



Artificial intelligence for a safety system

Jelenka Savković Stevanović

Faculty of Technology and Metallurgy, Belgrade University, Karnegijeva 4, 11000 Belgrade, Serbia.

DOI: 10.5281/zenodo.22824206

Submission Date: 26 July 2026 | Published Date: 18 Sept. 2026

Abstract

Scientific methods in process safety analysis means the gathering of information, the analysis of this information by suitable techniques, synthesis, and decision making, all utilizing a framework. In this paper an artificial intelligence algorithm for safety system developed. Framework definition includes all components, input and output attributes, state variables, behavior rules, and initial conditions. This trend will no doubt continue in the future as new methods are developed and as the available tools become more sophisticated. In this paper an artificial intelligence for a process plant safety system was built.

Keywords: Safety, artificial intelligence, algorithms, network, cause-event.

1. Introduction

Process safety analysis involves an examination of the overall process, alternative processes, safety and economics. If a wise choice is to be made, the cost of a project must be known and compared with the cost of other projects. In the same manner, the possible benefits of each alternative must be known in a fashion that will permit comparison. Cost estimates for various systems are vital not only because new system proposals are very expensive but also because there are so many systems competing for consideration.

Loss prevention is the goal of risk analysis. This issue helps readers will come across items of knowledge of process plant safety and loss prevention that inspire further application and consideration. They trust that the knowledge proves useful and its dissemination leads to further improvements in process plant safety systems analysis and development. Functional safety involves identifying specific hazardous failure which lead to serious consequences (death) and then establishing tolerable frequency targets for each mode of failure. Equipment whose failure contributes to each of these hazards is identified, and usually referred to as safety related.

Diagnosis means gathering information, formulating hypothesis and testing hypothesis with available data. Sometimes, it may need to be done several times if the hypothesis formulated turn out negative. The end of this process can make possible repair the fault.

Risk management in the standard is defined as the systematic applications of policies, procedures and practices to the tasks of identifying, analyzing, assessing, treating and monitoring risks.

Risk probability analysis, risk function and decision procedure were defined in failure system analysis. Qualitative information processing, concept safety modelling and applications are very important for process engineering management, diagnostic system for fault recognition and troubleshooting [1]-[3]. This part includes the theoretical and computational bases for proven techniques in diagnosis. The choice of a specific technique must mesh with the fault assessment, safety system and diagnostic method.

Because of the importance of failure system analysis, it is important to how to specify the three key components of a safety problem: fault assessment, qualitative and quantitative safety models and diagnosis. The study of risk and failure analysis by giving examples of different types of problems that may be encountered in process engineering is considered in these articles.

After discussing the essential features of every safety problem, varying degrees in solving a safety and reliability problem was provided. It is important that a potential user of process safety methods be able to translate a verbal description of the problem into the appropriate mathematical expression. It is also important for a user to understand how the problem formulation has a major impact on the case of problem solution [4]-[10].

Developing methods and tools for problem safety and reliability solving, very significant task for engineers, was studied in this paper.

2. Process safety system modelling and analysis

Process safety analysis begins with system definition. Definition includes system components, topology, input and output attributes, state variables, behavior rules and initial scenarios. Process safety analysis includes hazard identification, frequencies and probability analysis, consequence analysis and hazard cost analysis. Hazard identification methods can be used in different ways to model part of the incident scenario leading to a possible accident. In this paper cause-event dispersion modelling was studied.

Modelling method started with system, subsystem, elements, and their interrelations definition according to goal state [11]-[14]. It follows methods and procedures formulation for model development. Model establishing, solving, testing and applications is final phase of the safety system model building.

$$M_i = \sum_{i=1}^{n+m} f(\text{equipment, location, connections, supply, symptoms, fault}) \quad (1)$$

where n is number of basic elements, and m is number of subsystems.

The system topology or component interconnections are defined by the process connections of the working process model. The level of aggregation is defined by the modular component interconnections which define propagation paths of attributes within the system.

Initial research starting by phase of the development of a conceptual framework which facilitate the modular specification of models, and second phase the development of a logic framework which will permit object using attributes and simulation techniques to be linked into executable models.

Various rules in Artificial intelligence (AI) model can be applied to this system based on the transitivity relationships of the qualitative variable [15]-[17].

