

Accident triggered by electrical failures in Seveso sites

Maria Rosaria Vallerotonda^a, Silvia Ansaldi^b, Annalisa Pirone^a, Tommaso Bragatto^c, Paolo Bragatto^b

^aINAIL, Dipartimento Innovazione Tecnologica, via R. Ferruzzi n. 38/40 - 00143 Roma, Italia

^bINAIL, Dipartimento Innovazione Tecnologica, Centro Ricerca via Fontana Candida 1, 00078 Monteporzio Catone

^cUniversità degli studi di Roma "La Sapienza", Dipartimento di Ingegneria Astronautica, Elettrica ed Energetica. Via Eudossiana, 18 - 00184 Roma (Italia)

m.vallerotonda@inail.it

Electrical maintenance is important for appropriate of Major Accident Prevention Policy MAPP at Seveso sites. At Seveso sites, many accidents include in the causes an electrical failure, due usually to a poor maintenance. Power outages, in particular, originate cascade effects, leading to a possible loss of hazardous materials. The repository of the minor incidents and near misses recorded at Seveso sites is a valuable source for investigating electrical failures, causes, effects and possible prevention and mitigation measures. The present paper discusses a number of incident records, gathered at Seveso establishments, during the mandatory inspections, required by the Seveso Directive. Gathered documents cover different types of plant, including refineries, oil terminal, LPG depots and chemical plants. They have been analysed, using advanced method, including machine learning. The results of this analysis have been exploited to provide the establishments' operator with a few recommendations, essential to improve electrical safety and prevent major accidents.

1. Introduction

Electrical failure is a problem in any industrial system, causing to the interruption of essential functions and services, not to mention possible fires caused by short circuits. In Seveso plants, however, it is more complicated because an electrical failure can trigger a "cascade effect", which can eventually cause a loss of containment of a dangerous substance and, in the worst scenario, a serious accident. A power outage stops the dynamic systems, including pumps and compressors, interrupts flows and may cause equipment damage and uncontrolled process deviation, which can end in a serious accident. An electrical fault can be even more subtle: a trivial damage to a single cable may prevent the signal transmission and compromise the function of a control system. That could lead to a process deviation and eventually a release of dangerous substances with possible severe consequences. In theory, process plants should be designed to be resilient to electrical failures, by the adoption of redundancy criteria and strict safety standard; but in the real practice, that is not always true and electrical failures impacts even on critical systems and trigger accidents.

The most frequent causes of failures are the ageing of the systems, the lack of or inadequate maintenance, the obsolescence; moreover, electrical supply could be interrupted because of a power outage of the transmission and distribution networks. In this respect, Transmission and Distribution System Operators are facing the increasing frequency of extreme natural events (e.g., heat waves, flooding, ice sleeves) that lead to long duration outages; indeed Operators and stakeholders are currently assessing and enhancing system resilience against natural threats, as in Bragatto et al. (2019) and Falabretti et al. (2020). Nowadays, it still happens that, when power outage occurs, the regular operations are not guaranteed since back-up power supply are missing or not available. Grattan and Nicholason (2010) discussed an overview of typical low and medium voltage electrical equipment used for the control and protection of electric motors in the process industries. It emphasizes the taxonomy used to classify the different types of circuit-breakers and their failure modes and the effects used to quantify performance. As discussed by Kallambettu and Viswanathan (2018) in some countries, including UK, regulatory authorities require the owners or operators to address the risks that arise from electrical equipment

