE is the cost/benefit analysis framework developed by the SQUARE Team (SQUARE Team is a part of an independent research and development project of the Software Engineering Institute.) which aims at providing acceptable estimations for small enterprises in their information security improvement projects. The method uses categories of threats for gathering historical data on computer incidents and the ranges of financial losses because of exposures to these categories of threats [25] and takes advantage of publicly available sources of data on threat categories to estimate costs, benefits, baseline risks and residual risks [25].

Furthermore, certain well-recognised economic metrics are in common use, including the rate of return, maximum net present value or the return on investment [10]. Additionally, there are simple calculators of potential losses such as the Data Breach Risk Calculator of Ponemon Institute & Symantec Corporation [26], Tech//404 Data Loss Cost Calculator [27], Websense Hosted Email Security Calculator [28, 29]. The calculators provide quick and rough calculations, mostly for illustrative purposes of the financial impact of a security incident on an organisation. Their calculation formulas and methodologies are mostly implicit.

Practically, all of the presented methods aim at estimating the cost of a security breach. They focus on the benefit side of the cost–benefit equation, based on the question how much one can gain from investing into the information security, where the gain is understood to mean avoided security incident and its consequences. The cost side of the cost–benefit equation, defined by the question 'how much must I invest' is addressed by cost calculators, but the precision of their estimations is far from sufficient. Also the fact that their algorithms are usually hidden is not to their advantage. Finally, they concentrate on the hardware/software aspect of the investments leaving people and maintenance questions unanswered.

The method presented in this paper addresses these limitations. The calculations are made on the basis of a well-grounded framework of NIST SP 800-53 [23], for which the minimal set of input parameters was carefully selected. The algorithm is fully transparent.

4.2 Selection and adaptation of the costing system

Traditional costing methods are aimed at the determination of unit cost, based on known direct and indirect costs. This approach is inadequate for the assessments of security costs where it is the direct and indirect costs that are unknown, and that in fact constitute the primary object of the assessment.

ABC systems, on the other hand, are focused on activities as fundamental cost carriers. As such they appear particularly suitable, as they propose 'behavioural' assessment (in contrary to 'material' – related to physical assets) of security cost, based on the determination of all activities of security management process. In ABC each activity will be linked to relevant cost centres using cost drivers, and subsequently the cost of the activities will be determined.

Thus the analysis shows that ABC [30] systems are the most suitable for the determination of the cost related to information security implementation and maintenance activities.

4.3 Preparation of the list of activities

In the next step of method of development it was necessary to identify in detail the activities which form the process of information security maintenance and implementation.

To achieve this goal, security management standards and widely recognised literature were analysed, which among others included ISO/IEC 27001, Common Criteria, NIST publications (e.g. [23, 31]), Managing Cisco Network Security: Building Rock-Solid Networks by Florent Parent [32], Designing Security Architecture Solutions of Jay Ramachandran [33], Information Security Policies and Procedures – a practitioner's reference by Thomas R. Peltier [34], Harold Tipton's Information Security Management Handbook [35] or Steve Purser's A Practical Guide to Managing Information Security [36]. For the sake of versatility, a standard-based list of activities was preferable.

As a result of the analysis, NIST special publication – Recommended security controls for Federal Information Systems and Organizations (NIST 800-53 Rev. 3) [23] was selected as the primary source enumerating security activities. The choice was based on the fact that it is actually a standard followed by all American national organisations; it provides a comprehensive list of security components in all areas of the information security management and rationally addresses security problems, which means that the proposed requirements are not excessive, while compliance leads to a high level of information security in the organisation.

The list of activities based on NIST SP 800-53 comprises 101 activities in the following 18 areas of information security management:

- access control,
- awareness and training,
- audit and accountability,
- security assessment and authorisation,
- configuration management,
- contingency planning,
- identification and authentication,
- incident response,
- maintenance,
- media protection,
- physical and environmental protection,
- planning,
- personnel security,
- risk assessment,
- system and services acquisition,
- system and communications protection,
- system and information integrity and
- programme management.

The security evaluation described in Section 5 is covered by the activities in the area of security assessment and authorisation, taken from the NIST SP 800-53 CA family.

