# Heuristic Cyber Risk Assessment of Industrial Control Systems

*Ulrich Greveler*[1]

## *1. Introduction*

Industrial control systems (ICS) are systems, connected hardware devices and production controls used to automate industrial machinery and processes. They play a pivotal role in the digital manufacturing domain as they implement the large-scale fabrication process after prototype production and single-item production with 3D printing have run their course. These systems include programmable (logic) controllers (PLC), distributed control systems (DCS), supervisory control and data acquisition systems (SCADA). Control systems are implemented in many industrial sectors such as manufacturing, the chemical, electrical, pharmaceutical and oil / gas industries, power plants, logistics or food production. Control systems are essential to most critical infrastructures: energy and water networks, traffic control, postal service and telecommunication because they allow manufacturers to create the complete definition of a manufacturing process as they implement Digital Manufacturing in assembly sequencing and factory layout. Digital manufacturing enables companies to foster their productivity in both manufacturing planning and production processes – industrial control systems cover the production part and allow for real-time access to production data.

[1] IT Security Lab. Department of the Faculty of Communication & Environment
Rhine-Waal-University of Applied Sciences
Friedrich-Heinrich-Allee 25, D-47475 Kamp-Lintfort, Germany

The principal security goal for control systems is availability rather than confidentiality which is typically a primary goal for non-industrial computer systems in the conventional IT domain (*e. g.*, banking, trading, and services). ICS have customarily been created aiming at the purposes durability, dependability and ease of safe use (Krotofil and Gollmann 2013, 1).

In the past, before digital modelling and fabrication (i. e. digital manufacturing) were established concepts, control systems were not regarded as part of the information technology (IT) infrastructure and also had little in common with IT systems regarding technical components, digital devices, interconnection and interfacing. This has changed dramatically.

> (…) what used to be an analogue sensor has become a high-tech transmitter with multiple wired and wireless communication modes and even a web-server, so that the maintenance staff can take the readings without approaching the device or remotely calibrate it to the process requirements. (Krotofil and Gollmann 2013, 1).

Control systems are adopting information technology frameworks, support business information systems, are remotely manageable and are realized using industry standard information technology including network technologies and standard network protocols. They have a tendency to bear a strong resemblance to conventional IT architectures and support new IT capabilities (and also carry vulnerabilities associated with these capabilities) but provide notably less separation for control systems from external networks than predecessor systems, establishing the necessity to secure the control systems (Stouffer et al. 2011, 1). A potential objective of targeted cyber-attacks on industrial plants is the destruction of equipment and the sabotage of physical processes which are monitored and controlled by ICS (Krotofil and Gollmann 2013, 3).

Setting ICS security goals for fabrication sites is one challenge but evaluating whether the goals are achieved and related risks are addressed is yet another one. In this paper a heuristic security risk assessment of ICS based production facilities is proposed which may support a business owner’s decision making process whether the remaining risks are to be

accepted, mitigated or transferred (*i. e.* to let the company become an insured party).

The remainder of this paper is divided into three sections. At first cyber risk insurance products that have recently been presented by several insurers are discussed. They explicitly or exclusively cover cyber risks of businesses regarding electronic office business processes. They often fail to cover the potentially enormous damages stemming from breaches of the control systems, e. g. hardware and equipment damage or damages from explosions caused by compromised control systems. In the following section a heuristic and phased approach (targeting small and medium size enterprises) is presented that can support the assessment of fabrication sites which operate industrial control systems with a manageable amount of components. The last section draws conclusions from the conceptions laid out in this paper.

## *2. Cyber risk insurance*

Businesses conventionally carry insurance that provides protection against various technical, natural and financial risks. However, established policies do not fully cover the supplementary risk companies have to face as a consequence of being part of a connected digital world of things. Moreover, digital and computer network based exposures are progressively more subject to exclusion from established insurance contracts as business liability and property policies were initially aimed to respond to liabilities and natural perils that harm physical objects (Finch and Spiegel, 2014). While digital objects (e. g. stored data) can obviously be harmed by natural as well as intentionally inflicted perils, they cannot be contained in a set of tangible entities – and thus they are often excluded from risk coverage. Digital stored data is quickly moveable, can exist in the form of distributed identical copies and may even exist within virtual systems that cannot be pinned down to a piece of hardware – this distinct nature of digital objects makes the inclusion in a set of covered entities a complex undertaking.