failure and to have procedure to assure adequate operation and maintenance of electrical power systems and protection devices. HSE, which is the UK Authority for the Control of Major Accident Hazard, in particular, considers the ageing of electrical systems as an essential part of the much more general issue control of ageing at COMAH establishment (COMAH is equivalent of Seveso for UK). In the fundamental report published by HSE, there is a specific chapter on the ageing Electrical systems (HSE 2010); it provides both operators and regulatory bodies with many suggestions about the life cycle, the inspection and the maintenance of electrical control devices, cables, switchgear, transformers. This chapter is still the best general guideline on this matter, although the many progress in this decade. In particular, the concept of monitoring and maintenance have been overcome by the new approach of predictive diagnostics, which uses data driven algorithm to provide state-of-health and remaining useful life (RUL) of the critical electrical system, as discussed by Hofmeister et al. (2013). It must be said that there is an overlap between the issue of deterioration of electrical systems in general and that of the functionality of electrical safety systems, regulated by the standard (IEC 61511), for which many documents are available in the technical literature. However, IEC 61511 is not applied in most Italian Seveso plants, as too expensive and difficult. Furthermore, IEC61511 does not include power supply, switchgear, cables and transformers, which are involved in many failures and accidents.

A recent study by the European Commission (MAHB 2021) analysed and found, among the approximately 1100 major accidents recorded in the MAHB archive, 90 events, having as main or contributing causes, the failures of the power supply. The study considered the different types of faults and the different equipment involved; it was based on events occurred at European Seveso sites in the last two decades and reported to EU commission because their serious consequences for humans, environment or property. That study inspired the present work, which, instead, discusses events with no significant consequences. These events include minor accidents and near misses occurred at Italian Seveso sites. The study is focused on 86 events occurred in the last decade and caused by electrical failures. The results are compared with the previously mentioned European study (MAHB 2021). The considered events occurred under Seveso Legislation, which involves various process industries (refineries, petrochemicals, oil terminals and depots, chemical plants and warehouses). Thus, the results of different studies done in the scope of Seveso may be useful indeed for all process industries in order to prevent accidents related to electrical failures.

2. Materials and methods

2.1 Materials

During the mandatory inspections, required by the Seveso Legislation, the operators provide the inspector with a documentation of the operational experience, consisting of a summary report for each occurred anomaly, near miss or incident, according to the definitions of Italian regulation (UNI 10617). Since 2015, these documents have been collected on national basis for upper tier establishments. The document repository currently contains some 4200 reports, collected in five years by some 100 inspectors throughout Italy. The reports contain the description of the events, the analysis results with the identified causes, the technological devices and the organizational barriers (i.e. operational instructions or procedures) that failed or worked correctly, the recovery actions undertaken and the follow-up activities. They adopt a similar format, but are compiled differently for accuracy of details and information from one establishment to another. The value of those reports, however, is the textual description; thus, each report, usually one page long, describes, in a few sentences, *what* happened, *what* are the elements involved (equipment, substances, people), *what* failed and *what* succeeded. The challenge is to extract this information, i.e. textual data with their semantics, useful for several studies, including those for the recurrent issues related to well-known technologies, as discussed by Ansaldi et al. (2019).

2.2 Methods

The method adopted is hybrid, based on cognitive and statistical analysis. The cognitive method uses Natural Language Processing NLP and Machine Learning ML capabilities, parts of Artificial Intelligence techniques, to automatically extract and manage information from a bulk of data. Those types of tools are able to extract information from a text and classify into concepts according to taxonomies and ontologies; thus, Single et al. (2020) use these techniques to elicit concepts from eMARS accident database and build a knowledge base, Huges et al. (2019) to extract information from multilingual free-text safety incident reports in railway transport. The ML applied in this research is a supervised learning method, following the classification provided by XU and Saleh (2021), since the goal of the system is to learn a target function adopted to predict the values of an abstract concept. The cognitive method adopted, described in detail in (Ansaldi 2021), is able to extract, from the near miss reports, the types of equipment, the substances involved, the failure modes, the causes of events, the technical and organizational items and their relations (i.e. related_to, part_of, involves, and causes), thus, to represent the textual content into a relational model. NLP and ML tools by IBM Knowledge Studio (2021)

were used for training the model to recognize and extract the entities and their relations contained in the reports. A set of approximately 400 documents were annotated to train the machine-learning model. The archive currently counts more than 4200 reports, which are automatically analysed by the ML model when uploading documents. The EsOpIA (Operational Experience and Artificial Intelligence) is the application developed upon this deployed model to access and query the near miss archive. In EsOpIA, the search functionalities use both natural language and types of entities extracted by the model combined with logical operators.

