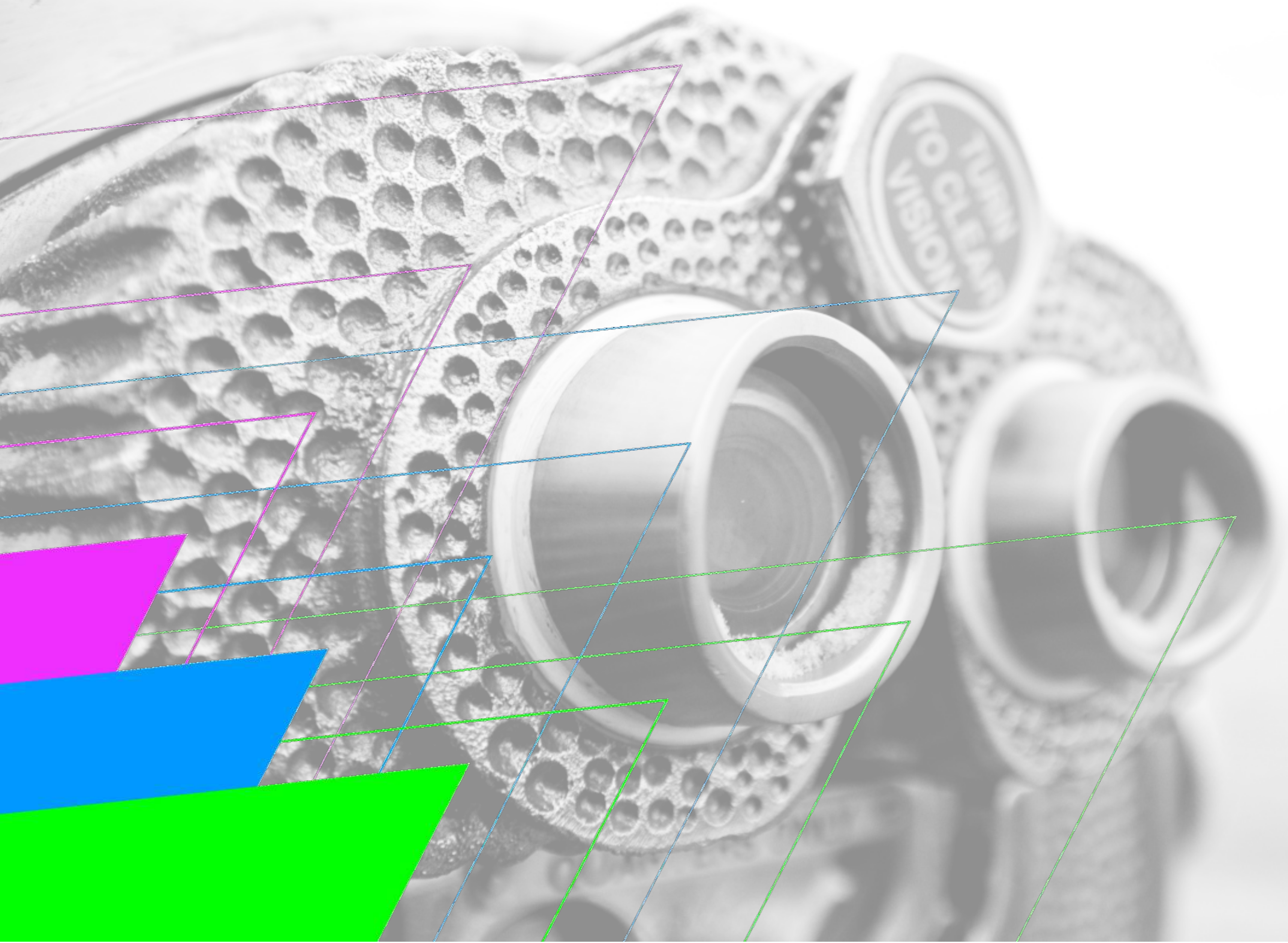
Enhancing Safety: The Challenge of Foresight

ESReDA Project Group *Foresight in Safety*

Chapter 6

Visibility of Early Warning Signs

Miodrag Stručić



ESReDA
European Safety, Reliability & Data Association

Table of contents

6 Visibility of Early Warning Signs

Miodrag Stručić, Joint Research Centre, European Commission, The Netherlands

6.1 Executive summary

Visualisation of early warning signs is critical for clear understanding of existing weaknesses' roots and to define effective actions to prevent their escalation. The process of visualisation is described by use of fictional devices and features to emphasize the importance of different phases in the process.

In the first phase of the visualisation process, "detectors" are used for detection of warning signs - "signals". Their "output" is further "modulated" through reporting systems to provide a robust repository of important facts, but also attributes about issues, as well as to increase awareness in our socio-technological Organisation. These signals are then "amplified" to an appropriate level of visibility, by which we are able to fully understand vulnerabilities of the Organisation. These insights, combined with the knowledge and experience of operations and design, provide necessary ingredients for smart decisions in fighting potential threats.

