Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 81 (2019) 582–587

www.elsevier.com/locate/procedia

52nd CIRP Conference on Manufacturing Systems

Oh, no – not another policy! Oh, yes - an OT-policy!

John Lindström[a,]*, Petra Viklund[b], Fredrik Tideman[b], Berndt Hällgren[b], Jonny Elvelin[c]

[a]*Luleå University of Technology, 971 87 Luleå, Sweden*
[b]*Luleå Kommun, 971 85 Luleå, Sweden*
[c]*W3IT Norrbotten AB, 972 95 Luleå, Sweden*

* Corresponding author. Tel.: +46920491528. *E-mail address:* john.lindstrom@ltu.se

Abstract

The paper addresses the need for a policy document in organizations concerned with Operational Technologies (OT) within their production and operational environments, and secondly how such an OT policy was developed and crafted by a Swedish municipality and its water production and wastewater management department. The first initial design criteria was to clearly distinguish the IT environment from the OT environment and the second design criteria was to achieve an improved, affordable and maintainable cybersecurity level for the OT environment. The results of the paper are an initial OT policy and an action plan for the necessary technical and organizational change in the OT environment.

Keywords: cybersecurity; Operational Technology (OT); OT policy; production systems

1. Introduction

The paper concerns the parts of an action research effort at a Swedish municipal water production and waste water management department, where the cybersecurity level for a majority of the Operational Technology[*] (OT) has been investigated, assessed, improved and responsibilities clarified. The term OT comprises the technology related to process industrial IT and automation and is apparently similar to much of the equipment (i.e., firewalls, routers, switches, servers, PCs, etc.) used in the IT environment. This equipment is required to monitor, operate and control, for instance, a company's production environment and processes [1] for: pulp/paper, oil, gas, electricity, heat, food, clean water, wastewater management, minerals and data centres, etc. However, the OT equipment is used for different purposes than the IT equipment and uses a number of completely different communications protocols (which, however, can partly be tunneled in an IP-based network). In addition, in OT-networks a number of specific devices such as Programmable Logic Controls (PLs), sensors, actuators, pumps, valves, SCADA based systems, etc. are commonly present (sometimes in large numbers) together with the main production equipment. The OT equipment and connected production equipment are commonly located in an OT network, which may be connected to an IT network or kept separated due to cybersecurity concerns. Cybersecurity is an issue for most OT networks and equipment [1-2] due to the long lifecycles, i.e., commonly 5-30 years compared to 2-8 years in an IT environment. Further, most of the OT equipment has been developed with an inherent low level of cybersecurity measures – often not exceeding username/password level and any additional security measures need to be "bolted on", which makes it complex and hard to manage over time. In addition, to not impair the availability level of the production networks, the

[*] "Operational Technology" briefly explained - https://whatis.techtarget.com/definition/operational-technology

2212-8271
10.1016/j.procir.2019.03.159

OT environments are commonly only updated once or twice a year, requiring comprehensive testing prior to the rollout of any updates, patches, upgrades or changes. This is a major difference compared to an IT environment, where normally critical security updates are rather quickly dispatched after swift testing and many organizations update their IT environment 3-5 times a year after adequate testing and verification. However, within water production and wastewater management the flexibility for smaller updates and changes is greater than in, for example, a pulp/paper setting.

Most organizations have an IT policy as well as IT or information security policies. Interestingly, very few organizations have an OT policy, although the OT environment may be both larger and more expensive than the IT environment and essential for the organization. Thus, an OT policy is likely necessary in organizations with production environments of significance – although many employees may say "Oh, no – not another policy!". The paper will outline the chain of events that led to the crafting of an OT policy as part of an action research effort.

The rationale for the action research effort was to initiate change and improve the cybersecurity level of the OT environment. However, it was first necessary to clarify the ownership of the IT and OT environments as well as the responsibilities for development, operations and maintenance, etc. Further, an OT environment is also often part of new offers such as Product-Service Systems/Industrial Product-Service Systems [3-4] or Functional Products [5-6], which means that providers of such offers must also consider an OT policy as well due to the additional responsibilities and risks transferred from the customer to the provider.

This paper addresses the question as to whether organizations with significant OT environments should have an OT policy or not as well as what may be needed technically and organization-wise to achieve an improved cybersecurity level for OT environments. Further, the purpose is to make senior management teams, IT- and OT-related personnel, and R&D managers aware of the need for an adequate cybersecurity level within OT networks and the organizational issues that may need to be managed to achieve this. The paper is organized such that the research approach follows the introduction and related work. Further, this is followed by the result section, including an analysis and evaluation and, finally, the discussion and conclusions section.