In the recent past, several insurers have presented new products explicitly or exclusively covering cyber risks. According to a risk transfer which

offers an analysis of up-to-date cyber insurance products (performed by product website compilation in March 2015) these products include damages that stem from:

- theft or unauthorized modification of sensitive data, such as health records, financial information, intellectual property or trade secrets
- computer fraud
- defamation
- malware that can damage data, damage wreck hardware, disconnect networked entities and gobble business processes
- web site defacement

These insurance products typically provide cyber coverage for businesses that fall into one or several of the following categories:

- collect, process, disseminate or store sensitive private data
- depend on electronic office business processes
- depend on PC client availability or computer networks
- use cloud based or outsourced IT infrastructures without a sufficient risk transfer to the vendors in place
- provide digital products or online services
- need to comply with payment card industry security standards
- perform business transactions via web shops of web service based operations

It is a disadvantage for industrial sectors using digital production controls that executives who explore offers and buy coverage to address cyber threats only take data breach incidents into consideration but neglect risks relating to industrial control systems. The latter are often generally excluded from coverage. Most cyber insurance policies currently visible in the marketplace (March 2015) cover a combination of conventional liability coverage protecting against claims by third parties (e. g. liability to customers and staff members for breaches of their private information) as well as first-party coverage insuring digital damages of different kinds to the insured. Excluded from coverage are damages stemming from breaches of the control systems:

- damage to hardware and equipment
- explosions caused by compromised control system
- long-term production outage (subsequent damage)

- environmental damage
- health damages and injuries of personnel, loss of human life
- destruction of production output, parts and material
- disruption of delivery chains (subsequent damage)

As the aforementioned damage categories can be of considerable financial magnitude, the exclusion of cyber risk coverage cannot only be explained by negligible awareness of control system related threats. There is also a reasonable motive to exclude damage categories that boost premiums to such an extent that the insurer's product is not marketable anymore. It might also be the case that risks are to be included which cannot be assessed by the insurer since none or too limited previous incidents have come to the attention of the underwriters who are then unable to perform ample statistical analyses.

## *3. Heuristic Risk Assessment*

Risk assessment is a periodic activity that deals with the analysis and monitoring of vulnerabilities and threats. Evaluating risks in industrial production processes involves assessing likelihoods of damaging events and respective impacts of these events within the production site, the environment and on affected products. The effectiveness of ICS security measures can be rated by their effect on reducing associated risks. Potential events that have become real incidents help to collect data allowing a re-evaluation of the risk assessment activity itself. Incidents also help to focus the awareness of decision makers who otherwise might develop a *blind spot* for risks that have never caused any damage to their production site or similar sites of competitors. Thus the public availability of information on incidents and on supplementary data of the impact has a positive effect on general risk awareness in the industrial sector.

A small number of incidents help to derive notions and concepts regarding attack patterns and impact settings. A large number of evaluated incidents enable risk controllers to calculate probabilities and actuarial damage expectations for certain types of attacks. However, in the industrial production sector we face the challenge to only have

(public) knowledge of very few incidents although some of these had a rather enormous impact. A rigorous incident-driven statistical approach to ICS related risk assessment is therefore infeasible in the foreseeable future. This opens the field for heuristic approaches to risk assessment that aim at using data and empirical results of other domains and utilizing them to industrial sectors by applying reasonable assumptions.

### *3.1 Notable Incidents*

As of this year only very few ICS control system security incidents with significant damages have become public knowledge. Notable incidents are the following (cited in chronological order).

- An Idaho National Laboratory experiment in the year 2007 demonstrated how malicious control commands can destroy industrial equipment. The researchers rewrote the ICS computer code for an electric generator, changed the operating cycle of the generator and sent it out of control. The attack involved the opening and closing of a circuit breaker that resulted in an out-of-phase situation and eventually caused the generator to self-destruct. (Zeller 2011)

- The *Stuxnet* worm is a highly targeted? selective malware analysing specific conditions on potential targets. According to reports it attacked Windows PCs using at least four different zero-day exploits (*i. e.* previously unknown vulnerability). The attack focused on particular Siemens programmable logic controllers. Stuxnet directly targeted the controlling parts of the physical machinery of the Bushehr nuclear plant in Iran but also infected 50,000 - 100,000 computers in Iran, India, Indonesia, and Pakistan. (Chen, 2010) While the management of the nuclear facility denied that the worm had instigated significant destruction, they admitted that a small number of personal computers had been affected. However, other reports mentioned a two-month delay in starting up the reactor that could have been caused by Stuxnet, but there has been no confirmation of the malware's involvement in this delay.