6.2 Introduction

Warning Signs, like the signs defined by road traffic regulations, provide information about immediate, delayed or potential danger. In every case they should be treated as Early Warning Signs (EWS), and every warning sign, if processed in the right way, will eliminate the possibility of its escalation. This is true even if an immediate event occurs – registered and processed through an efficient Operational Experience Feedback system can help affected stakeholders and those responsible for similar Organisations to prevent similar events.

There are many Early Warning Signs (ESW) that can be detected and adequately treated before they transform into a bigger problem. Some EWS however are too weak to be recognised as a threat to safety, but are still detectable. Once detected, those signs-signals should be "modulated" and "amplified" to an appropriate visibility level that can be justified as a treat by stakeholders. When signals are visualized and presented as a real threat, they can be efficiently treated to prevent further development into new incident or accident.

The main objective of this chapter is to define or give directions to define how to reveal or visualise EWS in socio-technological environment. Not only in-house, but also external and publicly available data, should be used to help in determination of EWS. Better understanding i.e. visualisation of this data can help Organisations that didn't experience the same or similar incident to foresee safety hazards, assess the risk of its occurrence, and initiate adequate measures.

It is not easy to quantify the contribution to safety processing of external experience, but due to similarities of hazardous industries in their safety concepts, the basic reasons for reported deviations should be examined with the same respect and effort as for their own.

6.3 Detection

Signals of decreased safety – Warning Signs in Hazardous Organisation - should be recognised and confirmed by any individual regardless of his/her organisational level (IAEA, 2018). Reporting these signals is of the highest importance for Organisation, not only because of immediate prevention of an undesirable event, but also to enable a system of multi-dimensional assessment whose main purpose is to improve the safety level of the Organisation i.e. reduce the probability of severe accidents. Detecting these signals is easier if they are obvious, but signals identified by "out of routine" practice could be very difficult to detect.

However, information about deviation, no matter how it is detected (Stručić., 2016), should activate the system which is able to "visualize" any warning signal. Good definition of EWS could improve their detection and treatment. For this purpose, it is equally important to define main detection modes and categorise them. To better understand detection modes it is necessary to distinguish different types of "detectors".

6.3.1 Built-in / Surveillance Detector

Most EWS are discovered by design. These include all forms of alarms and annunciators, as well as indicators and records required to monitor processes during all phases of operation. Also check/verification-lists predefined in written form (audits, QC, operating procedures) present an efficient tool to detect warning signals.

Good examples of built-in or Surveillance detectors are annunciators' panels in Nuclear Power Plant (NPP) Main Control Room (MCR). Even in the case that some "unimportant" signal is created in one of the less important locally controlled systems, the alarm from local panel will send a signal to the MCR and the Main Control Board alarm for local panel will go off. MCR operators usually ask the local operator for signal confirmation and react to this alarm in accordance with a well defined procedure. Process failures that often occur are treated instantly but they are also recorded in Log Books, Process Information System or reported through Corrective Action Program - CAP (IAEA, 2005).

Furthermore, some non-wired detection processes, e.g. auditing, are strictly following a prepared plan and procedure so that all non-conformances are recorded and reported through a final report. The same is true of Quality Control inspections which are performed in accordance with strictly defined check-list items. In the case of a verification procedures (e.g. Line-up checks) performed by an operator, the response to a discovered deviation is similar to the response to an automatically detected deviation.

Detection of these deviations usually brings immediate solutions and they are not followed by deeper investigations. These approaches produce large numbers of recorded items, but in our moment of Organisational and technological progress, it is still acceptable to leave most of them for later deeper assessments. In other words, there is still no available automated system[18] to connect all detected items, compare them, use available "experience" and immediately process them in the best way for optimized and safe further operation. Although technological design experts are striving to build a system that can predict all deficiencies and warn operators or auto-correct them, would it be ever possible? Certainly it would never be possible using only built-in/surveillance detection as the abandoned IAEA ASSET program showed.[19]

[18] *Or Artificial Intelligence system*

[19] *E.g. abandoned IAEA ASSET program for prevention of incidents and accidents where the main input was surveillance data which was not sufficient to foresee enough incidents to prove effective.*

6.3.2 Advanced systematic approach Detector

There are also Early Warning Signs which could be detected by assessment tools (IAEA, 1997) - Focused Self-Assessments, Safety Assessments (Risk Analyses), Peer Reviews, Advanced Surveillance programs[20], Performance Indicators programs, as well as Preventive and Predictive Maintenance. These tools enable discovery of the EWS in a systematic, predefined way, many times by teams with expertise and experience in specific areas. Although some of these approaches overlap with Built-in approaches, they enable discoveries of deviations thanks to performers' incisive and experienced approach, i.e. they give freedom to performers to examine a wider range of assessed items.

