Safety practice

Hazard identification – can power engineers learn from the process industries?

Matt Clay, Health and Safety Laboratory, UK

Summary

The power engineering sector features similar challenges to the early process industries at the time when they first developed hazard identification techniques.

This paper summarises a pilot study carried out by the Health & Safety Laboratory (HSL) working with an electricity Distribution Network Operator (DNO) involving engineers and managers to determine whether process industry techniques could be adopted successfully to power engineering applications. The study focussed on the application of HAZOP and bow-tie.

The study suggests that appropriately selected and competently executed hazard identification techniques may be employed to help power engineers deploy exciting new power technologies safely and efficiently.

Keywords: Hazard identification techniques; HAZOP; Bow-tie

Background

The process industries have mature hazard identification techniques which can be systematically used on new designs, process changes and retrospectively on existing plant. Techniques such as the Hazard and Operability Study (HAZOP) are successfully applied to process plant for which mature standards exist but add even greater value when considering novel, innovative designs which need to be assessed from first principles. Indeed, HAZOP was first introduced at a time when process design standards were less mature and therefore hazard identification from first principles yielded improvements which today would be implemented by default[1].

Readers of LPB will be familiar with a range of differing hazard identification techniques, including HAZOP which considers nodes within an interconnected system and causes and consequences of hazardous conditions which may arise from causes local to that node or indeed remote from it. Failure Modes and Effects Analysis (FMEA) is a component level approach which is commonly used to ensure product safety of mass produced engineering products but is less well suited to a complex interconnected asset comprised of many different units. Bow-tie analysis is a hybrid bringing together the strengths of fault tree and event tree analysis and shows the development of loss events from initiating causes to impacts to people, plant and the environment. Bow-tie analysis can be performed with the integration of failure frequencies to inform decision making but it is also commonly used in a qualitative way which greatly aids risk communication of engineered systems where failures are not necessarily obvious or visible during plant tours.

Many process plants are complex in nature and often feature 'interactive complexity'[2,3], such that subsystems can interact in an unpredictable, non-linear fashion that can be difficult to understand. They also feature 'close coupling'[2,3] whereby initiating events can rapidly escalate to a loss event with limited time for hardware or personnel to intervene. A further challenge is that latent defects can exist within complex engineered systems which can remain undetected. As well as being useful systematic tools in the hands of experienced practitioners, many techniques[4] also allow the visualisation of process hazards and associated protective/mitigatory barriers, since unlike many occupational safety issues, process safety hazards and control measures can be hidden from view. A common tool within the process industries is the construction of 'bow-tie' diagrams which aim to show the development of major accident scenarios from initiating events through to loss events and physical impacts. Bow-tie analysis[5] is powerful in that it shows – in one diagram – all of the preventative and mitigatory barriers which prevent or mitigate escalation from an individual initiating event. This, combined with other data can help facilitate an assessment of whether risks have been reduced to tolerable levels. However it is also useful as a communications tool to share understanding of what makes a plant safe at all levels.

Electrical – Power Engineering – hazards can lead to electric shock, flashover, fire as well as initiation of ignition. Electronic hazards where systems are operating at extra low voltage are more associated with the failure of control systems to function properly – hence 'functional safety'[6]. Hazard evaluation techniques are relatively mature in the functional safety discipline but appear not to be systematically used within electrical power networks. It is true that individual items of plant, such as transformers and switchgear, are subjected to hazard evaluation by the manufacturers – typically using Failure Modes and Effects Analysis (FMEA). However it is not thought to be common for network asset owners/operators to apply systematic techniques holistically to a network constructed of a number of items of discrete plant. Load flow and fault studies are systematically applied to networks, particularly at high voltage (>1000V) but these are typically associated with only one deviation from design intent – overcurrent.

Power distribution networks, whether public networks or smaller site based private networks, share many features with process plants. Typically large, high value assets such

0260-9576/17/$17.63 + 0.00

as transformers and switchgear are interconnected with underground cables and overhead power lines delivering power to consumers in the same way that process vessels are interconnected by pipework and deliver useful products from raw feedstocks. The interconnectivity and increasing automation in power networks also make them vulnerable to interactive complexity and close coupling in a similar way to a process plant. The consequences of failure can also impact on the offsite public, typically with a smaller hazard range than a process plant, although prolonged loss of supply has been suggested as a public safety issue.

