Blockchain and critical infrastructures - challenges and opportunities

Alexandru Georgescu, Carmen Elena Cîrnu
National Institute for Research and Development in Informatics - ICI Bucharest
alexandru.georgescu@ici.ro, carmen.cirnu@ici.ro

Abstract: Critical infrastructures are vital sociotechnical systems whose destruction or disruption would have a significant impact on the functioning of society on multiple levels. Blockchain or distributed ledger technology is a fast-growing technique for disintermediating transactions and exchanges of information in the absence of trust. It is likely that blockchain will eventually be used not only in novelty applications, but also in systemically important critical infrastructures. This article suggests that the obvious advantages that will compel the adoption of blockchain are also accompanied by significant disadvantages and sketches some of the resulting issues. A particular case study is done for SCADA systems.

Keywords: blockchain, distributed ledger, critical infrastructures, resilience, industrial control systems

INTRODUCTION

At the basis of the prosperity, stability and predictability of any society is an inventory of infrastructures, both technical and social/organizational, which constitute, alongside key assets and key resources [1], the bedrock for the functioning of that society. An infrastructure is said to be critical if its disruption or destruction would have a significant negative effect on the dependent population, territory or industry, involving human losses, casualties and financial losses, as well as longer term threats to safety and security [2]. The development of critical infrastructures parallels that of the society itself, ensuring that new risks, vulnerabilities and threats emerge not only from the individual critical infrastructures, but also from the exponentially increasing complexity of their interactions [3]. These interactions amount to interdependencies, which are varied, from geographic to physical, social and logical, but have increasingly manifested in the realm of cyberspace, which also provides an important medium for the propagation of risks and of disruptions, with the potential for highly destructive cascading disruptions.

Blockchain or distributed ledger technology is a recent innovation that had found initial application in so-called cryptocurrencies and other speculative or ideological projects. Its potential, however, far surpasses the fields which have most brought it to the public eye, as blockchain enables the automation of processes such as transactions involving trust through its distributed nature which, in theory, makes it difficult to defraud. Therefore, numerous applications requiring trust, either institutional or through some human observer as a third party, can be disintermediated and automated. This results in lower costs and faster processing of said transactions. The surface has only been scratched in terms of what can be achieved through the application of blockchain solutions, but some of the currently developing projects involve logistics chains, financial transactions, database management for privacy protection, decentralized markets, smart contracts and more.

Even as the various national and international authorities strive to introduce regulation to address some of the issues related to blockchain applications, it is becoming apparent that they are not restricting adoption, but managing it. However, this regulation does not yet account for the systemic effects of blockchain adoption on the security of the critical infrastructure system-of-systems, in which it is bound to become a tool for governance, as well as process management. This article explores some of the resulting facets in a non-exhaustive manner, seeing as how the novelty of blockchain makes it unlikely that we could anticipate every possible way in which it can be applied.

CONSIDERATIONS ON SYSTEMIC EFFECTS

Blockchain adoption is likely to become both an asset and a liability for the resilience and functionality of critical infrastructures and the wider system-of-systems. It is a connector between the components of complex systems and agents.

These increased interconnections are a source of efficiency and functionality, also when applied to security systems, but, like all new sources of complexity, they become also a source of new risks, vulnerabilities and threats, heightened by their unpredictable nature [4]. These are all part of the landscape of "normal accidents" [5] resulting from intra-system interaction and tight couplings, and deliberate interference and threats are likely to further deteriorate the security environment.

To understand the systemic effects of blockchain adoption, as evidenced by the wealth of potential application mentioned above, we need to think about the changes in the underlying model which governs economic and security activity. Currently, the vanguard of new developments is the Industry 4.0 concept of increased automation leading to new horizons of efficiency and productivity. An Industry 5.0 concept has been proposed [6] that combines man and machine interaction to achieve the best possible results. However, Gheorghe (2017) [6] claimed that the true advancement of the model would come by integrating security/trust into the equation and dubbed this Industry 6.0.