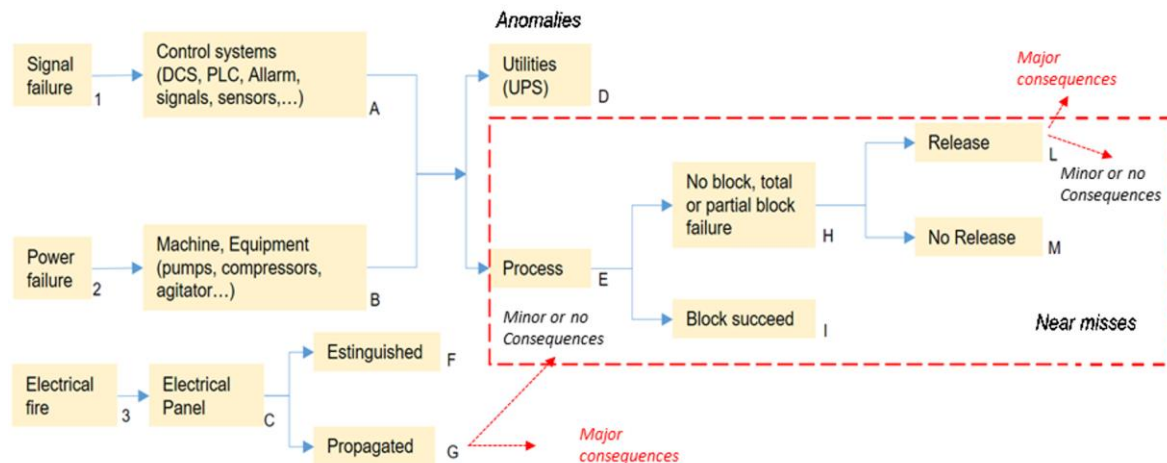


Figure 1: Schema related to “cascade effects”.

The schema depicted in Figure 1 shows how electrical failures can trigger cascade effects, having impact on control systems and utilities (i.e. anomalies) or on the process involving equipment and substances (i.e. near misses). For these events, it is discriminated the cases in which the safety devices interrupt the process (block succeed), from those in which blocks failed, partially or totally, or were missing, identifying the types of consequences with hazardous substances, including minor leakage, initial fire or none release. “None release” includes also the case of abatement into flare. The pathways of the schema are suitable to describe the cascade sequence. They were used for defining the queries to EsOpIA, which, in turn, are described as sequences of model parts, i.e. entities, concepts (instances) or relations, combined with logical operators. For instance, the query “power AND (event.failure AND technical-barrier (blocks, valves) AND event.loss”, means to search the cases related to power that have registered any type of failure (event.failure) of specific technical barriers (e.g. instances blocks and valves) with some loss of containment (event.loss). The system, however, is able to extract the other information, including the types of equipment or the substances involved. A further analysis was done, focusing on the role played by safety barriers, i.e. working, failed or missing. Considered barriers include technical control systems, protection systems, organizational resources and procedures. Trivial statistics was used to analyse the frequencies of the modes of occurrence highlighting the most common situations and to discuss the results with respect to accidents registered in eMARS repository (MAHB 2021).

3. Results

The search activity starts looking for reports that deal with power supply and then queries are refined by selecting types of entities, including failure modes (event.failure), loss (event.loss), technical barriers, or specifying concepts or instances, e.g. valve, DCS, UPS. The different pathways, named by the tags assigned to each box in the schema of Figure 1, represent the queries used in EsOpIA and described below with some examples.

3.1 Cascade pathways

The pathway 1-A-D in Figure 1 aims to identify the anomalies of safety utilities due to control systems failure; the queries consider the cases of event failures, such as blackout, outages, power interruption or overvoltage, and information related to the failed control systems are extracted. The results point out that the control systems involved in electrical failures include signals, inverter, sensors, and DCS. In the 15 reports extracted, one outlines that, due to a signal anomaly by the smoke and temperature detection systems of a drying department, the optical-acoustic alarms were activated and blocked the air conditioning and drying systems of the department; however, the event had no safety consequences other than those in economic terms. Another case describes that, without there activating any alarm signal, the PLC turned off; this had no consequences but could have caused problems in the operation of the reactors.