To organize the logic of the rules, states variables must be defined within the system AI. Three types of state variables can be defined within a given component. The first are those variables whose values can be controlled by the system operator. These are controllable variables. The second set of state variables are those variables whose values are observable to the system operator over the acquisition data system. Last are those variables whose values are not immediately discernible by the system operator such as attributes of inner state, and so on.

Scenarios are used to set initial states of the system state variables and attributes to predefined values prior to a model simulation run. This is necessary to evaluate “what if” scenarios concerning components.

3. Semantic network of causing faults

Knowledge bases represent knowledge using a system of “predicate function” and “symbolic data structures”. A function is a kind of procedure that is performed on certain input values, called arguments, and produces, or is associated with, a set admissible value.

A predicate is a function that evaluates to either true or false. For example, in the function (is equipment), “is” is predicate, and the function, which states that the equipment unit is in plant-subdivision, is either true or false.

A symbolic data structure that is used to represent symbolic knowledge and that can be stored. One symbolic knowledge representation structure is called a semantic network.

A semantic network is a node-and-arc graphical notation that represents objects for (action or events) and contain built – in real plant meaning, or semantics, about the objects (Fig. 1). The nodes represent the objects. They could also represent

actions or events. The arcs between the nodes represent predicates or attributes that indicate relationships between the objects (or action or events) shown in the nodes.

The semantic network shown in Fig.1 uses both predicates, such as “is” and “isa”, as well as attributes, such as faults, to represent objects in a plant subdivision and to show relationships between the objects. A trace of arcs that connect the nodes in this network shows that operator tend to be between plant and sensors table. This knowledge structure can infer information such as “a particular object can’t be a plant because plant is manufacturer”.

The semantic network also enables a knowledge system to infer information such as “a particular equipment connects with for example scrubber because, as shown, scrubber is the plant. With a semantic network representation, the knowledge system can also infer that “equipment 1 and equipment 2 are used for environment protection because, plant in general used for environment protection.

This type of inference is based on a principle called “inheritance”. Here “inheritance” means that since equipment 1 and equipment 2 are part of the plant, they inherit the characteristics of that plant.

Since the purpose of equipment 1 and equipment 2 is environment protection and their description is scrubber, both instances of equipment inherit the purpose of environment protection and the description of scrubber.

There are several other methods used to represent knowledge in a knowledge base. Besides semantic network, knowledge base system employs representation methods known as rules, frames, processes, logic, and script.

Despite knowledge representation difference, in general anything that one representation can do can be done by the others. Ultimately, a representation choice boils down to how the chooser thinks. About the knowledge in question and which representation method lends itself most efficiently to retrieval and deduction of facts.

The representation of knowledge it is one of the major problems in building a knowledge based system. It may take months to represent the relationships in a simple world such as plant division. How, then, can an expert represent the entire building? And once the knowledge has been represented, how is it possible to search it quickly and make inferences?