The advantage of the team approach lies in the fact that experts, who are usually not part of the specific assessed process, reveal deviations using their experience, knowledge, skills and techniques, and many times seeing things with "different eyes". They can reveal hidden deviations not visible to staff doing routine work in their field. It could be e.g. human or organisational issue easily visible from team member chosen from management or non-related domain experts.

Advanced surveillance programs, i.e. non-built-in detectors, give freedom to performer(s) to find unexpected inconsistencies or discover that faulty equipment or systems point to the deeper reason for a given anomaly. A typical example would be detecting a fault induced by ageing of a component[21] which is, almost by default, applicable for all other items in the corresponding group or system. Thus, Operating Organisation will not just fix the problem, but also launch actions to assess the system and find optimal solutions.

EWS discovered by one of these approaches is not always pointing to the main problem, therefore the assessments' results should be analysed for deeper causes. E.g. Performance Indicator detects negative trend of "Number of Overdue Work Requests", but additional effort is needed to find deeper reasons for this trend.

[20] *Various surveillance techniques and tools that are not originally installed in the Organisation. Those include e.g. advanced electronic diagnostic equipment components, new process data analysis programs etc.,*

[21] *Note that Ageing monitoring scope can overlap with Built-in detectors*

As mentioned, these approaches can overlap with Built-in ones, but their results are less predictable. This also means that trends of number of detected issues can vary significantly over time. In the case of a decreasing trend, an Organisation may think that further use of one of these tools is unnecessary, but in fact it is just the opposite – the declining trend should stimulate the Organisation to improve their detection program (explained more in Trends in detection of deviations subchapter – 6.3.5).

6.3.3 Analysis of Operational Experience and Technological-Organisational-Human performance Detector

A hidden EWS could be detected by revealing latent weaknesses using Causal analysis of internal and other industry's events. Good examples can be found conducting Root Cause Analyses which compile event investigation results. Thorough investigation followed by systematic definition of causes reveals warning signals which contributed to the evolution of an analysed event. E.g.