4.4 Assignment of cost centres and activity cost drivers

For all activities their duration times were estimated and activity cost drivers assigned.

Table 1 Costs assignment for AT-2

Estimated duration time		Resource cost driver
Working hours		information security officers/engineers
maximum	1	
minimum	3	
usual	2	
Working hours per user		users
maximum	1 × HR	
minimum	3 × HR	
usual	2 × HR	

Four estimates of duration time were evaluated for each activity:

- minimum duration time – the shortest possible time necessary to apply and maintain a security component during a year,
- maximum duration time – the amount of time required yearly for performing the activity which in normal conditions should not be exceeded by an organisation,
- average duration time – calculated as the arithmetic mean of the minimum and maximum duration time,
- usual duration time – the time observed in the daily practice of organisations. It indicates how much time organisations usually took to effectively perform the activity during a year.

As for resource cost drivers, the job positions of personnel responsible for or participating in the performance of the activities were selected and linked to activities, including for example information security professionals, IT administrators and human resources management professionals and users.

Then each activity was assigned resource cost drivers and time duration estimates. These assignments are either in the form of direct values or equations if the value is dependent on other parameters. For example, for the activity corresponding to the security control AT-2 security awareness, the data presented in Table 1 were specified.

4.5 Specification of input data

After the estimation of yearly activity duration times and the selection/assignment of activity cost drivers, the minimum set of input data for the method was specified. The input data correspond to the parameters describing the organisation.

The following data are necessary for the calculations: the number of users, the planned number of information security professionals, staff turnover indicators, mobile device usage index, the approximate number of individuals outside the organisation who have access to the organisation's IT system and average hourly pay rates for the employees on the posts designated as resource cost drivers.

4.6 Output data

The method facilitates estimation of the following parameters:

The total cost of activities associated with the establishment and operation of an information security system in an enterprise, based on the cost of work of all employees involved in the process:

- total cost of activities performed exclusively by information security professionals;
- the number of required working hours for information security professionals;
- the required number of information security professionals.

For each of the parameters the minimum, maximum, average and usual values are derived.

4.7 Case study

The method was applied to various use cases, demonstrating its adequacy and usefulness. In this section we present an example of using the method based on a real-world use case where the method was applied to obtain cost estimations for a branch of a Polish manufacturer of passenger and commercial tyres. The company sells its products to 60 countries on six continents.