2. Related work

An OT environment comprises the equipment, which is required to monitor, operate and control a production environment and its processes, and the related production equipment. The OT environments used in various industries are challenged by many of the obstacles and issues in the 5 main categories described by Lee et al. [7]. Further, additional areas of interest are: cybersecurity [1-2], predictive maintenance [8-10], monitoring [9], sustainable and intelligent production [11-13]. These are all relevant and should be considered in order to keep a high level of availability as well as robustness of the OT environments. However, more specifically, concerning cybersecurity within OT environments, which include Internet-of-Things (IoT) or industrial IoT, a number of security/safety-related laws and recommendations are specific for each country. Within the EU several directives and recommendations are applicable [cf. 14-15]. These provide the legal framework and recommendations for the operation and management of OT environments. A recent contribution to the improvement of cybersecurity within OT environments is the industrial internet-based Arrowhead Framework [16], which includes a baseline functionality level for cybersecurity, cloud-based automation, greater flexibility and engineering simplicity. The Arrowhead Framework further supports the RAMI4.0 framework, which is developed to enable transition from traditional ISA-95-based architectures toward Industry4.0-based production environments, where more and more IT will get into the OT. The use of more IT in the OT is also indicated by for instance Hahn [1]. Piggins [2] further outlines that hackers and viruses increasingly targets OT environments in terms of industrial control systems and SCADA-based systems, which requires an increased awareness and protection of these.

For most OT environments, availability and robustness are of the utmost importance. Simulation and frameworks for improvement of availability in industrial OT and production environments have been outlined in for instance [17-18], where operational data is used to improve the models.

Very little has been written on OT policies, although these policies can sometimes be integrated into other types of documents such as IT or information security policies, automation strategies or production environment plans. Thus, the term OT policy seems novel and fitting for the context, providing a missing piece for the management of organizations with extensive production and operational environments.

3. Research approach

The research approach employed in this study, done in collaboration with a Swedish municipality, has been based on an indepth qualitative study using action research. It would also have been possible to use for instance a spiral model with gradual refinement of the research as well. The municipality has a population of less than 100,000 inhabitants and is wide-spread geographically over more than 2000 square kilometers (which is a rather large area requiring extensive OT networks and large amounts of equipment). The target OT area has mainly been the production of clean drinking water and wastewater management, which are considered critical infrastructure by the EU [14-15]. The research targeted in this paper is the first cycle of an action research [19] effort where the researcher has had the roles of external expert/consultant. The research has been conducted from the start of 2016 until the end of 2018. Action research has been defined as "*a participatory, democratic process concerned with developing practical knowing in the pursuit of worthwhile human purposes, grounded in a participatory worldview which we believe is emerging at this historical moment. It seeks to bring together action and reflection, theory and practice, in participation with others, in the pursuit of practical solutions to issues of pressing concern to people, and more generally the flourishing of individual persons and their communities*" [19].

The characteristics of action research are: (1) that action researchers act in the studied situations, and (2) that action research involves two goals. The goals pertain to solving the problem (the role of the consultant) and making a contribution to knowledge (the role of the researcher); further, that action research requires interaction and cooperation between researchers and the client personnel and, finally, that action research can include all types of data gathering methods [20]. In accordance with [21], the action research approach encompasses 4 phases: diagnosing, planning action, taking action and evaluating the action in relation to a certain context and with a specific purpose. The results of a literature review, which was part of the first phase, were used as input for the diagnosis. The phases were completed with an iterative and reflective case management methodology.

The data pertaining to the first phase, i.e., technical and organizational needs for change, were collected during 8 workshops [22] (involving 4-12 key respondents from the IT department, OT development/operation/maintenance departments as well as management persons at each workshop) and 10 semi-structured open-ended interviews [23-24] with key respondents from the IT and OT departments. The workshops and interviews were conducted from early 2016 until late 2018. The respondents were well aware of and knowledgeable regarding IT networks and IT management, OT-networks, production systems/equipment and cybersecurity.