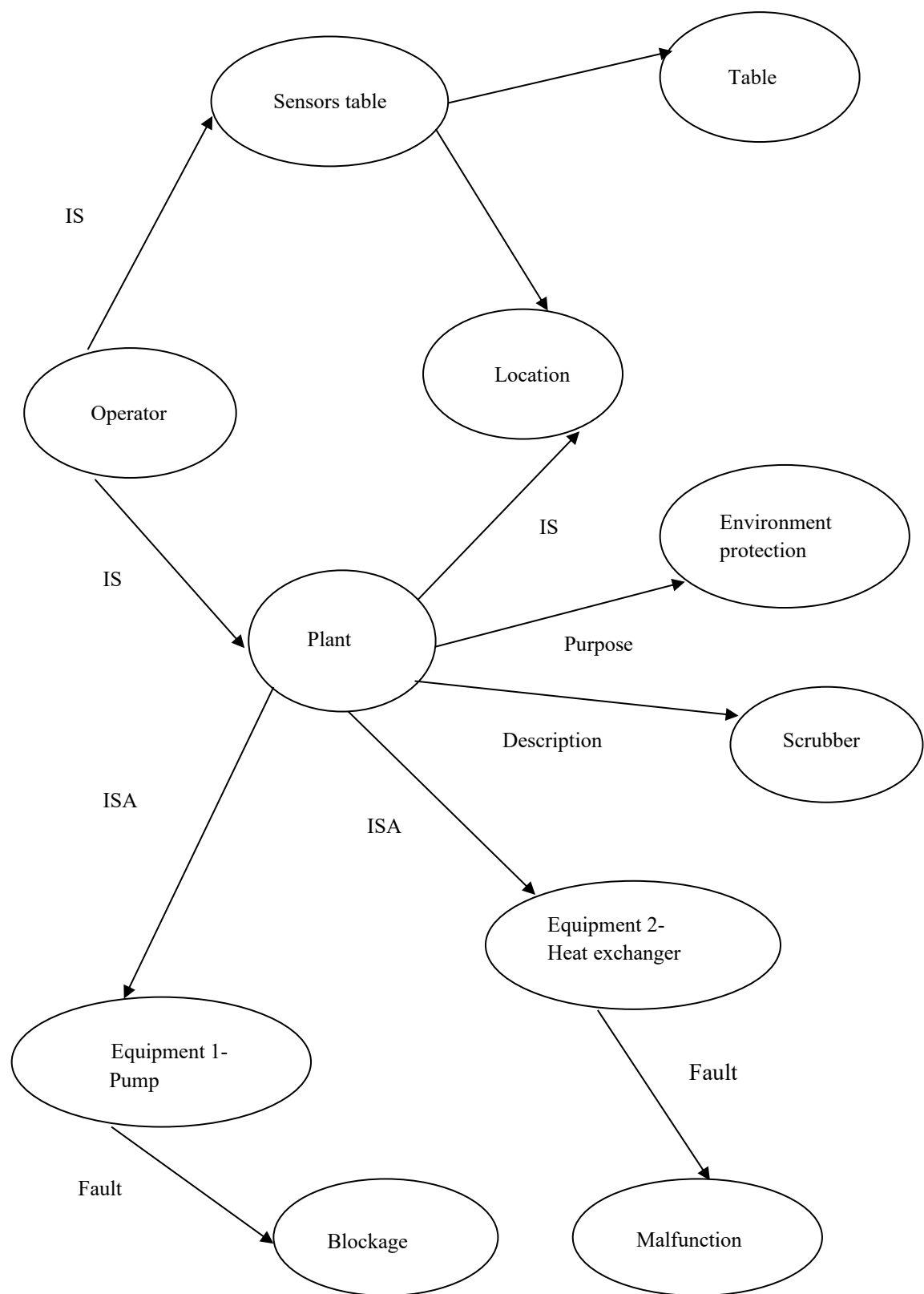


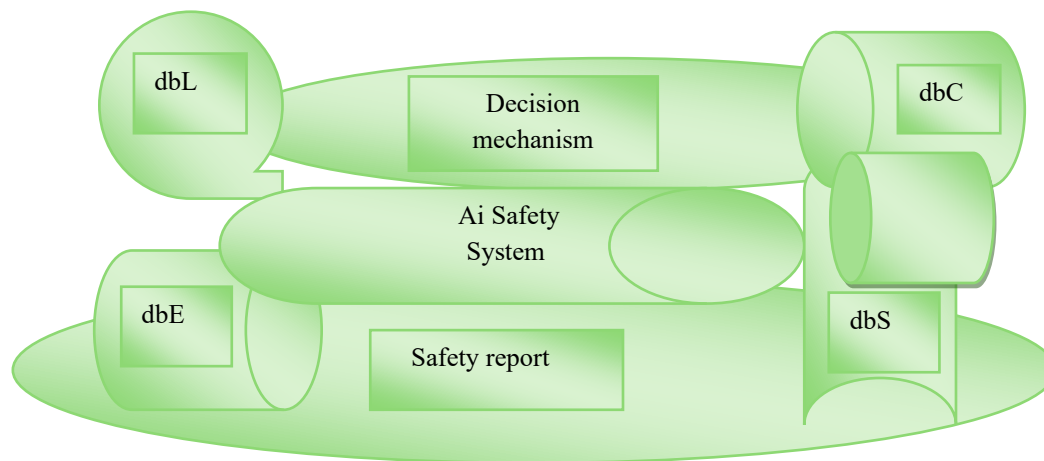
Fig. 1: Semantic network

Although there are many ways to represent knowledge, the most common form of knowledge representation is with “rules”. A rule is conditional statement that specifies an action to take place, or advice to follow, under a certain set of conditions. This *situation – action* or *symptom-cause* format of rules is particularly suitable for expressing knowledge that experts in the field have gained as a result of experience-their so called rules of thumb.