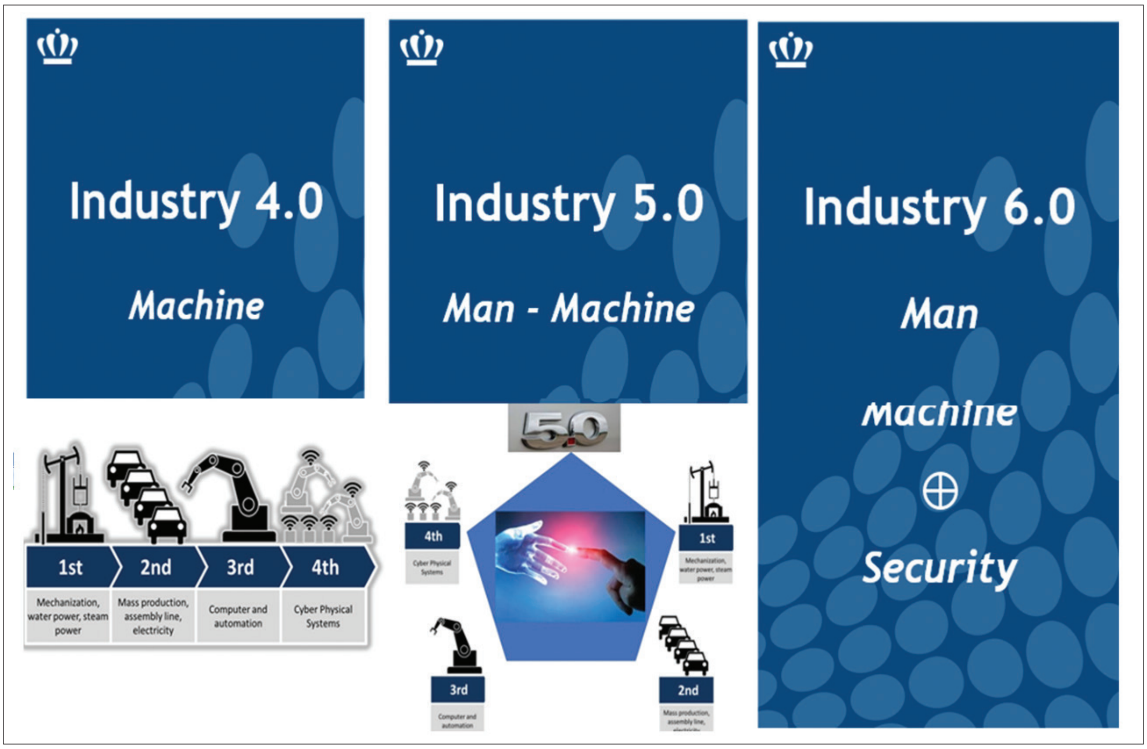
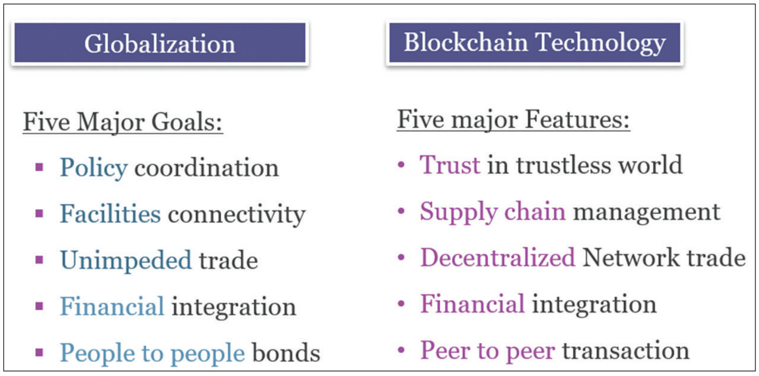


Figure 1. From Industry 4.0 to Industry 6.0 [6]

The concept anticipates the networking effects of the Internet of Things, as well as the impact of blockchain on the issue of trust as a solvent for the barriers, such as they are, in further increasing connectivity, reliability and security. The worldwide acknowledgement of cybersecurity as a fundamental fact of security in a networked world (and, therefore, a networked critical infrastructure system-of-systems) implies that the hard limits to the application of cyberconnectivity to infrastructures are set by security concerns, just like highways have speed limits. Anything that results in the diminishing of that security issue will increase the rate and depth of connectivity.

Security perceptions are just as important as security itself and this means that a complex system of independent but interconnected agents requires trust, something that blockchain is uniquely positioned to offer.