To collect data after the workshops semi-structured interviews with open-ended questions [23-24] were used, allowing the respondents to give detailed answers and the possibility to add extra information where deemed necessary [25]. The duration of the interviews was between one and three hours. The collected data were displayed and analyzed using matrices (cf. [26]) and the outcomes of the planning action efforts were summarized into matrices as well. The analyzed data were finally summarized into two matrices comprising the diagnosis in terms of technical and organizational needs for change (see Tables 1 and 2), and a plan for action (see Figure 2). Some results from the taking-action phase are also outlined in section 4.

The first initial design criterion for the organizational change required was to suggest a clear and rational division of responsibilities and where the IT and OT environments should be separated. The second initial design criterion was to achieve an improved, affordable and maintainable cybersecurity level for the OT environment. The design criteria are evaluated and discussed in the last section of the paper in order to learn if another policy (i.e., the OT policy) is actually needed and if the required changes have led to an improved cybersecurity level for the OT environments addressed. Semi-structured interviews were used during the evaluation of the result of the research and the design criteria.

4. OT environment – technical and organizational change and improvement of cybersecurity level

Figure 1 provides a simplified overview of the old IT/OT-architecture set-up. Further, in Figure 1 the IT networks had the outgoing main connection to the Internet, whereas the OT networks were connected in between via different technologies and mediums. The OT networks were built up using a rather traditional ISA-95 architecture [27].

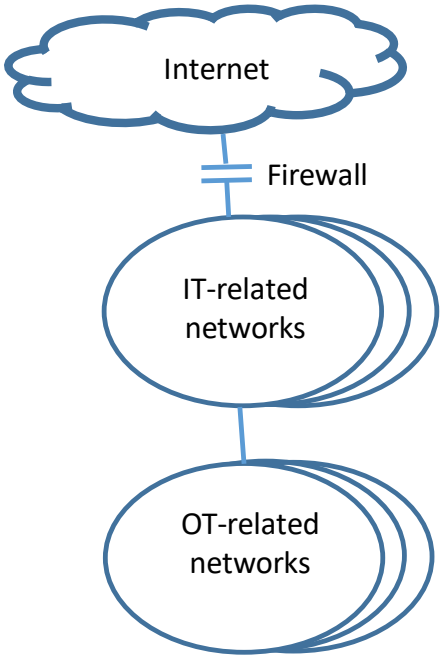

Fig. 1. Simplified IT/OT network set-up before the change.

During the diagnosis phase, the needs for technical and organizational changes were revealed and collected. These are listed below in Tables 1 and 2, and prioritized according to high importance (H), medium importance (M) and low importance (L). High importance means that something needs to be addressed within one year, medium importance that something needs to be addressed within 2 years, and low importance at a later stage. The prioritizations were decided by the municipality.

Table 1. Diagnosis - need for technical change.

Technical issue or need	Priority
1.) Division and demarcation in between the IT and OT environments. Problems or cyberattacks arising in either of the IT or the OT environments should not be able to propagate to each other.	H
2.) Key objects in the OT network must have 24x7 monitoring and alarms.	M
3.) Cyberattacks using IoT equipment for entry, such as cameras and sensors, at end-points should be prevented.	H
4.) The OT environment must continue to work without the IT environment in case of problems or cyberattacks.	H
5.) The plans and procedures in the production process must have alternative procedures (manual) as well as work-arounds in case of issues arising in the OT environment.	H
6.) An extended OT-test environment should be built up to be able to test more configurations and test cases prior to roll-outs in production.	M
7.) Use simulators to support decision-making in complex situations prior to taking action based on experience and estimations.	M
8.) Monitor and keep control of equipment that is connected to the OT network in order to prevent non-authorized equipment from being connected to the network and used.	H

9.) Improve the support process and support system for OT-related issues. Response times should be clarified and necessary changes made to adhere to the response times investigated (e.g., internal and external service level agreements).	H
10.) Ensure that all essential backup processes in the OT environment work and that the data can be restored. Should be done on a regular basis.	H
11.) Important OT servers should have own physical hardware and not only be run as virtual ones.	M
12.) Log management needs to be improved and logs should be further analyzed in order to detect additional anomalies.	M
13.) The level of documentation of the OT environment needs to be improved in certain areas. Further, the documentation should only be made available electronically to employees who need to know.	H

The technical change needs with a high importance (H) prioritization were passed on to the next phase action planning.

Table 2. Diagnosis - need for organizational change.