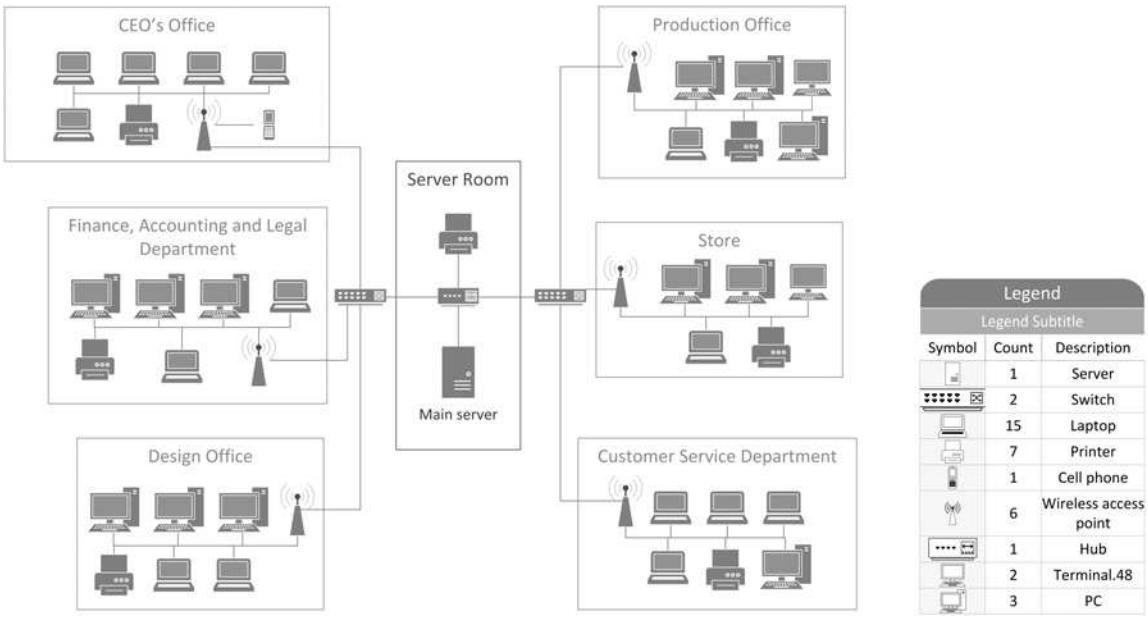

Fig. 2 *Information system of the analysed branch of a Polish manufacturer of passenger and commercial tyres*

doi: 10.1049/iet-ifs.2013.0159

Table 2 Input data for the Polish tyre maker

Indicator	Value
number of users	44
planned number of information security professionals	1
HR – hire rate	7%
TR – termination rate	19%
PDTR – promotion/demotion/transfer rate	4%
I_{midu}	36%
approximate number of outsiders having access to the organisation's IT system	0

Table 3 Estimates of average hourly gross pay rates in the company

Resource cost drivers	Average gross pay rate, EUR
information security professionals	5
IT administrators	4.5
human resources management professionals	4.75
users	3.25
senior-level executives or managers	13.25
physical security officers	3.5
security guards	3
budget planning and control professionals	8.25

Table 4 Estimates of the total yearly cost of activities associated with information security management for the tyres' producer

Total cost of activities, EUR			
minimum	maximum	average	usual
18 691	231 793	125 242	27 957

Table 5 Estimates of parameters associated with information security professionals for the company analysed

Estimated parameters associated with IT security professionals			
Cost of activities, EUR			
minimum	maximum	average	usual
3175	26 355	14 765	8687
Required working hours			
minimum	maximum	average	usual
172	1425	798	470
Required positions			
minimum	maximum	average	usual
0.5	3	2	1

The information system of the analysed division of the company is presented in Fig. 2.

The input data for the method are summarised in Tables 2 and 3.

The results of estimations are summarised in Tables 4 and 5.

5 Security evaluation approach for critical networked infrastructures

The cost estimations obtained using this method combined with the description of benefits of creating a security programme, potential costs of incidents and damage scenarios as well as an overview of cyber security assuring processes will constitute a business case for justifying the need for developing an integrated cyber security programme [15]. After this stage, when the buy-in of senior management is obtained and financial arrangements made, the development of the programme can be commenced, following the steps described in Section 3. The step that has a paramount importance for the effectiveness of the security assurance is the risk and vulnerability assessment, which involves a thorough evaluation of the vulnerabilities of the system. The approach that is suitable for the industrial control systems, where it is crucial that the interferences of the evaluation with the analysed system are reduced to only the absolutely unavoidable ones, is based on the simulation of attacks against the evaluated systems [16, 17]. In order to support these evaluations we have developed a number of tools, such as Industrial Security Risks Assessment Workbench (InSAW) [37] and MAlSim malware simulations toolkit [38].

The approach consists of the following phases:

- Analysis of the information system of the critical infrastructure, aimed at identifying the structure of the information system based on the available documentation, interviews with system administrators, designers and operators and visits and examinations on site.
- Reconstruction of the information system in the simulation environment – building a copy of the critical infrastructure information system in the dedicated laboratory based on the structure identified in the previous stage. Owing to the limitations of available resources, decisions are made with regard to which parts of the original system should be reflected completely and which subsystems can be approximated.
- Identification of use scenarios – analysis of usage patterns of the information system, recognition of the users authorised to use the system or potentially able to use it without authorisation, identification of user access rights and the operational space. The results are documented as use scenarios.
- Design of experiments – definition of the attack goals and affected system sections and textual and attack tree-based description of attack scenarios where subsequent steps required for a successful attack are indicated.
- Performance of experiments – commencing once a 'zero-state' of the simulation environment is ensured, followed by the creation of settings snapshot and running experiments utilising scripts and sensors for observation.
- Collection and analysis of results – gathering information about system events and processing it in order to extract the key, attack-related information. Conclusions as to the security of the information system are formulated, vulnerabilities indicated and countermeasures proposed.