In some respect, rules are similar to the conditional “if-then” statements of conventional programming languages. If – then statements are statements of the form IF this is the case, THEN do that, or IF this happens, THEN do that, or even IF this is the case, THEN that is TRUE.

For example, IF equipment is a pump, THEN pump belongs the plant. Rules differ from conventional IF-THEN statements because of their extreme modularity. A set of rules is an unstructured group of IF-THEN statements that control themselves in terms of knowing when they should be applied to solve a problem.

Besides semantic network, failure system employs representation methods known as rules, frames, processes, logic, or script. In this paper semantic network and data base network about location, connections, environment and symptoms were examined. System safety and frequency analysis were considered (Fig.2).



dbL- Location data base, dbC- Conections data base, dbE- Environment data base, dbS Symptoms data base.

Fig. 2: A software AI safety system architecture

4. A systematic cause - event analysis

A systematic cause - consequence analysis gives the results which are summarized in the form of a cause-event tree model. It follows the structure of a generic fault tree point to the release of materials, chemicals and, of an event tree from this point to the impact of the release on people, the plant and the environment [6]-[11]. Frequency and probability analysis involves frequency values of hazard, magnitude identification of each hazard and develop a sound criterion for quantification of logic tree. All hazard, major and minor need to involve. The relationship between hazard and risk must be defined. Consequence modelling develops troubleshooting system and formalizing hazard reporting as a learning tool and creates recommendation to correct hazard through a cause- feedback algorithm.

So many accidents have been caused by operator’s miss judgments or miss operations, there is a need to develop a system which can also suggest appropriate action to be taken when a hazard occurs.