Organizational issue or need	Priority
1.) Responsibilities to be clarified in terms of ownership and responsibility for development, operation and maintenance for the IT and OT environments.	H
2.) Continuous co-planning and sharing of information and changes in between the IT department and OT-related departments. This should be on operational as well as tactical levels during the normal work processes and also on strategic level when necessary prior to long-term and important decisions.	H
3.) Knowledge/skill map. Ensure that the required knowledge and skills are available within the organization and overlap individual employees in order to avoid gaps in case a key employee leaves or is absent on a long-term basis, etc.	H

The organizational needs with a high importance (H) prioritization, i.e., all of them, were also passed on to the next phase, planning action.

The high-level plan for action regarding technical and organizational change is outlined in Figure 2. Firstly, the responsibilities and ownership have been delimited at the firewall between the IT and OT networks. This clarifies organizational issues and improves the decision-making. Additional processes for enhanced interaction in between the IT and OT parts will also be set up, such as faster incident/problem management, general collaboration and change management. Further, the OT networks will be separated and segmented according to EU ENISA [13, 26] and national recommendations, using firewalls and other equipment, into smaller and independent networks. The individual OT networks, and the processes that run within these, will be independent of the functionality of the IT networks as well as other OT networks. The set-up of the smaller and segmented OT networks will be guided by the availability requirements, i.e., max downtime of 1/2/4/8/16 hours for the function provided by the specific OT network, which has impact on the level of redundancy of equipment, electricity backups and redundant outgoing communications connections, etc. For all essential functionalities, manual work-arounds will be documented and implemented in case the ordinary processes break down for any reason. Further, all communications outside of the OT network firewalls are encrypted and the networks outside of an OT firewall are considered as hostile. Authentication, access control and authorization will continue to be used in the OT networks; however, in some cases, with more advanced authentication methods and stricter access rights depending on the user's role and work descriptions.

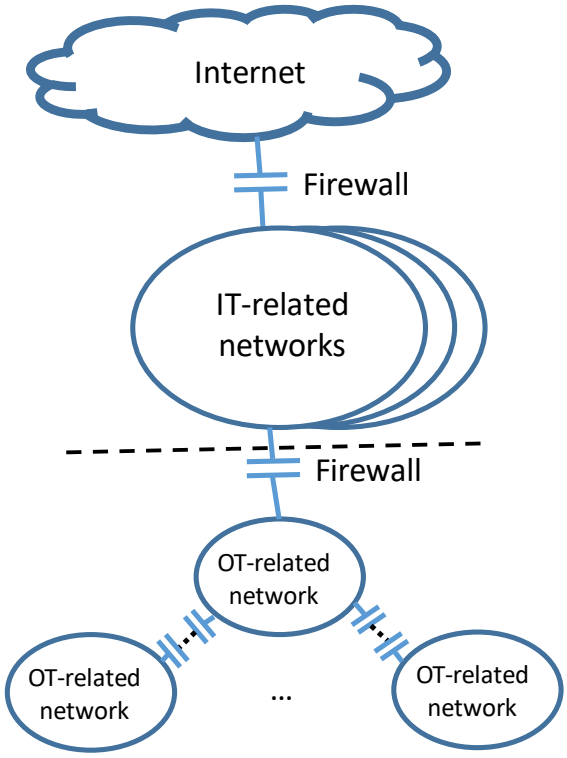

Fig. 2. High-level plan for action regarding technical and organizational change within the IT/OT networks.

Further, an OT policy was crafted in order to collect all essential OT-related requirements and operative and management needs into a policy document in order to: (1) highlight the OT area and its importance on top management level, (2) get a condensed collection of rules for management and operations within the OT area and (3) ensure an adequate cybersecurity level including all sub-matters which that encompasses. Further, some key objects in the OT networks will get improved monitoring. The initial OT policy crafted must first be accepted and decided upon by top management and the governing board of the municipality, and then later on gradually be refined as it is used and new matters are dealt with.

Thus, the plan for action (Figure 2) will make the municipal OT additionally robust, secure and have independent sub-networks that will continue to provide their functionality, even in the event of problems elsewhere in the IT or OT networks.

4.1 Analysis and evaluation

Concerning Table 1, the change needs with high importance, #1, 3, 4, 5, 8, 9, 10 and 13, are all part of the high-level plan in Figure 2 (although #3, 4, 8, 9, 10 and 13 are not all clearly visible in Figure 2). The change needs with medium importance, #2, 6, 7, 11 and 12, will be addressed later on. However, #2 and 11 are already being incrementally addressed.