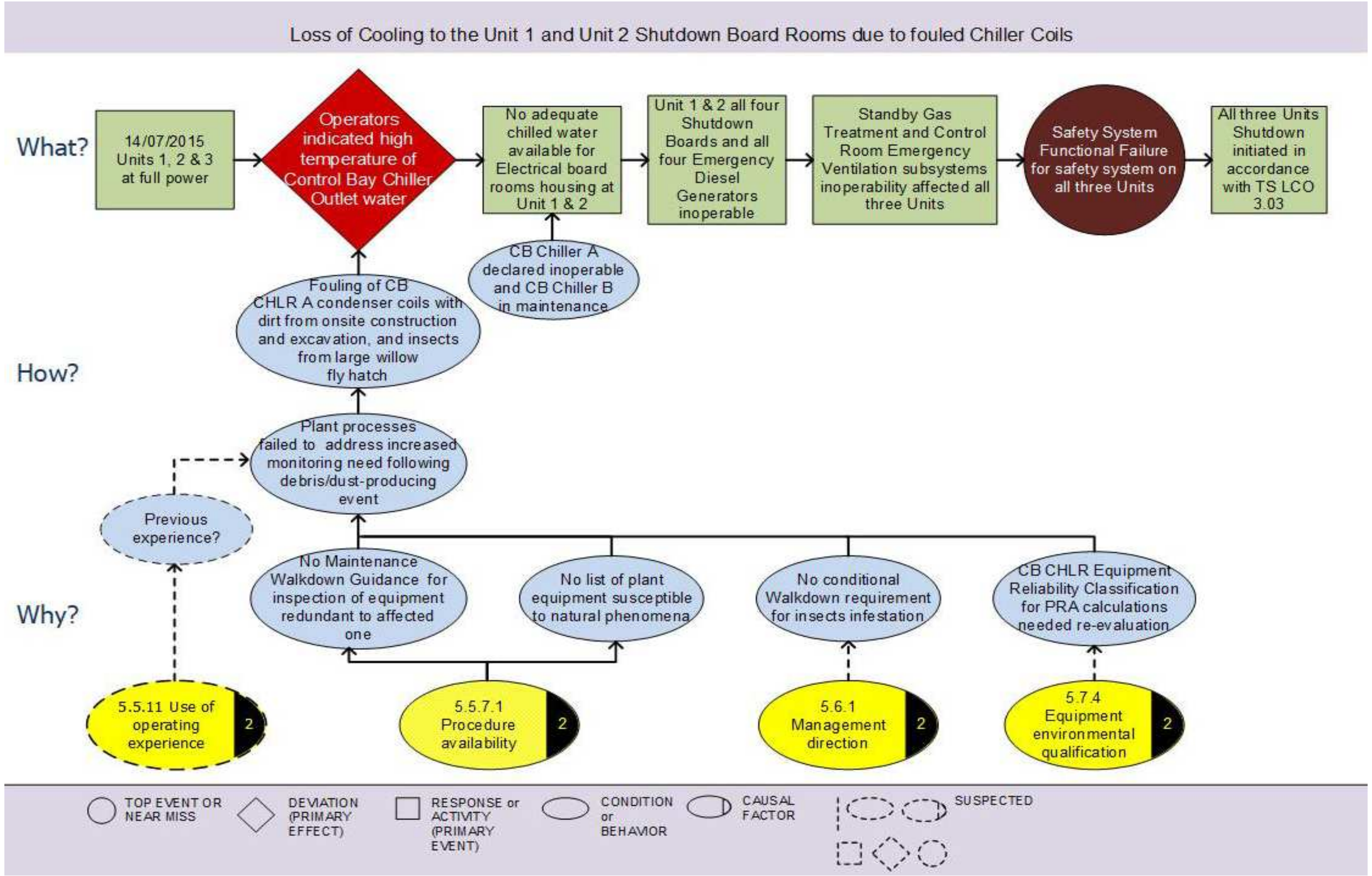


Figure 1. Event and Causal Factor Short Chart – Loss of Cooling event

factors connected with Personal Work Practice could reveal that Lack of Peer Check in Critical Task is one EWS.

There are many approaches, techniques and tools used in analysing events (Ziedelis and Noel, 2011) or Near misses (subchapter 6.4.1), but one technique often used for events in NPPs is Event and Causal Factor Charting (E&CFC). An important advantage of this charting technique is that visual presentation of analysis transparently shows the causes of an event that can then be easily used to define adequate action plans. This advantage could be used also for the purpose of presenting events after the analysis is performed. In two examples (fig 1. - 4.) of not-so-significant events in NPPs some not very transparent issues are highlighted (Strucic, 2017).

Example in Fig 1. presents an event in one NPP that had no adverse safety consequences but its Root Cause Analysis revealed some potential causes which the affected plant then eliminated by adequate actions to prevent a more serious event. What is not explained in the analysed report, is how one of the revealed problems was treated in the past. In this concrete case, non-use of operating experience or ineffective corrective actions are typical possible causes of repeated problems. It is visible in the highlighted part in Fig. 2.

The second example in fig 3. shows hidden Human and Organisational Factor (HOF) problems not revealed in the published report and most likely not in the original one either. While the Organisation could be satisfied that the revealed cause points to deficiency in the specific software, behind this cause there are possible warning signals of deficiencies in HOF domain which could create more serious problems. It is visible in the highlighted part in Fig. 4.

These examples show how to reveal additional or hidden warning signals which could be ignored or missed in routine Condition/Deviation report processing. This approach can be used by any similar Organisation interested in safety improvement of their own installations. The Operating Organisation where the event occurred can benefit the most, but all other similar Organisations can also find it useful.