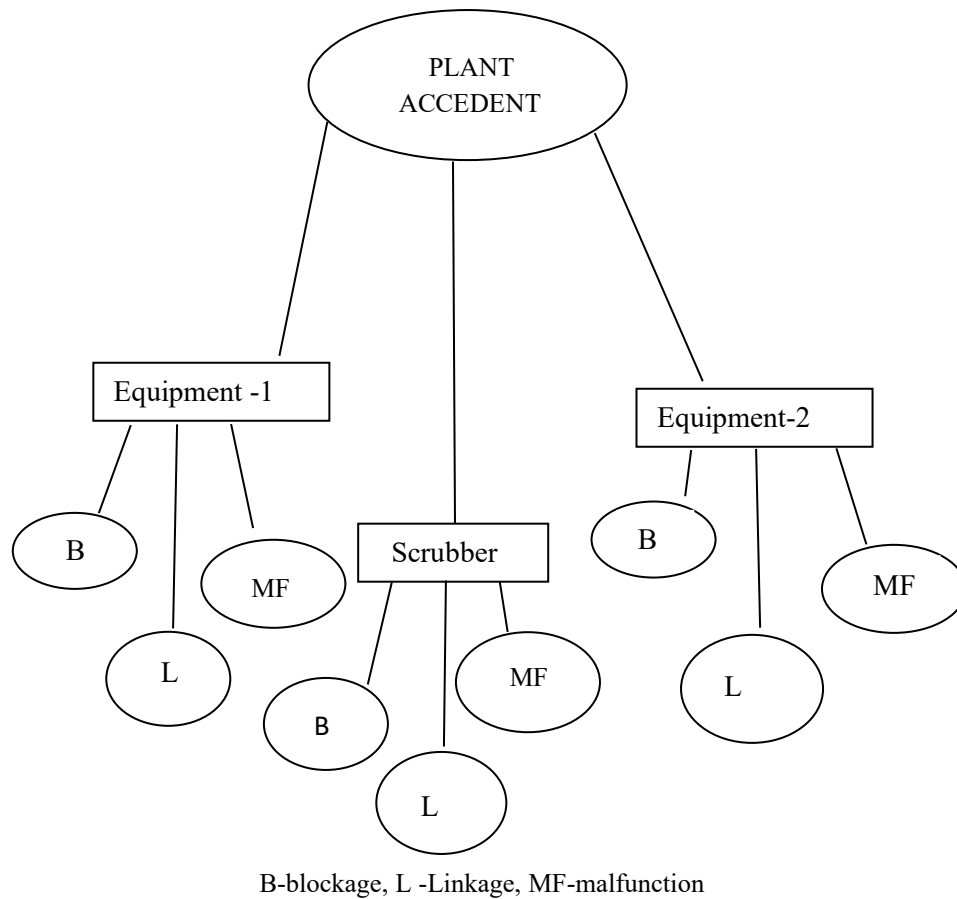


Fig. 3: Fault tree for some questions

The question of what is the best and most useful method to represent knowledge is still an open question in the risk diagnosis. Although rules, frames, processes, and combination of these, are common ways to represent knowledge, they are by no means the only ones.

Yet another common way to represent the type of knowledge generally used in everyday language, as well as much of modern mathematics, is formal logic. Formal logic is a technique to represent information so that it is possible to check formally whether or not the information is true. For example, whether or not symptom is a leakage can be represented in logic as the statement (known in logic as proposition):

5. Symptom (flooding)

Flooding is the “argument” of the statement. The statement evaluates either to true or false.

Predicates in logic express relations between objects. For example, occurs (flooding, top-scrubber) uses the predicate “occurs” to represent the fact the flooding occurs in the top of the scrubber.

The logic system used in diagnostic systems is known as predicate calculus. Typical predicates to these systems might be “works in”, “isa” or “earns”. The predicates are defined whereas logical connectives such as AND, NOT, and IF, which are also part of logic, are predefined by the logic system. It is possible to build an entire knowledge base or relational database using formal logic.

Basic facts about and relationships between equipment, faults, and plant symptom information are entered in a manner similar to that previously shown regarding flooding. Unlike database, it is not necessary to store the same amount of information or type of information for each person or item in a database based on logic.

6. Consequence analysis

A representative set of events needs to be established where quantification of risk is required. The set needs to contain sufficient members to ensure both the worst case events are included, and lesser, more frequent events are suitably represented. This will enable the effects of existing and postulated risk reduction measures to be considered. Separate events are generally necessary to incorporate the conditional probabilities of success and failure of protective systems.

The consequences of the events are modeled and the frequencies and probabilities of all significant events allocated. Sensitivity analysis and further refinement of the representative set may be needed to ensure that the set is sufficiently descriptive, robust and fit for the purpose.

The type and extent of assessment need to be no more than fit for purpose, that is proportionate to the scale of the risks with particular emphasis on the potential consequences. Likewise, the measures taken to control a risk also need to be proportionate. Proportionality is a measure of the concern that is appropriate for an installation and the cause of risk within that installation. The individual risk of death to workers in the chemical and allied industries is generally low. For hazardous installation subject to the regulations social concerns, and specifically social risk, are therefore the main determinants of proportionality. For this purpose, the possible consequences of an incident are given more prominence than the likelihood.

The options for reducing risk in most situations are limited, and the optimum option is likely to have been established as good practice and may be documented. However, such documents may only address some of the risks that need consideration. A complete statement of good practice may not be available, particularly where major investment decision is needed or hazards are regulated through safety case regimes. Current practice cannot be assumed to be sufficient for the control of major accidents.

7. List of all major accidents

The scope of the assessment should be clearly stated all safety reports. The criteria for making decisions based on the risk to people need to be clear. Relevant good practice needs to be described including the identification of recognized codes, standards and guidance and any appropriate, in house, company standards. Detailed hazard studies carried out at the design stage provide a good base for this.

The methodology and process adopted for hazard identification needs to be described. An analysis of known incidents both within the company and beyond is usefully undertaken using collected data. A list of all major accidents with a summary of initiating events is produced.

For each type of major accident, the extent and severity are described. The effects of variations in ambient conditions are considered. The consequences in terms of the numbers of persons who may be affected both on and off site are needed both for subsequent decision making and emergency planning. Control and mitigation systems are identified. The likelihoods of the consequences are described taking into account the probability that protective systems will not function on demand.