Regarding Table 2 all change needs were selected and will be dealt with. The change need #1, responsibilities and ownership, is clearly outlined as the dashed border in Figure 2. Change needs #2 and #3 will be managed as part of planned/ongoing administrative improvements.

Pertaining to Figure 2, according to the plan for action, the OT parts will undergo significant changes and some of the changes have already been made. Thus, the action research effort has already resulted in actual changes. The changes are further outlined below (and also discussed in the discussion and conclusions section).

Finally, the evaluation of the design criteria is summarized below:

- **The first design criterion** - a clear and rational division of responsibilities and where the IT and OT environments should be separated has been planned (see dashed line in Figure 2) and started to be implemented. Further, during the evaluation interview the question "Is an OT policy needed?" was posed. The answer was: "yes" in order to "complement the organization's IT policy and IT-related guidelines". Consequently, an OT policy and OT-related guidelines were crafted to set up and clarify the long-term management, responsibilities, authorizations and rules of usage for the OT parts over their lifecycles.
- **The second design criterion** – to achieve an improved, affordable and maintainable cybersecurity level for the OT environment – will be met. However, to be fully implemented, some of the changes may require one or more action research cycles. Further, the questions "Did it improve?" was also answered with a "yes" through "improved risk management (i.e., risk-based) and further robust/resilient and flexible infrastructure".

5. Discussion and conclusions

The paper contributes to the literature by introducing the concept of an OT policy as well as outlining the benefits of, and reasons for, having an OT policy that complements the IT policy. The OT policy can be seen as a way to increase the awareness of and manage many of the risks, issues and problems brought up in for instance [1-2, 7-11, 14-18]. It is quite common that the OT part is equally large as the IT part or even larger, more complex and expensive – which requires a firm long-term management over the lifecycles with clear responsibilities and authorizations. Further, the paper contributes to practice by providing a number of technical and organizational change needs that are likely similar in many other organizations with production or operation environments that have OT networks. The OT networks will become even more robust from separation and segmentation, as they will become smaller and less complex, and it will be easier to find and faster to fix problems as they occur compared to in larger networks. The managerial contribution of the paper is a case that can be analyzed and learnt from, that an OT policy can provide a good managerial tool and also highlight the importance of the OT area on top-management and risk-management levels.

The research has resulted in changes (see Figure 2), which is one of the main objectives of an action research effort. However, some of the changes may need one or more action research cycles to be fully implemented and taken up by the organization.

Both the first criterion and the second criterion were deemed to be met. However, to be fully implemented, some of the changes required may take one or more action research cycles.

Concerning future research, project proposals to improve the extent and generalizability of the OT policy have been initiated and will also include an evaluation with other industries and their problems and risks.

The results outlined in the paper can be useful for organizations working in IT and OT environments, aiding optimization and improvement of the management of the respective environment through the lifecycles. Further, the proposed clarification of responsibilities and ownership is key for long-term through-lifecycle management.

Finally, efforts like the one described in this paper are necessary for many manufacturing and process industry companies as well as public-sector organizations, such as infrastructure providers and municipalities, in order to achieve an adequate level of cybersecurity for their OT environments and to clarify the line of ownership and responsibility between the IT and the OT. This is well aligned with EU ENISA's problem description [15, 28], where it is stated that "*recent deliberate disruptions of critical automation systems prove that cyberattacks have a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences for the EU Member States' governments and social wellbeing. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level*".

Acknowledgements

The research has been partly funded by the Swedish Innovation Agency Vinnova's VinnVäxt Centre, ProcessIT Innovations, at Luleå University of Technology, Sweden. The authors would like to thank all participants and respondents for their time and valuable input.

References

[1] Hahn A. (2016). Operational Technology and Information Technology in Industrial Control Systems. In: Colbert E., Kott A. (eds) Cyber-security of SCADA and Other Industrial Control Systems. Advances in Information Security, Vol. 66. Springer, Cham, Switzerland.

[2] Piggin, R. (2014). Industrial systems: Cyber-security's new battlefront, Engineering & Technology, Septemtber, 2014.

[3] Mont, O. (2001). Introducing and developing a Product-Service System (PSS) concept in Sweden, The International Institute for Industrial Environmental Economics (IIIEE), Lund University, Sweden.

[4] Meier, H., Roy, R. and Seliger, G. (2008). Industrial Product-Service Systems – IPS2, CIRP Annals Manufacturing Technology 2008, pp1-24.