In the schema, the pathway 1-A-E-I describes the cases of anomalies of safety utilities that effect the process but the block devices worked correctly avoiding release of hazardous substances. As the previous case, the query takes into account the types of electrical failures, but highlights the technical barriers intervened to block equipment (e.g. pumps, agitators and compressors) and safeguard the process. One of the three results reports that, because of malfunction of the substation switch, the alarm missed, therefore, a compressor continued to run without the auxiliary utilities (e.g. jacket cooling water and lubrication oil). The compressor overheated causing minor damage, but without consequences for safety and the environment. Another report describes that a substation switch breakdown caused the disconnection of a turbo generator via DCS; therefore, the fan stopped and blocked the boiler. Consequently, due to the lack of steam, another turbo generator, working in parallel, stopped. The cases, described above, are anomalies since control systems failed; but in other three reports, similar events had impact on the process causing, together with failure of block systems, loss of containment of hazardous substances (pathway 1-A-H-E-L of the schema). One report describes that the anomalous signal emitted by a solenoid valve caused the intervention of control switchgear that interrupted the power supply to the process with a small release of substance.

Another question is to look for cases where power supply failure caused problems to the equipment and safety utilities but without arising process difficulties (pathway 2-B-D). The search is done on all types of event failure occurred at particular technical barriers, including UPS, monitoring system, fire-fighting system and generator. The 18 reports extracted show that the events have been blackout, short-circuit, power-interruption or functional interruption. One report describes that, due to disconnection of energy from the external network in the plant, all the equipment (pumps and compressors) stopped; the consequence was a general factory blackout, since the emergency electric generator did not work, but without release. In another event, a centrifuge stopped, apparently without reason (no high motor amperage, no high torque), and power supply failed. When the centrifuge restarted, there was a short circuit in it because one of the power cables was without insulation and thus, all the equipment stopped. This condition was due to the crankcase cover of the engine, which, with the vibrations of the machine, being supported by the cables, has worn one of them. The shutdown of all plant equipment and utilities did not cause any release.

The power supply failure, however, can affect the equipment and the process; therefore, it is important that the block systems succeed to avoid release of hazardous substances (pathway 2-B-E-I). The query, working on successful events (e.g. stop, block) activated by technical barriers, including blocks, valves, rupture disc, provided 26 documents. A report describes that a power outage caused the automatic energy system to intervene. Due to an anomaly of an under voltage relay, an overvoltage occurred unhooking the protection switch of a generator and failing the power supply with interruption of all equipment and processes, however, the safety devices worked avoiding release. Another document reports that a fault on the external power line caused a power outage and subsequent start-up of the UPS. The production plant stopped and at the same time, the valves closed and prevented the substance from reaching the mixing process.

There are 7 cases with similar conditions but the technical barriers for blocking the process, totally or partially, failed, without loss of containment, or the release was controlled (2-B-E-H-M). In one case, after a power failure, the emergency generator started to operate, guaranteeing continuity to the process. When the power is restored, the commutation required a temporary interruption of the functionality of the agitator, which caused a pressure increase in the reactor. The control system was able to change the number of revolutions of the agitator, thus the process did not have any consequences. In a similar case, the anomaly of the agitator speed, after the resumption of the power supply from the external network, led to an increase in pressure and consequent opening of the rupture disk with controlled release of the product.

In 5 cases, indeed, there was a loss of containment (pathway 2-B-E-H-L). Following a blackout due to a strong storm, the automatic emergency shutdown procedures of the plants started and the separate collection of chlorite circulating on the absorption columns was activated. An excessive amount of solution (yard run-off water and chlorite) reached the wastewater treatment plant; which had no overflow block, thus, the solution flowed out the pavement, and emergency actions have taken to avoid an environmental accident.