8. Discussion

1. Process safety system modelling and analysis is deriving.
2. Artificial intelligence for a safety system construction and operation was developed.
3. The knowledge and rules found in knowledge base of semantic network include data.
4. The systematic cause-event fault tree was illustrated.
5. The path of decision making for troubleshooting has shown.

9. Conclusion

In this article a model for AI safety system building was made. Artificial intelligence architecture in knowledge bases and data bases environment has developed. Cause-event tree was described and developed.

A systematic cause - consequence analysis gives the results which are summarized in the form of a cause-fault tree model. The consequence analysis was discussed.

Safety report was discussed.

References

1. Savković Stevanović, J. (2022). *Artificial Intelligence in Chemical Engineering Practice*. LAP-Lambert Academic Publishing. ISBN 978-6-20551509-9. Available at: www.lap-publishing.com and www.amazon.com.
2. Savković Stevanović, J. (1999). *Process Engineering Intelligent Systems*. 1st ed. Memphis, USA: RAJ Publishing, 1999. 2nd ed. Belgrade, Serbia: Srbisim Publishing, 2008. ISBN 978-86-911011-1-4.
3. Savković Stevanović, J. (2025). Artificial intelligence for diagnostic system constructs. *Journal of Global Research Engineering and Computer Science*, 5(2), 88–95. ISSN 2583-3960. <https://doi.org/10.5281/zenodo.12689400>
4. Savković Stevanović, J. (2010). An advanced learning and discovering system. *Transactions on Information Science and Applications*, 7(7), 1005–1014. ISSN 1790-0832.
5. Savković Stevanović, J. (1988). Expert systems. In *IES1988—2nd Information and Expert Systems in the Process Industries*, Belgrade, Serbia, 27–29 October, pp. 48–68.
6. Savković Stevanović, J. (2009). Information and knowledge representation. *Computer Ecology and Engineering*, 5(1), 35–40. ISSN 1452-0729.

7. O'Connor, Dennis E. (1983). *Using Expert Systems to Manage Change and Complexity in Manufacturing*. Digital Equipment Corporation, April 1983.
8. Savković Stevanović, J. (2009). Decision support system extraction. In *11th WSEAS International Conference on Mathematical and Computational Methods in Science and Engineering (MACMSE09)*, ID 639-126, pp. 44–49. Morgan State University, Baltimore, USA, November 7–9, 2009.
9. Savković Stevanović, J. (2011). Simulation in the knowledge base and database network. In *AIKED11—International Conference on Artificial Intelligence, Knowledge, Engineering and Databases*, ID 650-650, Cambridge, London, February 20–22, 2011.
10. Savković Stevanović, J. (2010). A knowledgeable intelligent system. In *AIKED10—International Conference on Artificial Intelligence, Knowledge, Engineering and Databases*, Cambridge, London, February 20–22, 2010, p. 6.
11. Cynar, L. (1986). Expert systems solve network problems and share the information. *Data Communications*, May, pp. 187–192.
12. Savković Stevanović, J. (2009). Information and knowledge representation. *Computers, Environment and Urban Systems*, 5(1), 35–40. ISSN 1452-0729.
13. Savković Stevanović, J. (2009). Knowledge extraction and concept learning. *Computers, Ecology and Engineering Quarterly*, 5(1), 22–28. ISSN 1452-0729.
14. Savković Stevanović, J. (2007). *Informatics*. Faculty of Technology and Metallurgy, University of Belgrade, Serbia. (In Serbian). ISBN 978-86-7401-244-4.
15. Savković Stevanović, J. (2017). Logistic system communication. *Computers, Ecology and Engineering Quarterly*, 13(1), 28–33. ISSN 1452-0729.
16. Savković Stevanović, J. (2025). Artificial intelligence models for knowledge producing. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, 10(2), 641–650. ISSN 2454-6194.
17. Savković Stevanović, J. (2025). Artificial intelligence for product formation. *Journal of Global Research Engineering and Computer Science*, 5(2). ISSN 2583-3960. <https://doi.org/10.5281/zenodo.12689400>

CITATION

Savković Stevanović, J. (2026). Artificial intelligence for a safety system. *Global Journal of Research in Engineering & Computer Sciences*, 6(5), 26–33. <https://doi.org/10.5281/zenodo.22824206>