Previous work published in LPB[7] and elsewhere[8] suggests that techniques such as HAZOP could credibly be applied to power engineering applications. In fact the HAZOP application standard IEC 61882 makes clear the wide application of HAZOP beyond the process sector and even beyond engineering disciplines – for example use during the systematic development of legal documents[9]. The Health & Safety Laboratory (HSL) has previously published a review of the features, strengths and weaknesses of differing Hazard Identification Techniques[10]. This work was built upon by working with an electricity Distribution Network Operator (DNO) to run a pilot study involving engineers and managers within the DNO to determine whether process industry techniques could be adopted successfully to power engineering applications. During the course of the work it was decided to trial two techniques:

- HAZOP study, suitably refined for power engineering applications;
- Bow-tie study.

It is generally considered poor practice to apply HAZOP by 'rote' – i.e. selecting in advance combinations of guidewords and parameters, particularly since parameters should be derived from a well specified design intent. However given the unusual application, some example combinations were produced in advance of the study together with the deviation as it would be called in power engineering. It is also the case that some assets contain conventional process fluids as well as the electrical subsystems – for example transformers with oil circulation. Accordingly 'NO FLOW' is as credible as 'NO CURRENT' in these applications.

The study

A number of applications were selected by the client company for study. A number of simpler low voltage assets within the low voltage (400V line voltage) network – including an LV pillar within street furniture and connected to an open radial ring network which could be reconfigured to allow for fault restoration. Part of the HV (in this case 11kV line voltage) network comprising of a cable network between substations and a cable joint was also subject to HAZOP and bow-tie. The LV application was relatively simple in architecture and whilst the HV nodes were relatively straightforward they were subject to SCADA control and telemetry in terms of controlling continuity of supply.

Participants in both types of study were provided a briefing, including worked examples from the process industries. The analysis then began, facilitated by HSL specialists. The construction of bow-ties was much more intuitive and required less facilitation than the HAZOP study, as might be expected.

The main finding of the pilot work was that both bow-tie and HAZOP worked credibly in power engineering applications. Bow-tie was more efficient once a suitably defined electrical 'loss event' had been decided upon by the participants. Initiating events were readily identified from the considerable experience of the participants and this sharing of asset risk intelligence was a very helpful experience. Participants particularly valued the way in which a bow-tie