[5] Alonso-Rasgado, T., Thompson, G. and Elfstrom, B-O. (2004). The design of functional (total care) products, Journal of Engineering Design, Vol. 15, No. 6, pp515-540.

[6] Lindström, J., Sas, D., Lideskog, H., Löfstrand, M. and Karlsson, L. (2015). Defining 'Functional Products' through their constituents, International Journal of Product Development, Vol. 20, No. 1, pp1-24.

[7] Lee, J., Kao, H-A. and Yang, S. (2014). Service innovation and smart analytics for Industry 4.0 and big data environment, Procedia CIRP 16, pp3-8.
[8] Cassady, R., Bowden, R. O., Liew, L. and Pohl, E. A. (2000). Combining preventive maintenance and statistical process control: a preliminary investigation, IIE Transactions, Vol. 32, Iss. 6, pp471-478.
[9] Lee, J., Ni, J., Djurdjanivic, D., Qiu, H. and Liao, H. (2006). Intelligent prognostic tools and e-maintenance, Computers in Industry, 57, pp476-489.
[10] Deloux, E., Castanier, B. and Bérenguer, C. (2009). Predctive maintenance policy for a gradually deteriorating system subject to stress, Reliability Engineering and System Safety, 94, pp418-431.
[11] Lindström, J., Kyösti, P., and Delsing, J. (2018). European roadmap for industrial process automation. Luleå, Sweden. Available at: www.processit.eu/roadmap. Last accessed on 15-Oct-2018.
[12] Lindström, J., Jonsson, M., Larsson, H., and Lejon, E. (2017). Towards intelligent and sustainable production : combining and integrating online predictive maintenance and continuous quality control. Procedia CIRP, 63, pp443–448.
[13] Choudhary, A. K., Harding, J. A. and Tiwari, M. K. (2009). Data mining in manufacturing: a review based on the kind of knowledge, Journal of Intelligent Manufacturing, 20, pp501-521.
[14] EU (2018). The Directive on security of network and information systems (NIS Directive). Available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive Last accessed: 15-Oct-2018.
[15] EU ENISA (2017). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, available at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot Last accessed: 15-Oct-2018.
[16] (eds) Delsing, J. (2017). IoT Automation – Arrowhead Framework, CRC Press, Boca Raton, FL, USA.
[17] Löfstrand, M., Andrews, J., Karlberg, M. and Karlsson, L. (2011). Functional Product system availability: simulation driven design and operation through coupled multi-objective optimization, International Journal of Product Development, Vol. 13, No. 2, pp119-131.
[18] Löfstrand, M., Backe, B., Kyösti, P., Lindström, J. and Reed, S. (2012). A model for predicting and monitoring industrial system availability, International Journal of Product Development, Vol. 16, No. 2, pp140-157.
[19] Reason, P. & Bradbury, H. (Eds.) (2001). Handbook of action research: Participative inquiry and practice, Sage Publications, London, UK.
[20] Gummesson, E., (2000). Qualitative Methods in Management Research, 2nd Ed. Sage Publications, Thousand Oaks, CA, USA.
[21] Coghlan, D., Coughlan, P. and Brennan, L. (2004). Organizing for research and action: Implementing action research networks, Systemic Practice and Action Research, 17(1), pp37–49.
[22] Remenyi, D. (2013). Field methods for academic research: Interviews, focus groups & questionnaires in business and management studies, 3rd edition, Academic Conferences and Publishing International Limited, Reading, UK.
[23] Patton, M. Q. (1990). Qualitative evaluation and research methods, Sage Publications, London, UK.
[24] Kvale, S. and Brinkmann, S. (2009). InterViews: learning the craft of qualitative research interviewing, Sage Publications, LA, USA.
[25] Fontana, A. and Frey, J. (1994). Interviewing, in (eds) Denzin, N. and Lincoln, Y., Handbook of qualitative research, Sage Publications, Thousand Oaks, CA, USA.
[26] Miles, M. and Huberman, M. (1994). An expanded sourcebook – Qualitative Data Analysis, 2nd ed, Sage Publications, Thousand Oaks, CA, USA.
[27] ISA-95 (2018). ISA-95 standard., available at: www.isa-95.com Last accessed: 15-Oct-2018.
[28] EU ENISA (2018). Recommendations for critical infrastructure and services. Avaialble at: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services Last accessed: 15-Oct-2018.