- A cyber-attack, performed by an advanced persistent threat group (APT) using spear-phishing and social engineering techniques, against a steel production plant in Germany resulted in massive damage since the plant was not able to shut down a furnace (BSI 2014, 31). The attackers managed to cause multiple components of the system to fail. While the resulting physical damage to the furnace could have been an inadvertent by-product of the attack, an analysis based on the attackers' actions showed that, they must have had advanced technical knowledge of the control systems and the victim's production environment. No examination of possible motives has been published.

### *3.2 Heuristic Assessment of Control Systems*

Since there are not enough reported incidents to allow insurers to base their premiums on incident rates per industry or to statistically calculate the size of adequate funds to be set aside for anticipated losses premiums cannot be calculated. But since on the other hand a growing demand to transfer cyber security risks for industrial control systems to insurance companies is expected some provisional projections of expected claims have to be considered. This way at least some imprecise premium estimation can be derived. In other words: There is not enough data but ballpark figures have to be computed anyway in order to jump-start the ICS cyber insurance market. A rationale for this rather casual attitude with quantities is that, after some time, claims can be recorded and claim statistics can be made available which then allow for premium corrections or a re-writing of contractual clauses describing the obligations for coverage of certain types of incidents.

In this paper we propose a straightforward heuristic which consists of four phases (*a*-*d*) and targets at small and medium size enterprises which operate industrial control systems with a manageable amount of components. It can be used to assess the cyber risk to which a company's production facilities are exposed and it can help to decide whether the risks are to be accepted, mitigated or transferred (*i. e.* to let the company become an insured party) and finally to weigh up the premium rate offered by an insurer.

The heuristic is straightforward in the sense that the two quantities *magnitude of the event* (damage impact) and *likelihood of occurrence* (***i.e.,*** probability) of each event are considered – and that the sum of the products of the quantities is calculated. Apart from this standard probabilistic risk assessment method, two further features are included: (*i.*) a category of IT components is defined which can be used to identify certain ICS components by resemblance and (*ii.*) events are partitioned into undirected and a directed incidents in order to explicitly include sophisticated techniques used to exploit vulnerabilities in a targeted manner by an highly skilled attacker.

Note that the introduction of proper security policies is the action which has to be undertaken *before* this assessment takes place – not afterwards. The assessment can help to evaluate the policies and refine them after assessment, though.

a. Identify ICS components that, from a purely information technological point of view, show some major resemblance to certain IT components which are to be categorized in the following short list
    - PC with network access
    - server (hardened)
    - server (office environment, web server)
    - database application
    - networking equipment device
    - mobile device
    - entry point (e. g., VPN gateway, old-fashioned dial-up modem, wireless access point, firewall)
    - external storage device

b. Assume incident probabilities for these components that are roughly the same as typical IT components. But make a simple distinction of
    - undirected incidents (*e. g.*, acts of negligence, malware infection, widespread port scanning of large address ranges)

    versus

- directed incidents (*e. g.*, advanced persistent threats; attacks with elevated skills, major resources or high precision).

c. In the next phase the impact of an undirected (1.) and a directed (2.) incident is to be evaluated for each ICS component. It might be helpful to express this as a verbal question to the process engineers who are familiar with the details of the relevant production processes and the hazards involved.

   1. What impact will it have if this component unexpectedly goes out of service for a considerable amount of time (*e. g.* some hours)?

   2. What impact will it have if this component is used by a highly skilled insider attacker to provoke maximal damage to people, to the equipment and to the production process (*e. g.*, explosion, self-destruction, stealthy interference with production parameters over a long time)?

d. Eventually, all impacts are weighted with the respective incident probabilities and are added up to a weighted sum providing a ballpark figure for a reasonable premium rate. For impact evaluations of the aforementioned steps *c-1* or *c-2* that lead to huge impacts, the incident probabilities should be re-visited in order to decide whether the estimation is sufficiently accurate and to analyse whether changes to the production process are more appropriate than a risk transfer. To provide an example: It might be possible to isolate a connected device from the network in order to mitigate some risks. If the network connection which is used during a set-up phase appears to be unnecessary after production start, it could be less expensive to bear the costs of a periodical connection and disconnection of a device solely for set-up purposes than to accept the risks of network based attacks during production processes.