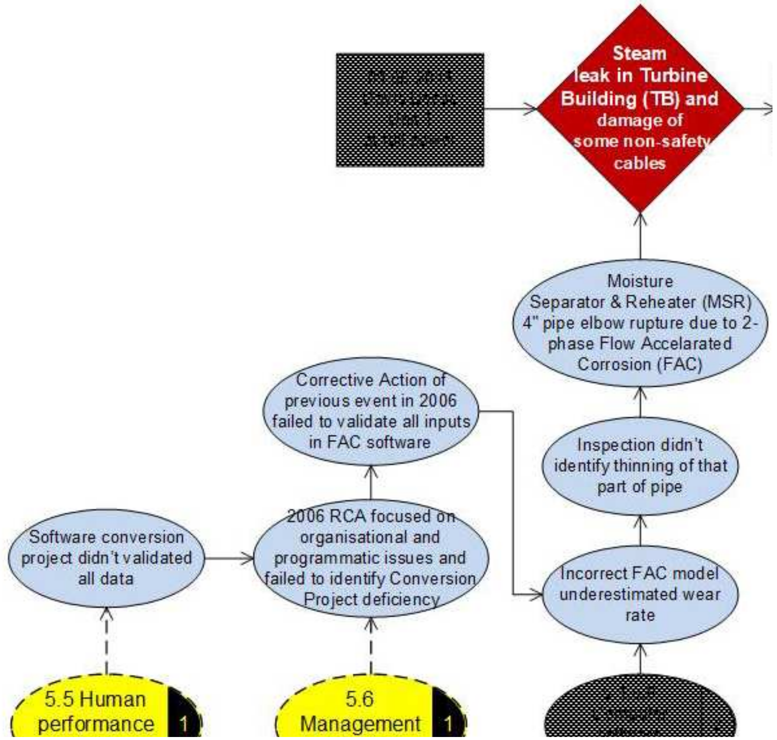


Figure 2. Event and Causal Factor Short Chart – Loss of Cooling event highlight

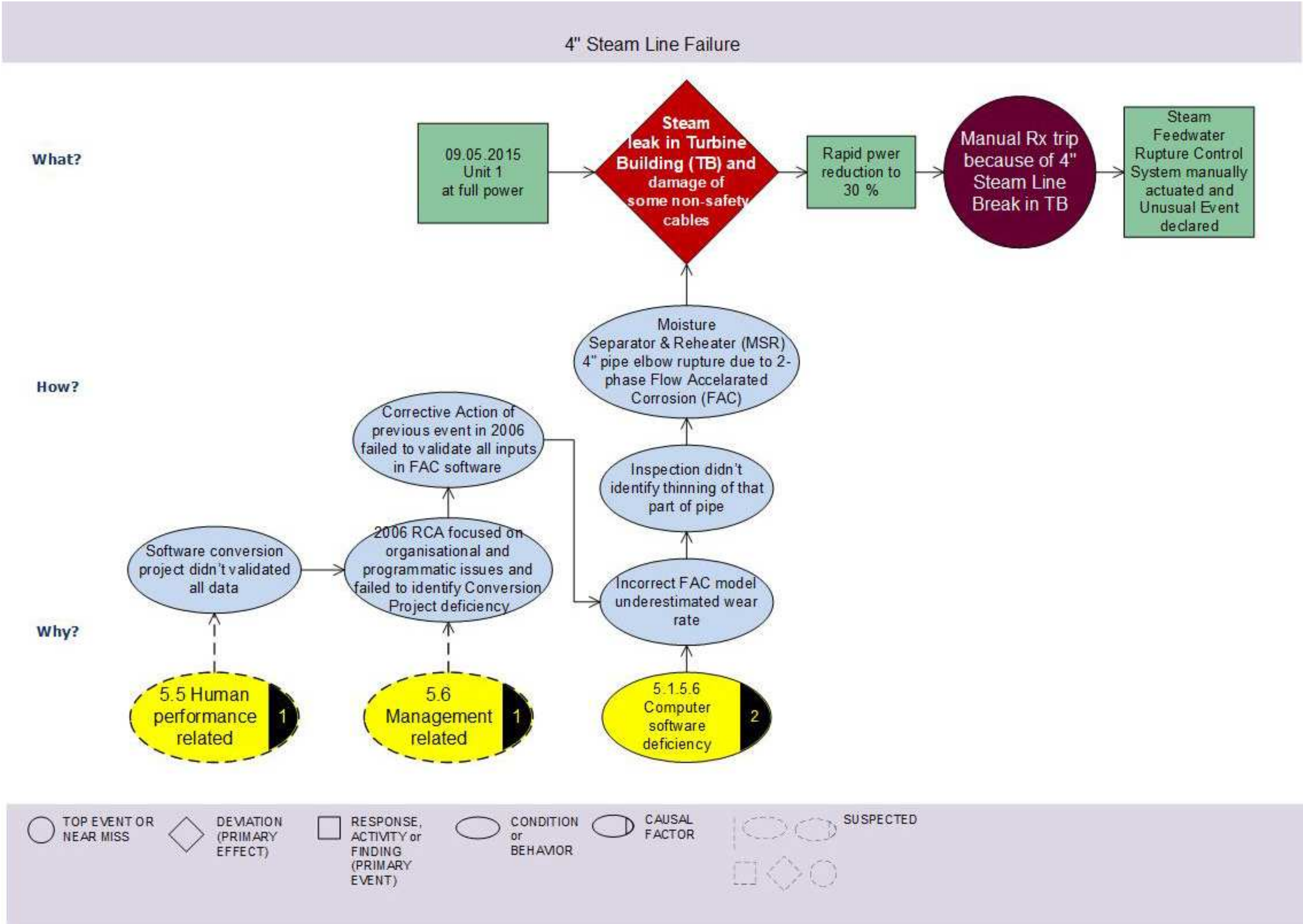


Figure 3. Event and Causal Factor Short Chart – Steam Line Failure event

It should be mentioned that short E&CFC diagrams (fig. 1-4) can quickly give to external operating Organisation the essential information needed for fast qualitative risk assessment of a potential similar problem (Strucic, 2017). Evolution of event is presented in the Primary event line – in the upper horizontal row. An experienced and knowledgeable stakeholder can find out if the event is applicable to his/her Organisation and what is the potential hazard. The mechanism of each defined deviation (red rhomb) genesis is explained in below connected boxes by the most appropriate answers to how and why questions.