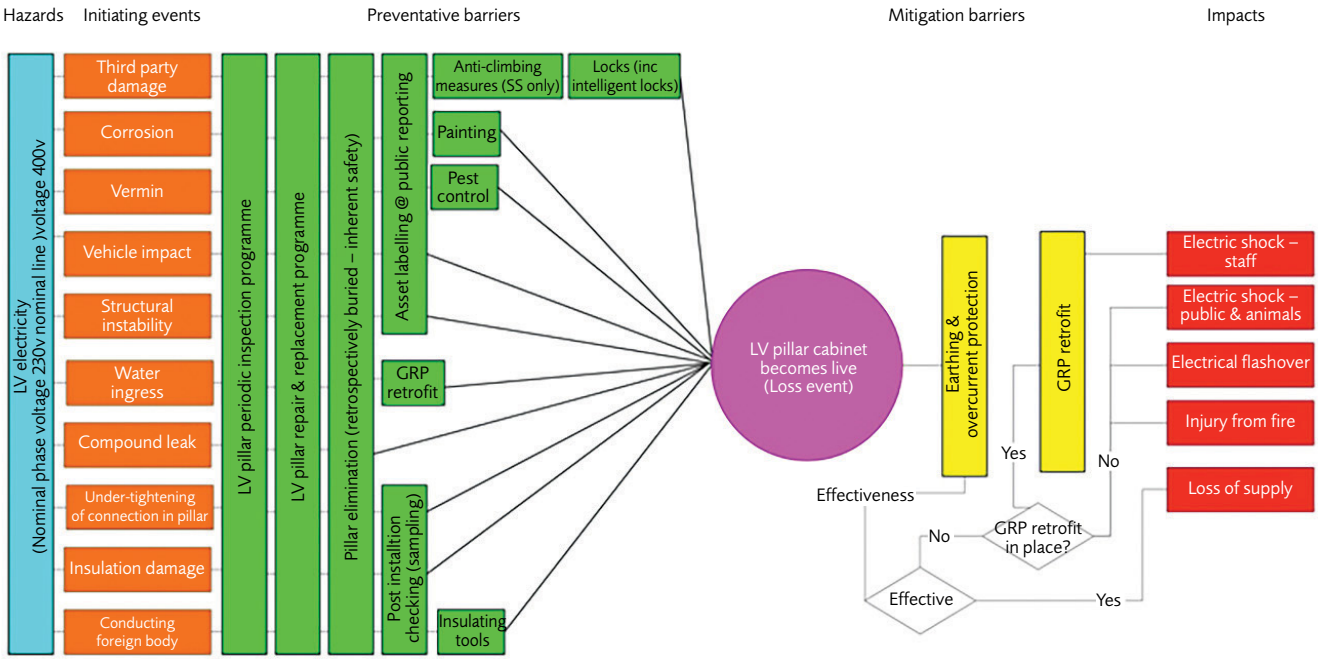

Figure 1 – Bow-tie applied to Low Voltage Pillar

0260-9576/17/$17.63 + 0.00

Guideword	Parameter	Example deviation & context
AS WELL AS *additional activity/event occurs*	VOLTAGE	Harmonics present – a power quality issue and can lead to localised heating and other failures
REVERSE *logical opposite of design intent occurs*	VOLTAGE	Reverse polarity on an overhead low voltage supply – i.e. phase and neutral transposed due to human error – can defeat some overcurrent protection and lead to other hazards to building occupants. Can be difficult to detect as equipment can function normally.
PART OF *only some of the design intent occurs*	VOLTAGE	Loss of one or more phase(s) on high voltage or low voltage feeder.
REVERSE *logical opposite of design intent occurs*	CURRENT	Backfeeding – e.g. from LV system onto HV system – may be desirable / undesirable depending on design intent.
MORE	IMPEDANCE	Protective earth connection is of higher impedance than the designer intended – leads to increased disconnection times in fault conditions – increased risk of electric shock.
MORE	IMPEDANCE	High resistance joint – causes heating which can lead to thermal runaway and joint failure – can lead to fire and/or flashover and give rise to electric shock risk.

Table 1– Example deviations in electrical networks

drawing could be used to visualise 'hidden' barriers as well as to make linkages to management systems which deliver or maintain the integrity of the barriers. It became apparent that many of the barriers were highly dependent on the information recorded in the company's asset management database, which highlighted the importance of this system to technicians, supervisors and managers.

The bow-tie output for one of the simpler assets studied is shown in Figure 1. This was for a Low Voltage (LV) pillar – effectively an above ground metallic junction box used to route power from a feeder to services supplying a handful of customers. Initially it was challenging to determine a central 'loss event' which is perhaps easier to do in the process sector – e.g. a runaway exothermic reaction. However the team eventually settled on the asset enclosure becoming live as the loss event since this approximated the CCPS definition of a loss event[5] being an irreversible physical condition with the potential for loss and harm outcomes.

The construction of the bow-tie, even for such a simple asset, was useful and was particularly valuable because:

- Several DNOs use a 'GRP Retrofit' which is a glass reinforced polymer cabinet that is oversized and fits over the existing metallic structure. These are particularly used in coastal environments where corrosion rates are accelerated. The exercise demonstrated the value of doing this, but also the limitations, for example such a retrofit prevents access to live parts by members of the public but offers no protection to staff having to access the inner metallic cabinet. Similarly it may prevent problems with water ingress but will not prevent corrosion of the original metal cabinet from ambient salt/water ingress.
- Highlighting the role of earthing and overcurrent protection as being mitigation of electric shock risk, not prevention. And therefore highlighting the importance of primary insulation, construction and commissioning as well as inspection activities. There is a common misconception that it is not possible to receive an electric shock from a properly earthed enclosure, this is not the case[11].
- Highlighting the relatively few barriers which provide common protection against many initiating events. This was particularly useful as these were in turn linked to key DNO management systems. For example several participants noted that if assets were missing from the asset management database then many barriers would be defeated by this common cause.

In terms of the HAZOP process, the combinations of physical parameters (such as 'voltage'), in combination with traditional process industry guidewords (such as 'as well as') yielded deviations which are meaningful in power networks (e.g. 'harmonics present'). Examples of the types of deviations which emerged during this work from applying guideword/parameter combinations are shown in Table 1. Creative consideration of combinations yielded some valuable deviations which were not as immediately obvious as those basic and well understood ones such as overcurrent.

These deviations were credible causes of safety and operability problems within the nodes studied. The issue was that existing designs meet well established standards in which these deviations have been considered and addressed, therefore the benefits yielded for the time invested were lower than might have been anticipated, even when considering that HAZOP is normally a time-consuming process[10]. DNOs also apply more rigour and analysis to higher value assets (e.g. transformers) and those assets operating at higher voltage levels with the potential to threaten security of supply more widely across a network. Accordingly whilst HAZOP works credibly, it yielded relatively few actions given the existing measures captured in the standards. One reason for this is that in contrast to some chemical industry applications (e.g. new production processes involving reactive chemistry), there are currently fewer variables which can be modified by electrical designers and design templates exist for new network additions. It does not appear from the available data that HAZOP is currently routinely used for power engineering hazards within UK DNOs for existing assets, although at High Voltage they have well established asset 'health indices' which consider failure modes and metrics (e.g. transformer dissolved gas analysis) which provide leading indicators of deterioration against those modes.