The experiments are performed in a secure and isolated setting of a computer security laboratory. The purpose of the main part of the laboratory setting, namely the mirrored information system, is to reconstruct the information system of the evaluated infrastructure. This part is flexibly configured depending on particular needs. For example, for the infrastructure of a power plant we mirror the process network (interconnecting diverse subsystems of the energy production process), the field network (interconnecting controllers and field devices), the corporate network etc.

Additionally, the environment comprises a number of auxiliary parts which support the configuration,

performance and observation of the experiments or provide any other auxiliary functionality:

- 'Threat and attack simulator' used to reconstruct the attacks and threats that can jeopardise the analysed information system. This is the part of the simulation environment where the simulated attacks are configured and launched.
- 'Observer terminal' for monitoring the traffic of the mirrored information system in order to evaluate the effects of the simulated attacks on the system. It tracks all the malicious or anomalous events happening in the mirrored information system during the tests and experiments and stores them in the central database.
- 'Vulnerabilities and countermeasures repository', where all information about system vulnerabilities and the relative countermeasures is stored. The repository is implemented within the InSAW framework [37].
- 'Testbed master administrator' used for remote network management and for the experiments. It controls the operations related to the initiation and termination of experiments and allows real-time observation of the behaviour of each system during simulations.
- 'Horizontal services' for providing the services necessary for the efficient management of the simulation environment, such as backup services or file sharing services.

The details of the approach can be found in [16, 17]. The costs related to security evaluation are estimated by our cost evaluation method (see Section 4) based on the activities in the area of security assessment and authorisation, taken from the NIST SP 800-53 CA family.

Other interesting reading on the subject of experiment-based or test-based security evaluations can be found in [39–42]. Hussain *et al.* [39] present experiment methodology conceived for the analysis of distributed denial of services, whereas Herzog [40] and Duggan [41] explain security testing methodologies which use systematic penetration testing. Meanwhile, Xu *et al.* [42] have developed a framework for real-time dynamic security assessment of power systems.

Some complementary studies include high-level analysis of possible threats to a power plant system [43] with categorisation of hardware devices involved or a review of security issues in industrial networks [44]. Formal models of a control system, attacks, security goals and requirements are defined in [45]. The problem of malicious human operators in critical infrastructures is analysed and addressed by Lopez *et al.* [46], who developed a solution based on industrial wireless sensor networks and ISA100.11a standard for alarm management.

6 Conclusions

The paper presents a systematic approach to secure industrial control systems defined in the NIST 800-82 [15] standard. We chose NIST 800-82 from the few existing publications which address this subject (see Section 3) because it is a comprehensive, well-written document, dedicated to the ICS systems, widely recognised and used by the stakeholders involved in the ICS field [1].

The approach presented in NIST 800-82 is based on two main components: the establishment of a business case and the development of a security programme. The focus on the business case constitutes a distinguishing feature of the NIST publication. Only a well-formulated justification of the need for the development of a security programme can make it possible to obtain the acceptance of senior management for performing (and investing in) cyber-security activities in the organisation. Senior management's reluctance in this respect has been identified as one of the major challenges in improving the security of industrial control systems [1].

In our studies we have identified the lack of tools which support developing the business case, in particular, the stage dedicated to the evaluation of costs related to information security (see Section 4.1). To fill this gap, we have developed a new cost estimation method described in this paper, where we also illustrate its application for the evaluation of costs in a branch of a Polish manufacturer of passenger and commercial tyres.

The method makes it possible to estimate the overall cost of 101 security-related activities following the definitions in NIST SP 800-53 (see Section 4.3) based on an easily obtainable set of input data (see Section 4.5), and in just a few simple steps. The activities taken into account during the calculations include, among other things, security assessment and authorisation. This is linked to our second proposal – namely a security evaluation approach, which aims at supporting the implementation of the risk and vulnerability assessment phase of the security programme development process defined in NIST 800-82.