Globalization

Five Major Goals:

- Policy coordination
- Facilities connectivity
- Unimpeded trade
- Financial integration
- People to people bonds

Blockchain Technology

Five major Features:

- Trust in trustless world
- Supply chain management
- Decentralized Network trade
- Financial integration
- Peer to peer transaction

***Figure 2**. Globalization goals and blockchain technology applications [6]*

Figure 2 emphasizes the match between the goals of globalization, which seeks to eliminate administrative and political borders to trade and other exchanges, and the potential of blockchain technology.

With this in mind, we may proceed to the likely effects of systemic blockchain adoption on the topography and architecture of the system-of-systems. As hinted at before, this will create changes mainly in the speed, efficiency and trust of systemic workings, as well as the flexibility of arrangements which prior security realities did not permit, at the margins. This will also create changes in the security environment. The direct application of a new technology or its indirect application through inclusion in existing security tools may decrease security concerns on the one hand, and increase them either through the vulnerabilities of said technology or through unanticipated interaction at systemic level. It is the role of decisionmakers and regulators to ensure that the equation ultimately gives a positive result.

The first change is a greater degree of decentralization. Blockchain, by answering the question of trust, renders trusted intermediaries obsolete. Those intermediaries, whether banks, notaries and others, were a factor for the centralization of the system and a bottleneck for certain types of interactions between system components, expressed as secure information exchanges or transactions. This development was apparent from the beginning with projects such as:

- Blockchain-based decentralized over-the-counter markets for financial trading;
- Financial transfers outside of banks or of the SWIFT system;
- Smart contracts for insurance, energy, financial transactions;
- Database query for sensitive information such as personal data (ex: for confirmation of identity in airports).

While ideologues would expect established actors to wilt and fade away as a result of decentralization, it is just as likely that they will retain their size and power through goodwill, networking effects, brand name and other considerations. But, systemically speaking, in the absence of coercion to continue using established intermediaries, the critical infrastructure systems will become more and more decentralized in finance, ITC and in all infrastructures, in general, in which secure data flows are required for management and coordination between actors.

A second change is the increased complexity of the system-of-systems. Decentralization enables an exponential rise in the number and frequency of interactions, as a result of lower costs and higher relative trust per unit of cost and time. The overall complexity rises, along with the chance for the manifestation of emergent behaviors which could not have been anticipated through the analysis of system components.

A third change is the increase in system opacity through this complexity, which makes system mapping and understanding much more difficult. The intermediaries which imbued transactions and interactions with trust were also valuable "systemic cartographers", through their inordinate insight into the activity they intermediated, as well as through their role as gatekeepers or bottlenecks for their respective areas. Without those and given the inherent properties for anonymity of blockchain, the system in question becomes less transparent. Meanwhile, even though blockchain applications like Bitcoin or ETH pride themselves on full transparency of the ledger (amounts and transactions are freely available online for any Bitcoin or ETH wallet) in combination with full anonymity of the user, it becomes very difficult in practice to understand the system as the information given lacks important informational substrates like context. This opacity increases overall systemic risk, including the ability to recognize important emergent phenomena.

At the same time, the opacity itself changes the behavior of actors, especially in their decentralized state on their respective fields of action. While regulators and government decision makers are important and invaluable in systemic action, the first line of decision and security governance are always the critical infrastructure operators/ owners/administrators, who are overwhelmingly private actors in Europe and the United States. Even where they are not private actors, their organization within state owned entities introduces a hierarchical divide from the actual state decision makers and regulators. These actors have limited fields of vision with the system-of-systems and must take decisions on the basis of incomplete information. The opacity and decentralization of the system-of-systems compound this problem and modify agent behavior in a way which might make it seem individually rational, but becomes collectively disastrous. Bank runs and market panics are examples of autonomous actors pursuing their self-interest in the presence of limited information and low trust in systemic performance, leading to a negative security perception, which leads them to act in a way contrary to their collective interests, but nevertheless fully rational at an individual level, since the one who acts last loses the most. It is also a form of prisoner's dilemma. Such a situation may arise in a blockchain mediated systems such as a purely financial one or a system relying on decentralized contracting in, for instance, energy. We see such effects in the volatility of the cryptocurrency markets, which is a subject not only of capital inflows and outflows, but also of opacity leading to the reliance on a single asset (Bitcoin) as a market mover.