Referring to the events of electrical fire, pathway 3-C-F, three reports have been found. In one case, a fire in the low voltage electrical substation occurred because a deteriorated cable powering a critical pump. Even if the asset damage was minimal, the destruction of the electrical substation, the most loss was in the production interruption. In another case (pathway 3C-G), a fire started in the switchgear room of a production department due to the explosion of a capacitor, likely due to batteries in service exceeding their fixed lifetime.

The Table 1 summarizes the number of reports extracted for each pathway used in the search activity.

Table 1: Report extracted for the pathways

1-A-D	1-A-E-I	1-A-E-H-L	2-B-D	2-B-E-H-L	2-B-E-H-M	2-B-E-I	3-C-G	3-C-F
15	3	3	18	5	7	26	5	3

3.2 Barriers' analysis

Table 2 summarizes the roles of technical and organizational barriers to prevent events or mitigate the consequences, according to the analysed near misses. The third row (BOTH) provides the cases in which both types of barriers were involved in the same report. For each type, the Table 2 shows the number of reports were barriers successful (OK), failed (KO) and would be implemented (MISSING). The protection devices (4 cases) and UPS (3) were efficient technical barriers, while UPS failed in two events, 2 reports claim the lack of alarm systems and 1 the absence of plant protection system. The organizational barriers that worked successfully are the activation of safety (4) and emergency (8) procedures. Incorrect planning (8), unsuitable or not implemented maintenance procedure (20), incorrect activation of emergency procedures (4) and safety procedures (3) are the organizational barriers that failed. The reports contain also the follow-up actions for improving the safety conditions, including the implementation of new technical and organizational barriers. One of the technical measures found necessary to ensure continuity of power supply during the performance of activities is to make sure the presence and functionality of the UPS. Many operators, however, require the installation of devices for parameter detection and alarm systems (9 cases), while others, in 8 cases, have planned changes of the systems. Among the organizational / managerial solutions, the updating and / or implementation, where absent, of plant management procedures (6) or equipment maintenance and controls (7) were identified as necessary, while in 4 cases it was essential to strengthen the training of workers (4) to make them more aware and prepared to carry out their activities in the plant.

Table 2: Affected technical and organizational barriers

Barrier	OK	KO	Missing
Technical	6	8	32
Organizational	12	35	18
Both	6	12	5

4. Discussion

4.1 Comparison with eMARS

The results are compared with those obtained in the previously mentioned eMARS report (MAHB 2021). The events extracted from EsOpIA are not contained in eMARS and vice versa, thus, they are two disjoint sets, for which it makes sense of doing a comparison. In particular, Table 3 shows the comparison of the initial causes, Table 4 reports the consequences in terms of functions compromised by the cascade of events.

Table 3: Causes compared with eMARS

Causes of primary failures	EsOpIA	eMARS
Electrical faults	42	35
Loss of power supply	34	34
Power failure due to emergency rollout	3	3
Procedural error	5	2
Electrical fire	1	2
No information available	2	14
TOTAL	87	90

Table 4: Consequences compared with eMARS

Affected functions	EsOpIA	eMARS
Utilities (e.g. cooling, water, steam)	24	39
Process equipment (e.g. reactor, boiler)	26	36
Components (e.g. pump, valves, agitator)	13	32
Safety systems (e.g. firefighting, monitoring)	23	18

The numbers of events of the two sets are very close.

Due to the causes, there is a good consistency of the results between near misses and major accidents. On the other hand, for the consequences, there is a remarkable difference between the two sets. That is reasonable because in major accidents the cascade of events goes further, while in near misses it stops earlier.

