Journal of Mechanical Science and Engineering 8(1) 19-22, 2021
ISSN 2354-9467 

# AN OVERVIEW OF THE DEVELOPMENT OF SAFETY SYSTEMS IN INDUSTRIAL CONTROL SYSTEMS

Aditya Reza Haswendra[1*]

[1]Department of Mechanical Engineering, Faculty of Engineering, Universitas Sriwijaya, South Sumatera, Indonesia

## ABSTRACT

Industrial machines can be very hazardous to human life, even automated ones. There are many regulations, laws, and technical approaches implemented to reduce the risks they can pose to people, especially industrial workers, and operators during maintenance or when direct intervention by people is required. With the industrial climate nowadays, which pushes for more and more safety for the workers, development in safety features of industrial control system has been increasing steadily. This paper analyzes some of the newest iterations of those safety systems and how they may influence the industrial field.

Keywords: Safety, Industrial Control System, Factory

## 1 LATEST DEVELOPMENTS OF SAFETY FEATURES IN INDUSTRIAL CONTROL SYSTEMS

Machine safety is crucial in industrial automation[1]. Safety-related control systems and functional safety offer manufacturers flexibility and a way of improving competitiveness as well as productivity. Safety becomes an integral part of the functionality rather than a required constraint to meet regulations and standards[2]. Risk in the industry is increasing over time because of the continuous shift from smaller to bigger and even bigger operations. From a small single production and batch operations to continuous large operations. Larger operations bring bigger risk in the case an accident happens. The consequences may include loss of life or injuries to workers, process shut down, environmental damages, and monetary losses[3].

A good industrial safety system can help mitigate this problem. For instance, collaborative robotic systems provide a good example illustrating the importance of safe control systems. These robots are purposely designed to work in direct cooperation with human workers within a defined workspace. The human and the robot simultaneously perform tasks during production operation. New developments on the new developments of safety systems in the industrial control system are discussed in this journal. These new approaches can help in determining the best approach to the design of the industrial safety system that is the most appropriate to the case in hand.[4]

## 2 RISK-ORIENTED APPROACH TO THE DESIGN OF THE INDUSTRIAL SAFETY SYSTEM

The risk-oriented methodology starts with a comprehensive evaluation of the entire system, in the form of hazard analysis. The method ranks each of the potentially hazardous components of the system based on its consequences and further risk of the potential undesired events related to the component. The main priority to be considered is human safety because the consequence of injury or loss of life of workers and other people has never been greater in the history of the industry. The shift of focus to put more value on human life, increasingly punitive regulatory bodies, and improving industry standards can incur huge losses to any industries which are not up to the standard of safety [5].

The two main approaches to the risk assessment are qualitative and quantitative assessments. The quantitative method uses various mathematical techniques such as probability theory, statistics, and so on. This approach is more objective and allows for the ability to properly react to a new risk [6].

*Corresponding author's email: arkrezah@gmail.com
https://doi.org/10.36706/jmse.v8i1.52

Things do go wrong, so it is important to create a risk minimization model, which includes the inherent risk of each operation. The frequency of the accident and the consequences or cost of the accident are both considered. These assessments result in a figure of layers of protection that aims to minimize the risks at different levels. The layers are divided into two, which are mitigation layers and prevention layers. Safety systems are more related to the prevention layers. The first layer takes into consideration all potentially hazardous processes and activities in the plant. The second layer is about the basic process control system which attempts to keep all process variables like temperature, pressure, level, and so on within the safe limit. The third layer is an alarm system that serves to alert the operators of a potentially dangerous situation.

The fourth layer is the Emergency Shutdown System (ESD), which is closely related to the topic of this journal. In the case when the operators fail to act on the warnings provided by the alarm systems, ESD takes action. ESD systems are always separated with their logic systems, sensors, and actuators to prevent the failure of the main system from stopping the function of the ESD. ESD must follow the following design systems: (1) Allowing the process to continue safely when specific conditions require it to. (2) Automatically bringing the process to a safe condition and (3) Taking action to mitigate the negative consequences of the accident. The fifth layer is simply physical protection like release valves and rupture discs in the case of overpressure, for example [7].

The further analysis phase uses a comprehensive process and hazards analysis (PHA). One of the methods of PHA is the Hazard and Operability Studies (HAZOP). HAZOP is a qualitative technique that focuses on the identification of possible hazards and problems of inoperability. The result of HAZOP is a table of process hazards aligning with the ranking of consequences. This ranking serves as the basis for allocation priority of the safety functions in the plant [8].

