The use of network models in the inspection of objects of industrial installations.

Jarosław Napiórkowski[1,*]

[1] Faculty of Cybernetics, Military University of Technology (WAT), Gen. Witolda Urbanowicza 2 Str., 00-908 Warsaw, Poland

Abstract. Today's industrial installations consist of many interconnected elements. The source of a threat or failure of an installation can be not only damage to a single element (device), but also the interaction between individual elements of such a system. In order for the installation to meet safety requirements, the risk of failure should be properly assessed and appropriate prevention systems should be selected and the effects of its occurrence reduced. In order to achieve this, many care for the safety of such structures, inspection organizations carry out risk analysis and risk assessment with various methods. Due to the large number of elements that comprise installations of this class, the problem is to find cleary, uncomplicated and easy to implemented (cheap and low time-consuming) way to identify the relationship between its various elements. Possibility of specify and visualize relationships between elements of installations, their vulnerabilities, safeguards and the effects of threats is an unquestionable advantage of the network models in case of risk assessment carried out on a model built in this way. They allow network analysis based on centrality analysis. Relatively simple method of analysis of these networks. This article discusses few from many areas of application the network model in risk analysis in technical structures.

1 Introduction

Failures of technological systems in industrial plants or incorrect operation of operational processes carried out in them may pose a potential threat to people, cause costly damage and at the same time have an adverse effect on the environment. In the face of the increasing demands of governments and public authorities regarding security as well as pressure from competitors, owners and operators require effective solutions to identify threats, increase safety and availability of installations and reduce maintenance costs. Therefore, owners and operators of industrial plants need a systematic approach to identify potential threats. It requires to provide inspection, testing and risk analysis [1] services in an area covering various fields of activity.

Examples of such areas are: technical installations (power plants, wind turbines, oil and gas platforms), pressure equipment, machines, lifts and cranes. Each of the given examples consists of many connected elements. The source of danger or failure of the installation can be not only damage to a single element of the installation or device, but also the interaction between individual elements of such a system.

A good and simply way to identify all elements (assets) of the technical structure is construct of a network model of technical infrastructure. In the same way we could identify known threats, vulnerabilities and safeguards. This process should begin with the development of a methodology for the production of a network model of the examined technical structure, which will result in each expert product the same graphical image of the examined technical structure. As a result, we obtain a graphic form of the model examined structure with each node environment analysis. Collecting all data in one model gives us a lot of possibilities to use them [2],[3].

A reference model illustrating such an approach is presented in Figure 1.

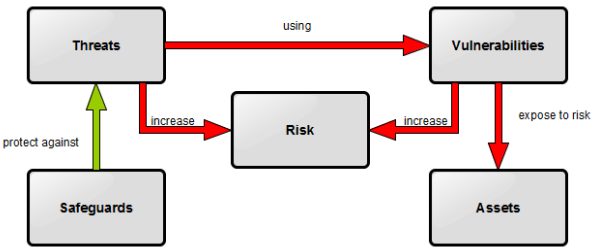

Fig. 1. Network reference model. Source: own elaboration.

This model is an extension presented in previous article [4]. New elements (edges in this graph) are safeguards and risk. These are the elements whose identification allows to build such an industrial installation model that will meet the imposed safety requirements. To this end, the risk of failure should be properly assessed and appropriate systems should be selected to prevent and reduce its effects, called security layers. In the case of installations used in the chemical, petrochemical, refining, or energetic industries, it is also important (for their owners) to reduce the costs associated with the unavailability of the installation.

* Corresponding author: jaroslaw.napiorkowski@wat.edu.pl

One of the reasons for unavailability may be the need to carry out an inspection. As inspection is understood as a systematic procedure used to assess equipment technical conditions. A helpful tool in this case is the planning of inspections based on risk analysis - Risk Based Inspection (RBI) [5],[6]. The RBI method defines the risk of operating equipment as the combination of two separate terms: the likelihood of an undetected failure and the consequence of such a failure. The answers to such questions can give the characteristics of the network model of the constructed technical plant.

2. Areas of application

In relation to industrial installations and operational technology (OT), other requirements are imposed than, for example, IT systems. While in the latter case the most important attribute of security is confidentiality and integrity, in the case of technical installations the most important is the availability [9] and safety of people and the environment.