The approach is particularly suitable for industrial control systems because it prevents any interference with the evaluated system [16]. In this paper we focused on describing the integration of the scheme with the security programme development process (see Section 3). Details of the scheme can be found in our earlier work [16].

The cost estimation method and the security evaluation approach constitute two concrete tools which support the process of establishing a business case and developing a security programme. By means of the costing method security officers or system administrators will be able to obtain, relatively quickly and easily, the cost figures prerequisite to encourage senior management to invest in information security. The security evaluation approach, on the other hand, consists of steps leading to the identification of system vulnerabilities and risks. Unlike many existing approaches (e.g. [40, 41]), it does not put the system in danger during the evaluation process.

Our further studies in the area will include, among others:

- supplementing the security evaluation method with activities linked to the security controls of the secondary and tertiary NIST SP 800-53 baselines,
- proposing a systematic approach to the determination of physical (hardware and software) assets involved in the information security management process,
- developing a costing method based on ISO/IEC 27001.

7 References

1 ENISA: 'Protecting industrial control systems – recommendations for Europe and Member States'. ENISA, 2011
2 Falliere, N., Murchu, L.O., Chien, E.: 'W32.Stuxnet Dossier'. Symantec Security Response, 2011
3 Byres, E., Lowe, J.: 'The myths and facts behind cyber security risks for industrial control system'. Proceedings of the VDE Congress, VDE Association for Electrical Electronic & Information Technologies, October 2004
4 Rezmierski, V., Deering, S., Fazio, A., Ziobro, S.: 'Incident cost analysis and modeling project'. Committee on Institutional Cooperation, 1998
5 Rezmierski, V., Carroll, A., Hine, J.: 'Incident cost analysis and modeling project 11'. Committee on Institutional Cooperation, 2000

