The Resilience of Fully Automated Plants

Florin Omota

Fluor, Taurusavenue 155, 2132LS Hoofddorp, The Netherlands

Florin.Omota@Fluor.com

1. Introduction

Within the context of energy transition and the 4th Industrial Revolution, companies in chemical and energy sectors are adopting new automation and digital technologies to enhance the health and resilience of downstream operations. The ultimate vision of Industry 4.0 is to create fully autonomous plants that operate without errors and in an optimal, cost-effective manner. These plants integrate best-of-breed digital technologies, including advances in Industrial Internet of Things, Big Data, and Artificial Intelligence.

Autonomous plants operate continuously without human intervention. This leads to higher production rates and reduced downtime due to shift changes or breaks. Robots and automated systems can handle dangerous tasks, such as handling chemicals or working in extreme conditions without exposing the operator to hazardous scenarios. Labor costs decrease significantly when fewer human operators are needed, or when they manage remotely all plant operations.

2. Methods

Resilience engineering focuses on understanding how complex adaptive systems cope effectively with unanticipated events, preventing production loss and plant unavailability. On one side, the mechanical equipment, and Basic Process Control System (BPCS) should have high availability to ensure that the plant operates efficiently and meets the production targets. On the other hand, the Safety Instrumented System (SIS) should have high reliability in preventing hazards and production loss. Spurious trips are safe, however, having a negative impact on plant availability.

Both availability and reliability of BPCS and SIS can be modelled and consequently improved by Fault Tree Analysis (FTA) and probabilistic calculations. SIS reliability modeling is well known and already implemented as per international safety standard for process industry IEC 61511:2016 (e.g. exSILentia software provided by EXIDA). In this work, the reliability and availability of both SIS and BPCS were modelled based on benefit-cost analysis. This methodology provides an evidence-based evaluation, helping organizations become more logical and data-driven.

3. Results and discussion

Two case studies will be explained in detail. The first case considers selection of the most effective configuration of instrumentation for a highly available control loop. BPCS control loop failure is one of the most frequent causes identified in risk analysis. The consequences of BPCS failures are not related directly to safety in autonomous plants, but mainly causing equipment damage and production loss. Therefore, a benefit vs. cost analysis was used to optimize the instrumentation configuration. The cost of plant unreliability can be calculated based on hazardous scenarios identified in the Hazard and Operability Studies (HAZOP). The configurations of redundant instrumentation considered in this study were as follows: transmitters with 1oo1, 1oo2 and 2oo3, and final elements mainly control valves based on 1oo1, 1oo2 and 2oo4 voting. Based on the severity of consequences, there is an optimal combination of instrumentation that minimizes financial loss and increases plant resilience. The Mean Time to Fail Spurious (MTTFS) as well as benefits of redundant instrumentation are illustrated for a fully automated green Hydrogen plant with a capacity of 40 MW. In case of less than one day production loss, there are no benefits of implementing redundant instrumentation for this case.

Table 1: Redundant instrumentation benefits when avoiding one week production loss

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Transmitters | MTTFS | Benefit, €/y |  | Valves | MTTFS | Benefit, €/y |
| 1oo1 | 30 | 0 |  | 1oo1 | 15 | 0 |
| 2oo2 | 150 | +5585 |  | 1oo2 | 75 | +10520 |
| 2oo3 | 94 | +8866 |  | 2oo4 1) | 43 | +17560 |

1. Configuration with two control valves and two on-off valves, same risk of failure in both directions, either valves open or valves closed

The second example explains the design concept of a control loop fully sharing the instrumentation with a high reliability safety function achieving SIL 3. Increasing the availability of BPCS makes the process safer and reduces the demand of SIS.

The next figure illustrates the configuration of a highly reliable BPCS control based on redundant instrumentation as well as SIL 3 safety function in SIS. The level control consists of a master/slave configuration LC/FC in two parallel lines. The safety function consists of a level trip implemented as 2oo4 voting, or 2oo3 with an extra spare instrument for maintenance.



Figure 1. High availability of level control and very reliable level trip.

The reliability calculations for BPCS and SIS were calculated based on FTA and the approach proposed by Omota (2024). The presence of two control valves installed in parallel configuration ensures high availability of the flow control in BPCS. Failure of any flow or level transmitter is also tolerable. From a safety perspective it should be noted slightly lower reliability with four on-off valves instead of a simpler 1oo2 configuration. Overall, the MTBF for BPCS system is about 100 years while the risk reduction factor (RRF) of SIS function is higher than 1000.

The scheme shown in Fig. 1 has also high flexibility allowing full valve stroke testing at any time, as well as full testing of any other instrument, either online or offline.

4. Conclusions

Random failures or other upsets occurring in fully automated plants can be effectively managed by a proper design by installing adequate spare equipment and instrumentation. The methodology proposed demonstrates how FTA and probabilistic calculations are cost effective solutions in the design of fully automated plants, increasing both availability of BPCS and reliability of SIS.

Overall, this approach not only boosts the resilience and safety of automated plants but also provides a practical framework for implementing robust design strategies.

Références

Chakrabarti, G., Don, D., Smith, M., Vora, P., 2021. The autonomous plant: Entering a new digital era. Mckinsey & Company, 1-11.

Ham, D.-H., 2020. Safety-II and Resilience Engineering in a Nutshell: An Introductory Guide to Their Concepts and Methods. Saf. Health Work, 12(1), 10-19.

IEC 61511:2016. Functional safety - Safety instrumented systems for the process industry sector.

Kabir, S., 2017. An overview of fault tree analysis and its application in model based dependability analysis. Expert Systems with Applications. 77, 114-135.

Nascimento, L., de Oliveira, A.L., Villela, R., Wei, R., Hawkins, R., Kelly, T. (2024). From Fault Tree Analysis to Runtime Model-Based Assurance Cases. In: Barolli, L. (eds) Advanced Information Networking and Applications. AINA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 200. Springer, Cham. <https://doi.org/10.1007/978-3-031-57853-3_38>.

Omota, F., 2024. Basic Process Control System (BPCS) Reliability in Risk Analysis. AIChE NL/B. <https://www.aiche.nl>.