Another change is the increase in system couplings, which Johnsen (2010) [7] as well as Perrow (1999) [5] identify as a main factor in the cascading disruption of complex critical infrastructures. Systems with low coupling values are naturally resilient to delays in processing and feature flexibility in operating methods, in resource management, in substitution and redundancy for processes or resources. Systems with high coupling values have a correspondingly higher speed of propagation and contagion of risk and disruption. The efficiency gains of blockchain use come at the cost of higher couplings, just like countries register new efficiencies, but also higher risk transmission, when they enter free circulation areas and no longer feature border checkpoints for trade or identity verification.

Yet another change, this time taking place in parallel with the system couplings, is the deterioration of the margins of normal operational capacity for the respective critical infrastructure. Efficiency has been noted as being anti-resilience, in that efficiency gains are most often secured at the cost of eliminating diversity in sources and resources, as well as redundancies, substitutive capacities and other resilience enhancing characteristics. The management of margins is one of the most useful resilience-enhancing techniques, by allowing a system to absorb detrimental effects while maintaining an acceptable level of output, thereby safeguarding the entire system-of-systems.

One example in this regard, which illustrates both the deterioration of the management of margins and the tightening of coupling as a result of increased efficiency, is the "just in time" system of inventory management, which keeps standing inventories at a minimum for factories, relying on consistently timely deliveries to keep the industry running at optimum capacity. It is a system which is prone to cascading disruption by outside elements, especially since supply and production chains have become steadily more global. Each of the factories or assets on the route towards finalizing a product and delivering it to a customer has both very slim margins of error for supply disruptions and a tight coupling which enables the rapid propagation of disruption.

The adoption of blockchain solutions, especially to mediate between different infrastructures as socio-technical assets, will also likely entail a change in perspective, organizational landscapes and mental modes, with unpredictable results from the perspective of security for general resilience or crisis and emergency management [7].

It is, ultimately, a difficult feat to estimate the net effect of blockchain adoption on the resilience of critical infrastructures and will likely depend on whether the impetus for initial adoption will be for security applications or for efficiency gains.

Table 1 below summarizes the effects theorized above

BLOCKCHAIN EFFECTS ON SCADA

Industrial control systems, in general, and Supervisory Control and Data Acquisition (SCADA) systems, in particular, are at the core of almost every technical infrastructure system, monitoring and controlling various processes [8]. The vulnerability of SCADA systems to cyber-attacks and other malicious interference, as well as random errors, is a very important subject.

SCADA systems are made up, in general, of sensors, interconnected computer systems and control software applications which enable the funneling of collected data to a central location which interprets them and issues commands, whose feedback is then analyzed.

Blockchain application would not have been, at first glance, a relevant technology for SCADA systems. However, these systems are no longer "obscure", shunted off into their own networks and communication channels separate from the Internet and with proprietary hardware and software solutions. For the purposes of controlling costs, easing maintenance and increasing efficiencies, as the infrastructure being controlled became, itself, more complex, SCADA systems moved online and began to tap into a market of ready-made equipment, communication protocols and technical standards for their operations [9].

BLOCKCHAIN EFFECT ON SYSTEM-OF-SYSTEM	EXPLANATION OF EFFECT
Greater decentralization	Blockchain disintermediates transactions and exchanges by introducing trust in a trustless world, thereby enabling decentralization.
Increased complexity	The lower costs and higher security of blockchain mediated operations, combined with the disintermediation effect, leads to an increase in the potential links between actors, system components and systems, leading to exponential increases in the complexity of the system-of-systems, since it is also defined by the relationships within it.
Increased opacity	The complexity of a system is in an inverse relationship with transparency. Its growth makes the system more opaque, because it becomes more unpredictable through emergent behaviors.
Tighter system couplings	The increased efficiencies, in time and costs, as well as the disintermediation effects of blockchain, increase the couplings between system components, thereby increasing the transmission rate for risks and disruptions.
Lower margins for management	The efficiency also comes at the expense of redundancies, substitutive capacities and other forms of resilience enhancement which economic agents, especially, consider to be costs to minimize.
Transformation of mental modes and organizations	Large scale adoption of blockchain ultimately means the rewriting of organizations, hierarchies, mental modes and other social "software" which ultimately impacts infrastructure at the operational level.

***Table 1**: Blockchain effects on system-of-systems (source: authors)*

This led to a deterioration of the security environment, especially as the advance of “hybrid warfare” or “new generation warfare” made these systems an attractive option for low cost, high impact and high deniability attacks.