Conclusion

The nature of electricity distribution in the UK and elsewhere is changing and is expected to continue to do so in the future. The traditional model of power generation, transmission and

0260-9576/17/$17.63 + 0.00

distribution is one in which hazardous feedstocks are used to fire centralised generation at a tightly controlled well defined site. Power flows have been largely in one direction and replicated design templates have been used to determine network architecture. This is being challenged by future network technologies. Distributed generation at commercial and residential sites now means that power flows are not unidirectional and are becoming highly dynamic. Energy storage technologies are likely to be deployed at various places in the electricity distribution system, possibly even as street furniture connected at low voltage. The separation between 'process technologies' such as gas distribution and electrical technologies may well become blurred as part of the 'energy cell concept'[12] which includes power to gas technologies. Similarly, the basis of safety for electrical devices may need to change, with conservatism built into traditional design standards needing to be replaced with more flexible approaches which deliver the same overall levels of safety.

It is important for the power sector to consider the benefits of the approaches described, whilst at the same time remembering that there are drawbacks to every technique. It is still important to develop and comply with industry standards and assess the role of human and organisational factors through asset lifecycles. Hazard identification at the design stage does not provide any assurance that the as-installed plant meets the specification. Similarly small failures can result in significant outcomes – such as the incorrect protection relay settings, which in combination with other events, led to a famous blackout in 2003 in the UK. Similarly new hazard identification techniques – such as STAMP[13] have been developed which take a systems approach which may be particularly suited for power technologies – particularly innovative assets which combine process and electrical hazards.

In summary, the power engineering sector may well feature similar challenges to the early process industries at the time when they developed hazard identification techniques for the first time. Intelligent use of these techniques, appropriately selected and competently executed, may help power engineers to deploy exciting new power technologies safely and efficiently.

The Health and Safety Laboratory would like to acknowledge the contribution of staff, managers and directors within UK Power Networks who worked with HSL to deliver this work.

References

1. *Kletz, T., (2006), HAZOP and HAZAN – identifying and assessing process industry hazards, Institution of Chemical Engineers.*
2. *Lekka, C. (2011), High reliability organisations, a review of the literature, RR899, HSE Books: Sudbury, http://www.hse.gov.uk/research/rrpdf/rr899.pdf accessed 07/12/2015.*
3. *Weick, K. E., and Sutcliffe, K. M. (2007), Managing the unexpected: Resilient performance in an age of uncertainty, Second edition, San Francisco: Jossey-Bass.*
4. *Crawley, F., and Tyler, B., (2003), Hazard Identification Methods, European Process Safety Centre/Institution of Chemical Engineers.*
5. *Centre for Chemical Process Safety., (2008), Guidelines for Hazard Evaluation Procedures, Third Edition, Wiley-Blackwell*
6. *BSI., (2010), BS EN 61508-1:2010 - Functional safety of electrical/electronic/ programmable electronic safety-related systems. General requirements, British Standards Institution.*
7. *Mitchell, F.R., (1992), HAZOP reviews electronic interlock/control systems and electrical distribution systems, Loss Prevention Bulletin*
8. *MacDonald, D., (2004), Practical HAZOPs, Trips and Alarms, Newnes.*
9. *BSI., (2016), BS EN 61882:2016 – Hazard and operability studies (HAZOP studies) – Application guide, British Standards Institution.*
10. *Gould, J., Glossop, M., Ionnides, A., (2000), Review of Hazard Identification Techniques, Health & Safety Laboratory Report HSL/2005/58. http://www.hse.gov.uk/research/hsl_pdf/2005/hsl0558.pdf accessed 07/12/2015.*
11. *Jenkins, B.D., (1993), Touch Voltages in Electrical Installations, Wiley-Blackwell.*
12. *Weinhold, M., (2014), The Future of Energy, Siemens AG, Hannover MESSE 2014. https://w3.siemens.com/topics/global/en/events/hannover-messe/program/Documents/pdf/The-Future-of-Energy-Michael-Weinhold.pdf accessed 07/12/2015.*
13. *Leveson, N., (2003), A New Approach to Hazard Analysis for Complex Systems, Int. Conference of the System Safety Society, Ottawa, August 2003.*

0260-9576/17/$17.63 + 0.00