This is the reason why there is a significant difference in the goals of ensuring security/safety.

Security has its roots in protection against theft. Today, the field covers many areas, from personal to national security, including financial crime, information protection, burglary and espionage. Security refers to those problems in which people take intentional actions to achieve a profit or a desire to cause damage.

At it's simplest, safety means protection from accidents. Safety is related to the health and well-being of people at work and in other activities.

In the current industry one can clearly see the trend regarding process safety existing in western countries, where the term "Safety first" is the main slogan of the activity of most chemical, petrochemical and refinery plants.

For this reason, the owners' goals or those that make industrial establishments define the tasks of maintenance services as:
- maintenance of the entire infrastructure (technological and auxiliary installations),
- renovation and modernization of technological installations,
- renovation of equipment and machines,
- renovation and regulation of safety valves.

This is confirmed by the fact that over the last dozen or so years, the industry has been gradually aiming at the transition from the previously used system of preventive and planned repairs, depending on rigid deadlines, on systems based on the current technical condition of the equipment. The basis for such activities was firstly starting, and later, improving, the methods for diagnosing the actual state of the devices.

2.1. HAZOP (Hazard and Operability Studies)

One of the techniques supporting such an approach to safety is the HAZOP analysis, which is aimed at identifying all potential threats and losses that may occur in plants. The analysis of threats and operational abilities is a structural method of identifying potential threats occurring in industrial processes. HAZOP is a common method of hazard analysis for complex systems. The basic steps in this analysis:
- forming a HAZOP team,
- identifying the elements of the system,
- considering possible variations in operating parameters,
- identifying any hazards or failure points,

HAZOP is a structured and systematic technique of testing a specific system in order to identify potential threats in the system and potential problems related to the system's ability to operate and in particular to identify the causes of disruptions and production deviations that may lead to non-compliant products. The HAZOP method is an analysis of threats and operational abilities used to assess process risk.

HAZOP analysis starts with the division of the system into nodes for which a set of physical parameters is determined, such as: flow, temperature, pressure, level, etc. The combination of parameters with the relevant keywords enables a concrete interpretation of the deviation from the design assumptions. The HAZOP analysis consists in considering all possible connections "parameter - keyword" and examining the possibility of deviations suggested by the interpretation of pairs (parameter, key word). For each deviation, the causes are identified, the probability of deviation is determined and the threats caused by them are determined. It also assesses whether the applied hardware and procedural safeguards are sufficient in relation to the effects caused by unwanted events and, if necessary, make its own recommendations.

The results of the analysis are recorded in the so-called HAZOP table, which contains information about considered nodes (connection, parameter, key word, interpretation). For each irregularity detected, the fields concerning the causes, consequences and remarks and doubts to be clarified shall be completed.

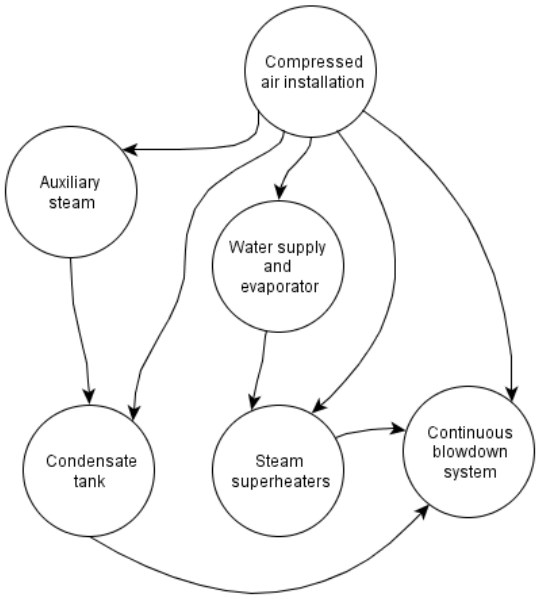

Fig. 2. Information flow graph (water and steam part of the boiler)- example from HAZOP analysis. Source: own elaboration.

The method is recommended especially when designing new buildings, when the project is well documented (there are P & ID schemes) and when modernizing existing installations, processes or facilities. It can be used to identify problems at an early stage of the project, but it does not limit its use to identify potential threats in existing systems.