doi: 10.1049/iet-ifs.2013.0159

6 Caulkins, J.P., Hough, E., Mead, N.R., Osman, H.: 'Optimizing investments in security countermeasures: a practical tool for fixed budgets', *IEEE Secur. Priv.*, 2007, **5**, (5), pp. 57–60
7 Mead, N.R., Stehney, T.: 'Security quality requirements engineering (SQUARE) methodology', *SIGSOFT Softw. Eng. Notes*, 2005, **30**, (4), pp. 1–7
8 Mercuri, R.T.: 'Analyzing security costs', *Commun. ACM*, 2003, **46**, (6), pp. 15–18
9 US Department of Commerce: 'Federal information processing standards publication 191: guideline for the analysis of local area network security'. 1994
10 Sonnenreich, W., Albanese, J., Stout, B.: 'Return on security investment (ROSI): a practical quantitative model', *J. Res. Pract. Inf. Technol.*, 2006, **38**, pp. 55–66
11 Li, J., Su, X.: 'Making cost effective security decision with real option thinking'. Int. Conf. Software Engineering Advances, 2007, ICSEA 2007, 2007, p. 14
12 CMS: 'Cost calculators and ROI', http://www.cmsconnect.com/Marketing/CalMain.htm, accessed April 2014
13 Postini, 'Return on investment calculator', http://www.postini.com/services/roi_calculator.html, accessed April 2010
14 Stouffer, K., Falco, J., Scarfone, K.: 'NIST SP 800-82: guide to industrial control systems (ICS) security'. NIST, 2011
15 Stouffer, K.: 'NIST SP 800-82 guide to industrial control systems (ICS) security. Revision 1'. NIST, 2013
16 Leszczyna, R., Fovino, I.N., Masera, M.: 'Approach to security assessment of critical infrastructures' information systems', *IET Inf. Secur.*, 2011, **5**, (3), pp. 135
17 Fovino, I.N., Masera, M., Leszczyna, R.: 'ICT security assessment of a power plant, a case study'. Proc. Second Annual (IFIP) Working Group 11, Tenth Int. Conf., 2008
18 ISO/IEC 27005:2011: 'Information technology – Security techniques – Information security risk management', 2011
19 NIST SP 800-30 Rev. 1: 'Guide for conducting risk assessments' (Gaithersburg, USA, 2012)
20 'Airmic: Together Leading in Risk', http://www.airmic.com/, accessed April 2014
21 'Risk Management', http://www.enisa.europa.eu/activities/risk-management, accessed April 2014
22 'Process control and SCADA security - good practice guidelines', http://www.cpni.gov.uk/advice/cyber/scada/, accessed April 2014
23 National Institute of Standards and Technology (NIST): 'NIST SP 800-53 Rev. 3 recommended security controls for Federal Information Systems and Organizations' (US Government Printing Office, 2009)
24 ANSI/ISA, ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems: 'Establishing an industrial automation and control systems security program' (ISA, 2011)
25 Xie, N., Mead, N.R.: 'SQUARE project: cost/benefit analysis framework for information security improvement projects in small companies'. Carnegie Mellon University, 2004
26 'Data Breach Risk Calculator', https://databreachcalculator.com/, accessed April 2014
27 Tech//404 data loss cost calculator', www.tech-404.com/calculator.html, accessed June 2009
28 'TCO calculator: websense hosted email security calculator', http://www.websense.com/content/TCOCalculator.aspx, accessed April 2014
29 Symantec, 'Small business risk calculator', http://eval.symantec.com/flashdemos/campaigns/small_business/roi/, accessed April 2014
30 Drury, C.: 'Management and cost accounting' (Thomson Learning, 2004, 6th edn.)
31 National Institute of Standards and Technology (NIST): 'MIST SP 800-12: an introduction to computer security: the NIST handbook' (US Government Printing Office, 1995)
32 Lusignan, R., Steudler, O., Allison, J.: 'Managing cisco network security: building rock-solid networks' (Syngress, 2000)
33 Ramachandran, J.: 'Designing security architecture solutions' (Wiley, 2002)
34 Peltier, T.R.: 'Information security policies and procedures: a practitioner's reference' (Auerbach Publications, Boston, MA, 2004, 2nd edn.)
35 Tipton, H.F., Nozaki, M.K.: 'Information security management handbook' (Auerbach Publications, Boston, MA, 2010, 6th edn.), vol. 4
36 Purser, S.: 'A practical guide to managing information security (artech house technology management library' (Artech House, Inc., Norwood, MA, 2004)
37 Fovino, I.N., Masera, M.: 'InSAW – industrial security assessment workbench'. IEEE 1st Int. Conf. Infrastructure Systems and Services: Building Networks for a Brighter Future, 2008, pp. 1–5
38 Leszczyna, R., Nai Fovino, I., Masera, M.: 'Simulating malware with MAlSim', *J. Comput. Virol.*, 2010, **6**, (1), pp. 65–75
39 Hussain, A., Schwab, S., Thomas, R., Fahmy, S., Mirkovic, J.: 'DDoS experiment methodology'. Proc. DETER Community Workshop on Cyber Security Experimentation, 2006
40 Herzog, P.: 'OSSTMM 3 – the open source security testing methodology manual'. ISECOM, 2010
41 Duggan, D.P.: 'Penetration testing of industrial control systems' (Sanaia National Laboratories, Albuquerque, 2005)
42 Xu, Y., Dong, Z.Y., Xu, Z., Meng, K., Wong, K.P.: 'An intelligent dynamic security assessment framework for power systems with wind power', *IEEE Trans. Ind. Inf.*, 2012, **8**, (4), pp. 995–1003
43 Creery, A.A., Byres, E.J.: 'Industrial cybersecurity for power system and SCADA networks', *IEEE Ind. Appl. Mag.*, 2007, **13**, (4), pp. 49–55
44 Cheminod, M., Durante, L., Valenzano, A.: 'Review of security issues in industrial networks', *IEEE Trans. Ind. Inf.,* 2013, **9**, (1), pp. 277–293
45 Amin, S., Cárdenas, A.A., Sastry, S.S.: 'Safe and secure networked control systems under denial-of-service attacks', in Majumdar, R., Tabuada, P. (Eds): Hybrid Systems: Computation and Control (Springer, Berlin, Heidelberg, 2009), vol. 5469, pp. 31–45
46 Lopez, J., Alcaraz, C., Roman, R.: 'Smart control of operational threats in control substations', *Comput. Secur.*, 2013, **38**, pp. 14–27