This process will predictably require a low level of formality in small sized companies operating a controlled production environment. Senior

management should ensure that the assessment project is provided with the resources needed for comprehensive evaluation of all productive areas. It might be encouraging for the assessment team if the senior management highlights areas that should be analysed right at the beginning so that possible resistance of department heads or senior process engineers of crucial production areas is escalated to the management and discussed at an early stage: show stoppers shall be identified before the show has reached its climax.

A difficult task stems from the fact that a major challenge for ICS security is the lack of economical ways to conduct safe and useful experiments which help to measure the impact of successful cyber-attacks on physical entities (Krotofil and Gollmann 2013, 3). The measurement needs to take place by conducting thought experiments, *i. e.* exploring the potential consequences of an attack by speculating and educated guessing on its final outcome, partly supported by software-based simulations (if available). First experimentation environments that can simulate physical and cyber systems have been set-up for the analysis of networked industrial control systems (Genge et al. 2012, 1146).

## *4. Conclusions*

The growing dependence of manufacturing and digital industrial automation on interconnected control systems has resulted in a demand for evaluating cyber security related threats and associated impacts. In this paper we presented the cyber risk related exposure of control systems and the problems arising when these risks are to be transferred to third parties (*e. g.*, insurers). While businesses usually carry insurance to preserve against certain kinds of well-known risks, damages from attacks to control systems are not covered by traditional or cyber-risk policies. Moreover, the available data for risk assessment is insufficient.

To tackle this challenge we described a heuristic approach to assess ICS related risks by using the available data of information technology incident reports and by mapping this data to production controls in a straightforward, simplified and economical way.

After the implementation of proper security policies, the proposed assessment takes place in four phases: First, ICS components that resemble certain categorized IT components are identified. Then incident probabilities are determined based on those probabilities for typical IT components with a simple distinction of undirected incidents and directed incidents. For directed incidents elevated skills and major resources are assumed. In the third phase the impact of an undirected and a directed incident is to be evaluated for each ICS component by analysing the answers of process engineers to verbal questions. Finally, impacts are weighted with incident probabilities and added up to estimate a reasonable premium rate.

Since a purely statistical approach to ICS related risk assessment is infeasible (too few incidents are publicly known), our heuristic approach can be applied when premium rates have to be suggested or vetted.

It is foreseeable that production businesses will be growing their awareness of the fact not “just” their data but also their physical assets are at risk. With an increasing number of interconnected digital production systems in fabrication facilities, the number of incidents will most probably rise and the emerging risk area of production related cyber threats will be put on senior management agendas. Insurers have opened the market for ICS cyber risk related products so the future will show what kind of claims will be recorded and which claim statistics will be made available to the public. We will then be able to confirm how accurate our heuristic approach to the cyber risk assessment of industrial control systems turns out to be.

## *References*

BSI (2014): Bundesamt für Sicherheit in der Informationstechnik (Herausgeber, ohne Autorennennung): Die Lage der IT-Sicherheit in Deutschland 2014. BSI-LB15503. Druck- und Verlagshaus Zarbock Frankfurt am Main, November 2014.

Chen, T. (2010): Stuxnet, the Real Start of Cyber Warfare? IEEE Network Journal, issue of November/December 2010. IEEE Press.

Finch, B. E. and Spiegel, L. (2014): Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act. Santa Clara High Tech. LJ 30 (2013): 349.

Genge, B and Siaterlis, C. and Fovino, I. and Masera, M. (2012): A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Computers and Electrical Engineering, Volume 38, Issue 5.

Krotofil, M.; Gollmann, D. (2013): Industrial Control Systems Security: What is happening? Industrial Informatics (INDIN), 2013 11th IEEE International Conference on. IEEE.

Stouffer, K., Falco, J., Scarfone, K. (2011): Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-82.

Zeller, M. (2011): Myth or reality — Does the Aurora vulnerability pose a risk to my generator? 2011 64th Annual Conference for Protective Relay Engineers. IEEE.