To the knowledge of the authors, there are no specific blockchain projects for SCADA systems, but there is a potential for them given that validation of data stream and control network integrity have emerged as a significant security concern in the wake cyber-attacks such as the Stuxnet virus [10]. This sort of trust issue is one that distributed ledger systems are uniquely placed to solve. It is likely that blockchain adoption is taking place on a path of least resistance, with early adopters being in areas of high aggregate value, but low value and risk per mediated transaction, whereas SCADA systems are a “niche” area that is highly regulated and employed by fundamentally conservative actors.

It seems more likely that blockchain integration within SCADA systems will not come through purposeful design, but through incremental innovation and the integration of blockchain-based solutions such as more secure communication standards that address specific flaws. We could see a new generation of blockchain based solutions being applied in this field, as research and development efforts make it easier for blockchain to meet the latency requirements of SCADA applications or to serve as sufficient advance warning of malicious or erroneous activity. Ultimately, this too represents a source of risk, since many of these systems are, in fact, a combination of systems of different generations interacting haphazardly and possibly unexpectedly. A proof-of-concept for blockchain use with SCADA systems will come when we will have the first blockchain applications for the Internet of Things with a net positive impact on security.

SCADA systems face atypical security challenges in comparison with the normal ITC systems, as well as different priorities, which is reflected in the publications by various standardization bodies and in the order of security attribute importance in the SCADA systems as opposed to ITC systems.

From a security perspective, the most important attribute for SCADA systems is the availability of assets. SCADA processes take place in real time and require intact feedback loops and finetuning capacity [11]. Blockchain applications are not so obvious in this area, as they are geared towards certainty and consensus, not speed.

The second more important attribute is integrity, representing the absence of unauthorized, possibly malicious, interference or destruction of information [12]. As mentioned before, this can be an important area for blockchain applications, by increasing trust in the integrity of information flows. Since subtle forms of interference take longer to build towards critical points and can be resolved if detected in time, the use of distributed ledger solutions to verify data integrity in short-term hindsight becomes feasible. Under certain conditions, integrity becomes more important than availability, especially if catastrophic effects follow from the materialization of a negative event.

Blockchain solutions address important security concerns for communication channels – the integrity of data packets and their content, the extent of the built-in protection systems and the vulnerabilities of communication at the level of data transmission.

ICT systems, on the contrary, place distinct emphasis on integrity of access to data and on confidentiality, an area where blockchain found its initial applications and is seeing the largest effervescence of activity. This is not such an important concern for SCADA systems, since data flows are continuous, predictable and not necessarily classified or proprietary.

Of course, third party use of blockchain can make important contributions to overall SCADA security, by ensuring a better verification of identity for people trying to access computers in the network.

There are four types of cyber-attacks which can take place against SCADA systems [13], as presented in the table below.

TYPE OF ATTACK	EXPLANATION OF ATTACK
Reconnaissance	Attackers collect data through various means to map the SCADA system, identify devices and relevant information about these systems, such as manufacturer, model, supported protocols etc.
Response and measurement injection	The attacker seeks to obtain, modify and then distribute information packets from substations to central stations in order to perpetrate hoaxes of actual disinformation. The attacker may even maliciously compose data packets so as to encourage a certain imprecise response by the operator, based on bad inputs.
Command injection	Attacks against both human-operated systems and automatic systems, whereby the control network is compromised and the ability to control and configure responses is usurped. The transmission of hoax command packets can have disastrous results, by ordering devices to function at critical levels or to disengage warning systems.
Denial of service attacks (DoS)	DoS attacks prevent a legitimate user from accessing the system and performing the desired operations, and are mainly performed through the flooding of servers, communication channels and devices with signals and data packets. In addition to preventing the performance of one's duties, these attacks also disrupt the feedback loop which is vital for system integrity.

***Table 2**: Types of attacks on SCADA systems ([13] organized by authors)*

Overall, blockchain based solutions can bring an improvement to SCADA systems in dealing with response and measurement injection attacks, as well as command injection attacks, since they specifically refer to the issue of trust. It is also important to consider the possible security ramifications of blockchain implementation, given that the distributed ledger nodes are not immune to attacks or manipulations, as shown by the visible tribulation of the cryptocurrency community. Hahn and Govindarasu (2011) [14] argue that there is a trade-off between system performance and system security, just as was argued in the systemic effects portion of this paper. Therefore, the implementation of blockchain within or near SCADA systems in order to improve efficiency and performance will also likely increase certain categories of vulnerabilities for the network.