2.2. RBI (Risk Based Inspection)

Another need expressed by managers of plants is the desire to minimize the downtime of industrial installations, regardless of their causes (shutdowns, breakdowns, repairs, etc.).

The answer to this need is a comprehensive risk management system for the operation of equipment that allows predicting when the device may fail.

The Risk Based Inspection (RBI) methodology is helpful here - methods of planning inspections and preventive tests of facilities / installations, which helps organizations select cost-effective and appropriate maintenance and inspection tasks and techniques, minimize to efforts and costs, to shift from a reactive to a proactive maintenance regime, create an audit system to obtain a agreed operational window, and implement a risk management tool

The Risk Based Inspection (RBI) methodology for planning pressure equipment inspection is based on the American Petroleum Institute (API) API Recommended Practice 580 Risk Based Inspection and the API Recommended Practice 581 Risk-Based Inspection Methodology, in which it is defined as the process of risk assessment and risk management. The risk is defined as the product of the probability of an event occurring due to degradation of the material, consisting in the unsealing of the pressure shell and the consequences it causes. RBI analyzes are conducted individually for each of the pressure devices, i.e. tanks, process furnaces and technological pipelines, and are aimed at determining:

- probability of device damage caused by the impact of material degradation mechanisms, which depend on from the current technical condition, type of construction material, physical and chemical properties of the working medium, operating parameters and the influence of external factors on the device,
- consequences caused by damage to the device, which depends, among from the design and size of the device (e.g. capacity), its location and the physical and chemical properties of the working medium.

For example, the greatest benefits from the full implementation of RBI in one of the largest oil company in Poland dealing in crude oil extraction and processing as well as wholesale and retail sales of petroleum products are:

- greater reliability of installation work,
- the period of continuous refinery operation between maintenance shutdowns should be extended from 4 to 5 years,
- multi-million savings related to avoiding breakdowns,
- bigger production.

In this organization RBI analysis about 8.5 thousand. devices and finding out which ones are most vulnerable to damage. By focusing research on specific devices, we reduce the risk of failure.

As you can see, gathering data about devices and operating conditions is important in each of the above cases. This data can be presented as a graph.

2.3. Piping and instrumentation diagram (P&ID)

A piping and instrumentation diagram, or P&ID, shows the piping and related components of a physical process flow. They are a schematic illustration of the functional relationship of piping, instrumentation and system equipment components used in the field of instrumentation and control or automation.

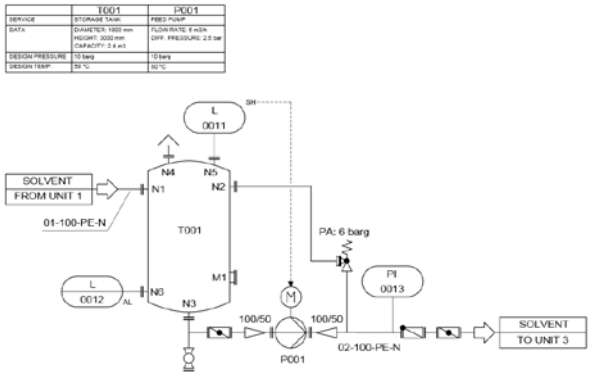

Fig. 3. Piping and instrumentation diagram of pump with storage tank piping symbols according to EN ISO 10628 instruments according to EN 62424. [10]

Each of the elements in the above drawing and relations between them can be presented as a graph.

3 Identification of network nodes

Complete knowledge of all elements of technical infrastructure and the interrelationship between its elements is one of the key activities related to the management of an industrial installation. This is not an easy task to accomplish. Each installation consists of hundreds of elements and thousands of interdependencies. Each of them must be uniquely identified [7, 8]. It is not an easy task to inventory them. In proposed model we have four types of nodes representing:

- assets/elements
- vulnerabilities
- threats
- safeguards

The element whose value we want to determine is the node representing the risk [11, 12].

The author's proposal is the methodology that is used for this purpose, allowing for simultaneous identification of resources of their vulnerability and their connections that enable them to give up threats.

Applying an approach based on such methodology will lead to the development of an algorithm describing

the process of identifying resources, vulnerabilities and threats in the desired context. Thanks to this, it was possible to build a network model corresponding to the actual state of the industrial installation.

The diagram presented in Figure 3 is a graphical representation of the proposed methodology.