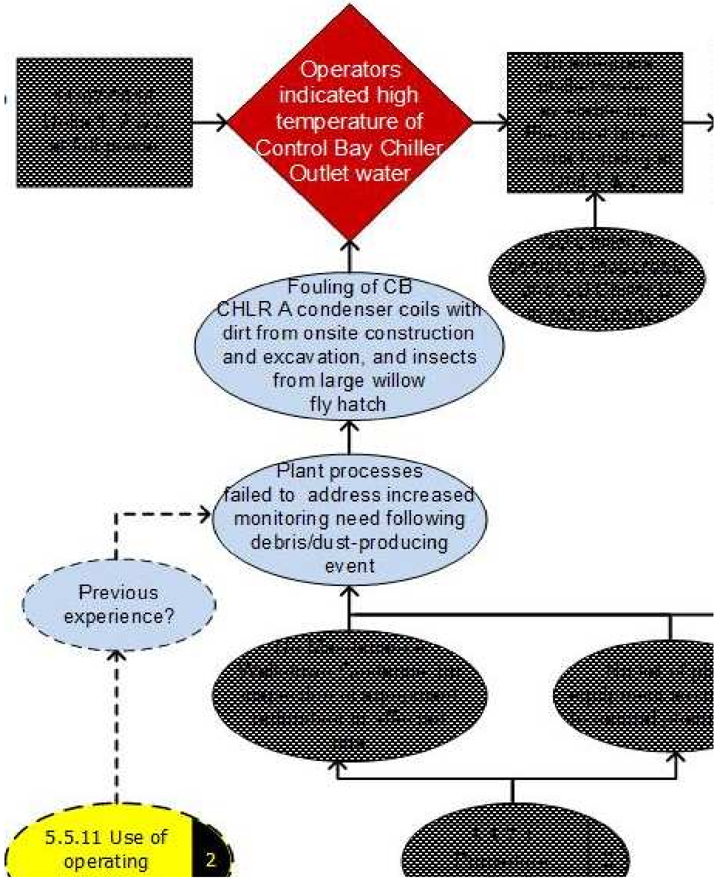


Figure 4. Event and Causal Factor Short Chart – Steam Line Failure event

Understanding causality of deviations gives the stakeholder an idea of vulnerability of the operating Organisation under his/her responsibility. Knowing potential hazard and how vulnerable the Organisation is to similar or same deviation provides stakeholder the rough estimation of their own risk. Therefore, stakeholders can easily decide if action for changes or further self-assessment in the Organisation is needed.

6.3.4 Detection by "chance”

Many times, the problems, especially of human or Organisational nature, are discovered during activities different than ones described in previous subsections. Those could be just a "side product" of activity like meetings, trainings, work-related trips or even some activities outside the regular working hours or Organisation premises.

Also “Equipment related” deficiencies can be detected by “chance”. As a concrete example, when one NPP unit experienced an unplanned Reactor Shutdown and activated some systems important to safety (IAEA, 2015), two major systems faults were discovered. Fortunately, the safety system activation wasn’t required and these deficiencies didn’t result in unsafe conditions. This case clearly showed that surveillances, tests or any other defined assessment approach could not detect these problems. A good lesson from this event teaches operating Organisations to thoroughly examine all their major unplanned transients and find deficiencies that couldn’t be found by regular established processes.

Since reporting requirements are not able to address items detected by “chance”, they may not be processed and easily can be forgotten. However, deviations found "by chance" could be of high importance since other systematic and well-defined processes didn’t detect them and probably won't. Therefore, Organisations should increase their awareness of all minor, hidden or accidentally found warning signals and encourage employees to report them too.

6.3.5 Trends in detection of deviations

In any discussion of detectors, it is important to mention the possibility of trending detection modes. The Topical study of Nuclear Power Plants design deficiency (Stručić, 2016) reviewed the worldwide operating experience from NPP events where design deficiencies are addressed. One of the outcomes, the trend graph, has been created during this study (Figure 5.).

The Detection Mode trend graph, based on information provided in IAEA International Reporting System (IRS) (IAEA, March 2020, https://nucleus.iaea.org), shows that the number of events with actual consequences is increasing over time, which suggests both that other detection approaches should be employed and existing detection should be improved. A sudden drop in the number of events that are detected by surveillance and reviews may be an indication of obsolete or inadequate deficiency detection methods.