CONCLUSIONS

The distributed ledger technology is receiving increased attention, with entrepreneurs and companies vying to implement it for a reduction in costs, increases in efficiency and better security. The breadth and depth of the proposed projects is significant. Ultimately, blockchain technology will have a measurable effect on critical infrastructures and on the critical infrastructure system-of-systems, to whom cyber connections have become a main category of interdependency and a main vector for the transmission of risks, vulnerabilities and threats. This article explored the possible changes which blockchain adoptions may enable within the system-of-systems, finding that there are systemic security concerns which should be addressed by regulators and national decision makers. A case study was also developed on the potential impact of blockchain on industrial control systems, finding a much more muted effect, in line with the lower variety of applications for this niche field.

Overall, the issue bears further study, especially since the rising complexity of critical infrastructure systems will be compounded by blockchain, leading to unexpected systemic behaviors and new vectors for the transmission of risk.

References

[1] Gheorghe, A., Vamanu, D., Katina, P., Pulfer, R. (2018) *Critical infrastructure, key resources, key assets: [Risk, Vulnerability, Resilience, Fragility, and Perception] Governance*, Springer, Topics in Safety, Risk, Reliability and Quality Series, Vol. 34, ISBN 978-3-319-69224-1

[2] Katina, P.F., Hester, P.T., (2013) *Systemic determination of infrastructure criticality*, International Journal on Critical Infrastructures.9(3), p.211–225.

[3] Katina, P. F., Keating, C. B. (2015) *Critical infrastructures: A perspective from systems of systems*, International Journal of Critical Infrastructures. 11(4), p.316–344.

[4] Keating, C. B., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A. A., Safford, R., Rabadi, G. (2003) System of systems engineering. Engineering Management Journal. 15(3). p.35–44.

[5] Perrow, C. (1999) Normal Accidents: *Living with High-Risk Technologies*, Princeton University Press, ISBN: 9781400828494

[6] Gheorghe, A. (2017) *Internet of Space: Issues for a System of Systems Engineering Approach*, presentation during the 6th annual conference on Space Systems as Critical Infrastructure organized by the Romanian Space Agency and IAA.

[7] Johnsen, S. (2010) *Resilience in risk analysis and risk assessment*, in Moore, T., Shenoi, S. (eds). *Critical Infrastructure Protection IV* - Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. IFIP Advances in Information and Communication Technology series (311), p. 215-227. Washington DC, SUA: Springer, ISBN 978-3-642-16806-2

[8] Mehta, B., Reddy, Y. (2015) *SCADA systems, in Industrial Process Automation Systems*, Elsevier, pp. 237–300. doi: 10.1016/B978-0-12-800939-0.00007-3.

[9] Nazir, S., Patel, S.,Patel, D. (2017) *Assessing and augmenting SCADA cyber security: A survey of techniques, Computers & Security*, 70, pp. 436–454, doi: 10.1016/j.cose.2017.06.010.

[10] Karnouskos, S. (2011) *Stuxnet Worm Impact on Industrial Cyber-Physical System Security*, IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, pp. 4490–4494, doi:10.1109/IECON.2011.6120048

[11] Zhu, B., Joseph, A., Sastry, S. (2011) *A Taxonomy of Cyber Attacks on SCADA Systems*, in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp. 380–388, doi: 10.1109/iThings/CPSCom.2011.34

[12] Maynard, P., McLaughlin, K., Haberler, B. (2014) *Towards Understanding Man-In-The-Middle Attacks* on IEC 60870-5-104 SCADA Networks, in 2nd International Symposium for ICS & SCADA Cyber Security Research 2014. BCS Learning & Development. doi: 10.14236/ewic/ics-csr2014.5.

[13] Morris, T., Gao, W. (2013) *Industrial Control System Cyber Attacks*, ICS-CSR 2013, Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013, pp. 22–29, ISBN: 978-1-780172-32-3, http://ewic.bcs.org/content/ConMediaFile/22618

[14] Hahn, A., Govindarasu, M. (2011) *An evaluation of cybersecurity assessment tools on a SCADA environment*, in IEEE Power and Energy Society General Meeting, doi: 10.1109/PES.2011.6039845.