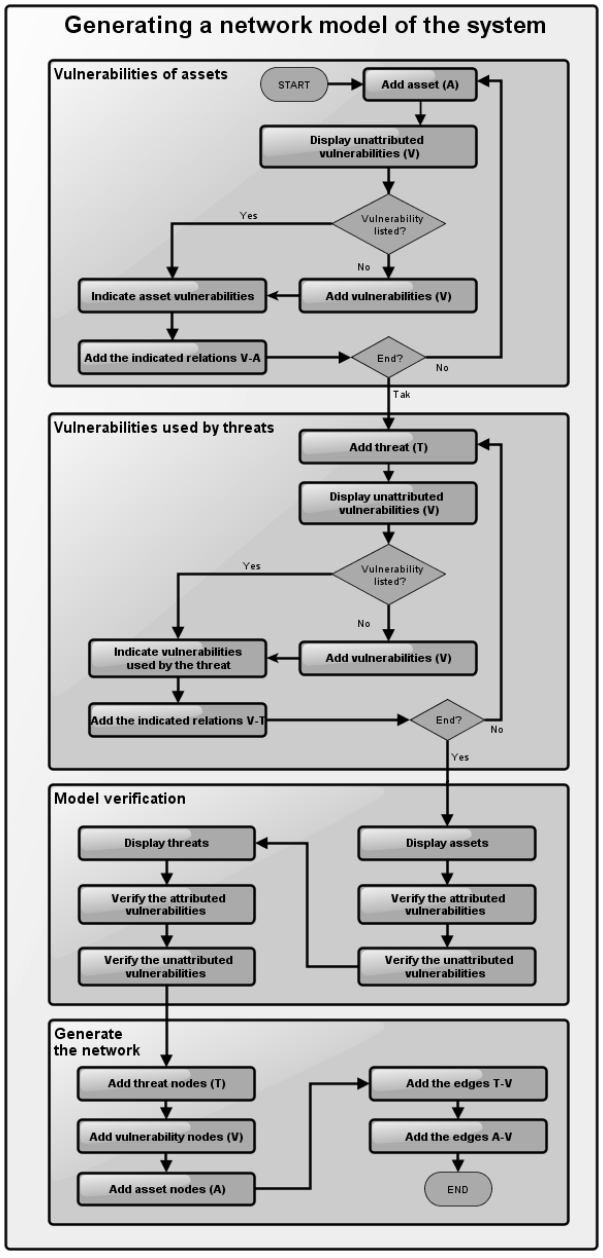

Fig. 4. Generation diagram of the network model. Source: [4].

The use of this model has led to the development of an algorithm that describes the process of identifying resources (e.g. from P&ID diagrams) and vulnerability (e.g degradation sites in RBI analysis) and threats (e.g. degradation mechanisms in RBI analysis) [13]. Having described the full installation model in the form of a graph, we can calculate typical characteristics computed for network nodes. A good methods for analysis of networks [14] are centrality measures like:

- degree centrality - simple centrality measure that counts how many neighbours a node has. It can be used to illustrate the popularity or influence of nodes. It is useful for determining which nodes are critical (key node) for spreading information or influencing nodes located in the immediate neighbours.
- closeness centrality - measure of centrality in a network, calculated as the sum of the length of the shortest paths between the node and all other nodes in the graph. This is therefore the expected distance between the node and any other node. Thus the more central a node is, the closer it is to all other nodes.
- betweenness centrality - ability of a node in the network to create connections with other nodes. A node with a higher value of this parameter than other nodes in the network is often called a hub.
- eigenvector centrality - importance of a node depends on the importance of its neighbours.
- radius centrality – if we need to find influential nodes in an area modelled by a network.

Especially important for us is degree centrality measure and in fact distribution of vertex degrees.

In a network with a power distribution of vertex degrees, many nodes have only one edge, but you can also find nodes with a huge number of edges, so-called hubs. This disproportion in an unusual way translates into the properties of scale-free networks and makes them very interesting research objects.

4 Conclusions and future work

Most of the technical installations can be presented as a network. Such representation has a wide range of applications (e.g. RBI, HAZOP) as well as in the registration of elements and their interrelations in such installations. In the case of industrial installations, the network generation process can be automated based on existing piping and instrumentation diagrams.