## 3 APPLICATION OF MULTI-SENSOR FUZZY INFORMATION FUSION ALGORITHM

This method aims to improve upon the traditional control methods to control the surrounding environment of industries, where a large number of sensors are used to monitor and control various parameters like environmental temperature, ventilation conditions, and many more. The information collected is usually processed separately which increases the processing workload and also ignores the connections between sensory information sources and the loss of features obtained through a combination of organic information. People describe variables qualitatively and cannot judge the safety conditions of industrial companies accurately. Compared to a single sensor signal source, a multi-sensor signal enables more reliable prediction results [9].

Fuzzy theory can handle many vague concepts in industrial production, which can help to provide a way to improve the objectivity of evaluation. Fuzzy comprehensive evaluation utilizes fuzzy linear principles transformation and maximum membership to formulate comprehensive evaluation, taking into account a variety of factors related to evaluated aspects. Fuzzy data fusion technology can be applied to industry safety monitoring. Under a fuzzy comprehensive evaluation technology and extracted feature fusion, a fuzzy data fusion algorithm can be proposed. Multi-sensor information fusion is used to synthesize information from multiple sensors or sources and eventually form a comprehensive safety decision analysis. The information that is collected at each sensor point can be more accurately assessed after data fusion in the fusion center. This enhances the monitoring reliability and improves the detection performance of the system, which provides a realistic basis for industrial safety. This increases the confidence level of the detection system capacity and improves monitoring performance, which is significantly superior to traditional industrial security monitoring methods [10].

## 4 ACCIDENT CAUSATION ANALYSIS AND TAXONOMY (ACAT) MODEL OF THE COMPLEX INDUSTRIAL SYSTEM FROM BOTH SYSTEM SAFETY AND CONTROL THEORY PERSPECTIVES

More and more complex systems are in use in industries. In complex systems, the incident frequency is low but the consequences are often dire, therefore it is important to gain valuable and sufficient information from limited incidents that happen. This is often done by summarizing laws

and common patterns from different failures to avoid similar accidents from happening again in the future. Models that have been published are either domain-specific or too general or complicated for practical application. The Accident Causation Analysis and Taxonomy (ACAT) model of the complex industrial system from both system safety and control theory perspectives addresses the two main issues of accident analysis which is determining what is a failure and how does it happen. [11].

First, complex systems are parsed into six components, namely machine, man, management, information, resources, and the environment from the view of system safety factors. From the perspective of control theory, actuators, sensors, controllers, and communication are defined as functional abstractions of system factors. The combinations of system factors and control functions form a matrix model for the analysis and classification of the cause of the accident, accident causation analysis, and taxonomy (ACAT) model [12].

Compared to existing complex systemic analysis methods, ACAT models can benefit not only accident analysis but also accidents Statistics. Its basis of a system framework, a solid theory, and accident reviews can benefit greatly from this. It helps accident investigators to understand accidents from a broader point-of-view and gather more information and can warn managers to consider all system factors to identify hazards and prevent accidents [11].

## 5 MODEL-CHECKING AS A PROTECTIVE METHOD AGAINST SPURIOUS ACTUATION OF INDUSTRIAL CONTROL SYSTEMS

Spurious actuation is defined as a failure mode where the actuation of an I&C function occurs without real demand. The terms “inadvertent operation” or “active failure” are also used. By their nature, such failures are more complex to analyze than “failure to actuate”. Spurious actuation can be caused by any failure between the process measurement sensors and the actuators, including erroneous operator command [13].

Model checking is a formal verification method by which the desired property of a (hardware or software) system is verified over a system model through exhaustive enumeration of all the reachable states and possible behaviors. When the design fails to satisfy the desired property, the model checker (a software tool used for analysis) produces a counterexample that demonstrates a behavior that violates the property. There is a long list of generalized design issues identified with model checking. These issues almost always depend on one of the following: (1) A memory element, such as a flip-flop switch of a hatch, (2) A delay element, (3) A feedback loop, (4) Detailed validity processing. The other recurring features of the scenarios include: (1) Exact timing of external events, meaning an event that occurs independently to the same processor cycle, (2) Human user interaction, usually personnel whether in operation or maintenance doing something not recommended or at the wrong time, (3) Interaction between several systems, which won’t be found when analyzing the systems in isolation, and (4) Process signal freezing on some fixed state [14].

The main difficulty of this method is achieving 100% test coverage. The tests must be exhaustive. The requirement specification documents of tools might not detail unwanted functionalities that usually accompanies their intended functionalities. Perceived cost is also a hindrance in this method. Further developments of practical user-friendly and domain-specific tools are expected to alleviate this issue [15].