4.2 Suggestions for Operators

Operators and control bodies are provided with a few suggestions, based on major accidents and near miss experiences as follows:

- protection of equipment: safety devices must be present and redundant on electrical equipment so that they are protected from any anomalous conditions during their activity and so that due to an interruption there are no negative effects on the equipment, on substances in process, on workers and on the environment;
- automation of intervention activities: making the intervention sequences more automatic makes the process more efficient and safer;
- training of personnel on emergency stop scenarios: increasing and strengthening the exercises of personnel on emergency scenarios makes them more aware and efficient to manage emergency conditions;
- independent and redundant power supply systems for critical equipment: equipment considered critical must be monitored and controlled by a specific DCS and powered by a UPS that is independent from the plant electrical network, checking component adequacy when new components are installed or replaced;
- the redundancy of the power supply systems guarantees the continuity and safe conduct of activities; strengthening of checks and maintenance of electrical components: regular checks and maintenance of the network and critical electrical components ensure the minimum safety conditions during life and use, but also the monitoring of aging and degradation problems of the same.

5. Conclusions

Effects of power outages on Seveso sites are still underestimated. From common experience, it emerges that they are caused by the combination of several shortcomings such as high grid usage, high-energy demand or anomalies due to the deterioration of electrical equipment. Even though the analysed events have no severe consequences, the causes that generated them are well known. It is therefore necessary for the operators to revive the knowledge and awareness of the importance of electrical system in chemical accident prevention. The cascade schema of accident sequence, was supposed a priori, and were confirmed by the analysis of many different documents, highly facilitated by the use of a few powerful ML techniques.

References

- Ansaldo, S.M., Pirone A., Vallerotonda M.R., Agnello, P., Bragatto, P.A. 2019. Near misses from the Seveso inspections: use of knowledge based methods for safety improvement, *CET Chemical Engineering Transactions*, 75.
- Ansaldo, S.M., Agnello, P., Pirone A., Vallerotonda M.R. 2021. Near miss archive: a challenge to share knowledge among inspectors and improve Seveso inspections. *Sustainability* 2021, 13, 8456. <https://doi.org/10.3390/su13158456>.
- Bragatto, T., Cresta, M., Cortesi, F., Gatta, F.M., Geri, A., Maccioni, M., Paulucci, M. 2019. Assessment and Possible Solution to Increase Resilience: Flooding Threats in Terni Distribution Grid. *Energies* 2019, 12, 744 <https://doi.org/10.3390/en12040744>.
- Falabretti, D., Lo Schiavo, L., Liotta, S., Palazzoli, A. 2020. A Novel Method for Evaluating the Resilience of Distribution Networks during Heat Waves. *International Journal of Electrical and Electronic Engineering & Telecommunications*, Vol. 9, No. 2, pp. 73-79, March 2020. <http://dx.doi.org/10.18178/ijeetc.9.2.73-79>.
- Grattan, D. Nicholson, S 2010 Integrating switchgear breakers and contactors into a safety instrumented function *Journal of Loss Prevention in the Process Industries* 23 784- 795.
- Hofmeister, J. P., Wagoner, R. S., & Goodman, D. L. (2013). Prognostic health management (PHM) of electrical systems using condition-based data for anomaly and prognostic reasoning. *Chemical Engineering Transactions* 33, 991 – 996.
- HSE 2010 Plant Ageing Study. Health and Safety Executive, Research Report 823. Crown Copyright© <https://www.hse.gov.uk/research/rrpdf/rr823.pdf>
- IBM Watson Knowledge Studio. Available online: <https://www.ibm.com/it-it/cloud/watson-knowledge-studio> (accessed on 20th December 2021).
- Kallambettu, J., & Viswanathan, V. (2018). Application of functional safety to electrical power equipment and systems in process industries. *Journal of Loss Prevention in the Process Industries*, 56, 155-161.
- MAHB 2021 Learning from incidents involving power supply failures *Chemical Accident Prevention & Preparedness L. L. Bulletin* No. 15 <https://minerva.jrc.ec.europa.eu/en/shorturl/minerva/>
- UNI 10617. 2019. Establishments with major-accident hazards. *Safety Management systems. Essential requirements*. UNI. Milano Italy.
- Xu, Z.; Saleh, J.H. (2021). Machine learning for reliability engineering and safety applications: Review of status and future opportunities. *Reliab. Eng. Syst. Saf.* 211, doi:10.1016/j.ress.2021.107530.