The article presents the use of graphs in applications related to the execution of hazard analysis and risk assessment [15]. It is a simple tool whose applications are very widely used. The same ability to calculate the characteristics of the network results in practical conclusions, different network configurations can be considered to identify its weaknesses (bottlenecks), search for alternatives that ensure its better functioning [16, 17].

In the course of further work, the author wants (based on example P&ID diagrams) to build network models several types of real installations and then compare the results of network analyzes based on centrality analysis (on various centrality measures like degree centrality, closeness centrality, betweenness centrality, radius centrality, eigenvector centrality) with the results of RBI and HAZOP analyzes performed on real industrial installations. The result of the comparison may be used to determine the centrality measures applicable to different types of installations and different hazard analysis or risk assessments. This will allow you to build a catalog of centrality measures that can be used in various areas of application. Depending on the results of this work may prove to be easier to use tool to perform technical expertise than the known methods of hazard analysis and risk assessment.

References

1. *PN-EN 31010:2010 Risk management - Risk assessment techniques*
2. M. Kiedrowicz, *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych*, Roczniki Kolegium Analiz Ekonomicznych, vol. **33**, pp. 209-234, (2014).
3. M. Kiedrowicz, *Generalized Data Model in Distributed Registers*, Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2017", 4-8 of September 2017, pp. 171-183, Trento–Vattaro, Italy (2017).
4. P. Adamczyk, G. Kiryk, J. Napiórkowski,. A. Walczak, Network model of security system. *MATEC Web of Conferences* **76**, 02002, DOI: 10.1051/matecconf/20167602002, (2016)
5. A.A. Mokhtar, M. Che Ismail, A. Bakar Zainordin, S. Shahid, *A Framework for Estimating Piping Reliability Subject to Corrosion Under Insulation. MATEC Web of Conferences* ***13*** *03001 (2014)*, DOI: 10.1051/matecconf/20141303001
6. H. Muhajir, G. Dwi Haryadi, A. Widodo, *Remaining Life Assessment of Superheater Tube in Boiler of Coal Fired Power Plant*. MATEC Web of Conferences **159**, 02041 (2018), DOI: 10.1051/matecconf/201815902041
7. M. Kiedrowicz, *Objects identification in the information models used by information systems*, Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2016", pp. 129-136, Perugia, Italy (2016).
8. J. Dudczak, *Podstawy analizy obiektów przemysłu chemicznego.* Wyd. Pol. Szczecińskiej, Szczecin (1987)
9. A.S. Markowski, *Zapobieganie stratom w przemyśle.* Cz. III. Wyd. Politechniki Łódzkiej, Łódź (2000)
10. https://commons.wikimedia.org/wiki/File:Pump_with_tank_pid_en.svg
11. M. Kiedrowicz, J. Stanik, *Models and Method for the Risk Assessment of an Intellectual Resource*, WSEAS Transactions on Information Science and Applications, vol. **14**, pp. 174-183 (2017)
12. M. Kiedrowicz, *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity,* MATEC Web of Conferences, vol. **125**, DOI: 10.1051/matecconf/201712502010, Greece (2017).
13. M. Kiedrowicz, *The importance of an integration platform within the organization*, Scientific Papers of the Maria Skłodowska-Curie Warsaw Academy, Quarterly, pp. 83-94, vol. 4 (46), Poland (2014).
14. B. Korzan, *Grafy, hipergrafy i sieci*, WAT, Warszawa, (1980)
15. M. Kiedrowicz, J. Stanik, *Selected aspects of risk management in respect of security of the document, lifecycle management system with multiple levels of sensitivity,* B. Kubiak, J. Maślankowski (eds.) Information Management in Practice, pp. 231-248, ISBN 978-83-64669-05-7, Poland (2015).
16. M. Kiedrowicz, T. Nowicki, R. Waszkowski, *Business Process Data Flow between Automated and Human Tasks*, Proceedings of the 3rd International Conference on Social Science (ICSS 2016), vol. **1**, ISBN: 978-1-60595-410-3, Shanghai, China (2016).
17. M. Kiedrowicz, R. Waszkowski, *Business rules automation standards in business process management systems,* B. Kubiak, J. Maślankowski (eds.) Information Management in Practice, pp. 187-199, ISBN 978-83-64669-05-7, Poland (2015)