## 6 CONCLUSIONS

The usage of machines and automatic control systems in industries carries an inherent risk to both human life and financial damage. Various means have been implemented to reduce this risk especially the development of safety systems in industrial control systems. With the industrial processes moving up from simpler to more complex ones, and the increasingly tight regulations aimed to protect human life, environment, and enforce an ethical industry, accidents are getting more and more feared. The fact that accidents cost a lot more nowadays from the huge fines and invaluable human lives that might be lost in an accident serves as a good incentive for industries to continue pushing for safer and more reliable systems. This safety part of the developments of industrial control systems will not slow down anytime soon. Industries must always look up to the newer and safer implementation of industrial control systems to protect their workers and their capital.

## REFERENCES

[1] L. E. G. Martins and T. Gorschek,

"Requirements Engineering for Safety-Critical Systems: Overview and Challenges," *IEEE Software*, vol. 34, no. 4, pp. 49–57, 2017, doi: 10.1109/MS.2017.94.

[2] Y. Chinniah *et al.*, "Safety of Machinery: Significant Differences in Two Widely Used International Standards for the Design of Safety-Related Control Systems," *Safety*, vol. 5, no. 4, pp. 1–16, 2019, doi: 10.3390/safety5040076.

[3] S. Chokkadi, C. C U, and Y. Jeppu, "Teaching Safety Critical Control System: A Success Story of Industry Academia Relation," *IFAC-PapersOnLine*, vol. 51, no. 1, pp. 524–529, 2018, doi: 10.1016/j.ifacol.2018.05.088.

[4] S. Rebello, H. Yu, and L. Ma, "An Integrated Approach for Real-Time Hazard Mitigation in Complex Industrial Processes," *Reliability Engineering and System Safety*, vol. 188, no. February, pp. 297–309, 2019, doi: 10.1016/j.ress.2019.03.037.

[5] K. Elena Vadimovna and K. M. Sergeevich, "Risk-Oriented Approach to Design of the Industrial Safety System: Problems, Solutions," *International Journal of Applied Engineering Research*, vol. 12, no. 16, pp. 5463–5471, 2017.

[6] W. Eljaoued, N. Ben Yahia, and N. B. Ben Saoud, "A Qualitative-Quantitative Resilience Assessment Approach for Socio-Technical Systems," *Procedia Computer Science*, vol. 176, pp. 2625–2634, 2020, doi: 10.1016/j.procs.2020.09.305.

[7] P. Zhu, J. P. Liyanage, S. S. Panesar, and R. Kumar, "Review of Workflows of Emergency Shutdown Systems in the Norwegian Oil and Gas Industry," *Safety Science*, vol. 121, no. February 2019, pp. 594–602, 2020, doi: 10.1016/j.ssci.2019.02.037.

[8] P. Baybutt, "A Critique of the Hazard and Operability (HAZOP) Study," *Journal of Loss Prevention in the Process Industries*, vol. 33, pp. 52–58, 2015, doi: 10.1016/j.jlp.2014.11.010.

[9] X. Zhou and T. Peng, "Application of Multi-Sensor Fuzzy Information Fusion Algorithm in Industrial Safety Monitoring System," *Safety Science*, vol. 122, no. September 2019, p. 104531, 2020, doi: 10.1016/j.ssci.2019.104531.

[10] S. Lu and S. Wang, "Intelligent Monitoring of Taijiquan Exercise Based on Fuzzy Control Theory," *Microprocessors and Microsystems*, vol. 82, no. December 2020, p. 103859, 2021, doi: 10.1016/j.micpro.2021.103859.

[11] W. Li, L. Zhang, and W. Liang, "An Accident Causation Analysis and Taxonomy (ACAT) Model of Complex Industrial System from Both System Safety and Control Theory Perspectives," *Safety Science*, vol. 92, pp. 94–103, 2017, doi: 10.1016/j.ssci.2016.10.001.

[12] C. D. Nwankwo, S. C. Theophilus, and A. O. Arewa, "A Comparative Analysis of Process Safety Management (PSM) Systems in the Process Industry," *Journal of Loss Prevention in the Process Industries*, vol. 66, no. November 2019, p. 104171, 2020, doi: 10.1016/j.jlp.2020.104171.

[13] A. Pakonen and K. Bj, "Safety and Reliability. Theory and Applications," *Safety and Reliability Theory and Applications*, 2017, doi: 10.1201/9781315210469.

[14] A. Pakonen, I. Buzhinsky, and K. Björkman, "Model Checking Reveals Design Issues Leading to Spurious Actuation of Nuclear Instrumentation and Control Systems," *Reliability Engineering and System Safety*, vol. 205, no. August 2020, p. 107237, 2021, doi: 10.1016/j.ress.2020.107237.

[15] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Information Processing and Management*, vol. 58, no. 1, p. 102397, 2021, doi: 10.1016/j.ipm.2020.102397.