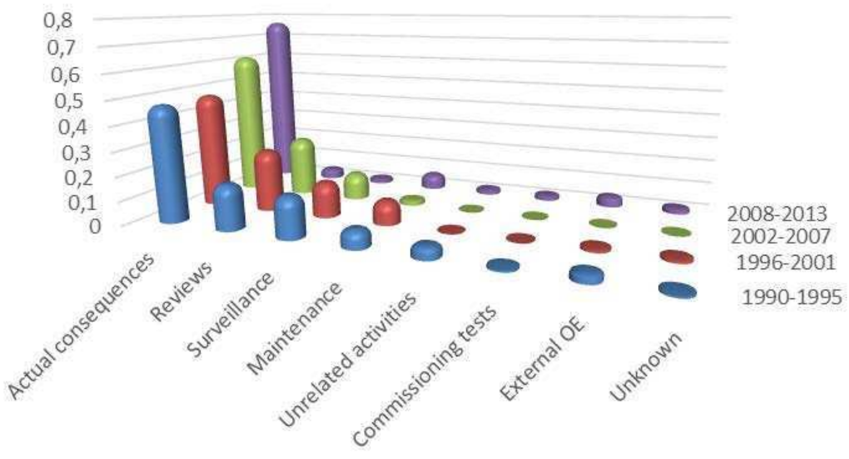


Fig 5. Trend graph of detection modes of design deficiency in IRS

The graph of detection mode trends could indicate if the main tools for detection of deviations are becoming inefficient. If there is no appropriate recording and coding/categorisation of events in operating Organisations, it could be difficult to create trend graph, otherwise this could be used as one Performance Indicator as well.

6.4 Reporting system

The simple concept of Problem-Screening-Analysing is a natural approach for handling any problem. Hence, it can be very practical to use Corrective Action Program (IAEA, 2005) concept for any kind of problem (IAEA, 2012).

It worthwhile to note the definition of USA Nuclear Regulatory Commission - *CAP is the system by which a utility finds and fixes problems at the nuclear plant. It includes a process for evaluating the safety significance of the problems, setting priorities in correcting the problems, and tracking them until they have been corrected* (USA Nuclear Regulatory Commission, March 2020, https://www.nrc.gov/reading-rm/basic-ref/glossary/corrective-action-program.html).

6.4.1 Deviation Report

Whatever the source or detection mode of EWS is, the first step in any CAP process is to record the detected deficiency (acquisition phase in fig. 6) through a Condition/Deviation Report Form. Practically, the whole process of visualisation is useless without input – acquired anomalies, errors, mistakes, discrepancies, wrongdoings, or simply, any deviation or problem. Operating Organisations should promote a Reporting Culture (Reason, 1998) and encourage all employees to report all noticed deviations and potential problems.

Furthermore, there are many definitions of Near Misses but are they really necessary? "Things are never so bad they can't be made worse", a favourite Humphrey Bogart quote (Brainyquote.com, March 2020, https://www.brainyquote.com/quotes/humphrey_bogart_108860) is relevant – it reminds us that all events, major or minor, need only some small effort of evil or bad luck to become worse. By this interpretation all events can be considered as Near Misses. And, needless to say, any event labelled Near Miss can easily propagate under some realistic circumstances to become a disaster. Thus, all undesirable events, regardless of the consequences, should be reported and analysed.

Organisations should be aware and avoid traps of non-reporting. The first notice or record of any deficiency or irregularity is the crucial step which is easily missed, e.g. because the person who discovers it cannot foresee all possible consequences, interactions or users of reported/recorded information, and doesn't consider it important to report through the official reporting system.

The reporting system should be easily accessible and user friendly for all employees, regardless of their position or duty. The reporting form should include questions about:

- What happened?
- Time, location and involved subject(s); and
- Author – This is important for evaluators to know whom to ask for possible additional question. But it must be emphasised that anonymous reporting should be encouraged as well and always be an option;

The author should be encouraged to include all information necessary for further processing (equipment number, coordinates, time of discovery, procedure used, circumstances, misbehaviour, outcome, proposed action etc.). Reporting application could ease this input with predefined lists of equipment or persons, as well as other relevant categories.

Once the record is created, screening of the deficiency should be performed as soon as possible.

6.4.2 Screening and categorisation

When the first key step is done, i.e. the deviation is registered in the Reporting System, the responsible personnel should take care of further processing of the report as soon as feasible. Besides technological classification (equipment numbers, mode of operation, failure mechanism…), additional categories should be entered: If there is an urgency to react; what corrective measures are taken; what could be possible consequences; what is a safety significance level; which department and person is responsible; dissemination list etc. - information necessary to effectively fix the problem, transfer lessons and experience, and provide basis for possible deeper evaluation.

This phase is partially automated, and may be further automated in future, but human involvement is indispensable. Having a good knowledge of design, operation and Organisation increases the accuracy of categorisation and enables more efficient further processing. A broad understanding of possible data used by different stakeholders or by other programs in the Organisation is one of the benefits of having experienced and knowledgeable screeners.

A good example of an efficient screening process highlights two levels of screening phase. All reported deviations from previous day are discussed at morning multidisciplinary Screening Committee meeting where decisions are made how to treat the reported issues and who will be responsible for further actions. It is usually organised immediately after Operations' meeting where often first-hand information about safety and technical issues are given. In parallel, the Independent Safety Engineering Group is taking care of coding, administration and coordination of all CAP items. This experienced staff is further involved in analyses and trending of events, which is a highly important part of whole CAP process (Bach, 2007).

6.5 Visualisation

As explained in the previous sub-chapter, the destiny of each item in the CAP depends, in the first place, on screening. Typically, after screening of the Deviation/Condition Report, Apparent Cause Analysis is performed, tasks are sent to responsible persons and information is disseminated. Very few of events are immediately investigated and more deeply analysed by Root Cause Analysis. Whatever method or tool is used, it is important that the deviation's causes are registered and can be further processed.

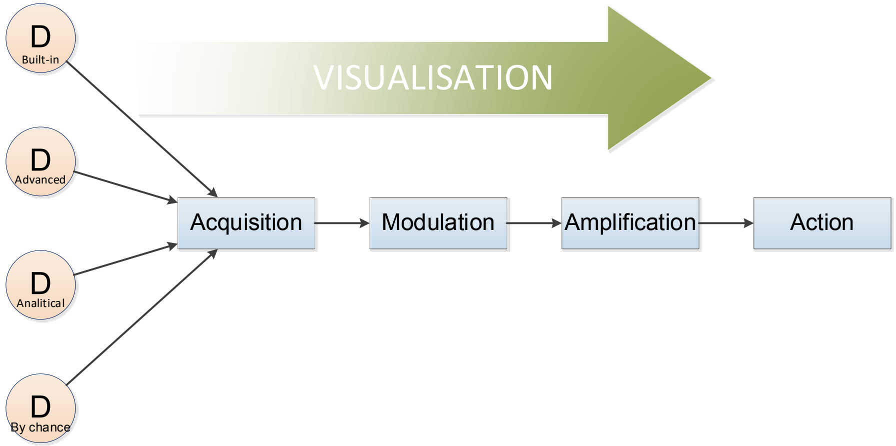


Fig 6. Simplified diagram of whole process from signal detection to action

All deviations present Warning Signals of unsafe or unreliable operation. Obviously, causes are not all deeply investigated for all reported deviations and, accordingly, there are also many Hidden Warning Signs which look "invisible", but still, all of them are producing Weak Signals that can be captured, modulated[22], amplified and treated (Fig 6). Fortunately, all conditions are kept in a Reporting System database and could be assessed any time and analysed by some additional assessment processes.

Typically, Common Cause and Trend analyses (IAEA, 2012) use CAP database for later identification and assessment of latent deviations. Furthermore, there are other processes like Focused Self Assessments (Stručić et al., 2006) or Peer Reviews

[22] *Note that "Modulation" of signal in this metaphorical model is mainly used in sense of transforming EWS to the factual "signals" – Cause or Probable Cause's Effect – input to "Amplifier" module (6.5.1).*

that always look in CAP for analysis inputs. Correctly performed, all these assessment tools would reveal hidden signals and find solutions for each. Together with use of Root Cause Analysis tools, they should bring to light all Warning Signals and their causes that can be efficiently treated to prevent recurrence of events or occurrence of similar events, and their escalation into accident.

Therefore, Weak or Hidden Warning Signals can be and should be visualized to the level where effective corrective actions can be easily defined and implemented.

6.5.1 Amplification

Corrective Action Program (IAEA, 2005) or any other similar approach that requires further processing of internally reported deviations, events and Near Misses is intended to correct their causes. Depending on the Organisation's policy and procedures, screening process usually results in Direct Action, request for Apparent or Root Cause analysis, or just report closure without corrective actions. Whatever is the outcome of screening, it is necessary to optimise resources and ensure that all information is preserved for later use. Fear of "feeding the beast" with a large amount of reported items should be alleviated through policy, to support a strong reporting culture. In the case that the reported item is not immediately fully processed, i.e. the report is closed, it can be managed in another self-assessment process such as Performance Indicators program or Common Cause analysis to assess the causes of reported deviations.

In any case, each revealed "Cause", which produced, contributed or might produce an undesirable Effect, is a Warning Signal too. The same "Cause" could be also the Weak or Hidden Warning Signal of deeper problem inside the Organisation. Therefore, it should be amplified to become widely visible and manageable.

Figure 7 presents the process of amplification of this deficiency signal, i.e. cause. Each signal (cause) should be tested for necessity of deeper investigation. That is usually true for direct causes, which if corrected will not necessarily prevent reoccurrence of the event or creation of a bigger accident (Ziedelis and Noel, 2011). Thus, it would be necessary to investigate it and find deeper cause, i.e. to find why this cause existed. This cause, in this metaphorical model, is processed as effect of deeper cause. Note that C/E (Cause/Effect) converter is used for this transformation.

Hence, a "signal" is "amplified" through the "Amplifier" module, i.e. investigated one level deeper to define the immediate cause of this effect. The new cause is tested if it is deep enough and manageable by Organisation (Roed–Larsen et al. 2005). If not, it should be investigated further. After some iteration, Deepest Manageable Cause is defined as final output of the Amplifier Module. This process reveals "invisible and unknown" facts, which are basically unrecorded deviations of the Organisation. Note that this iteration process can go in many directions: from finding specific cause that could be eliminated with surgical precision, to discovering generic problems that need a more comprehensive action plan.

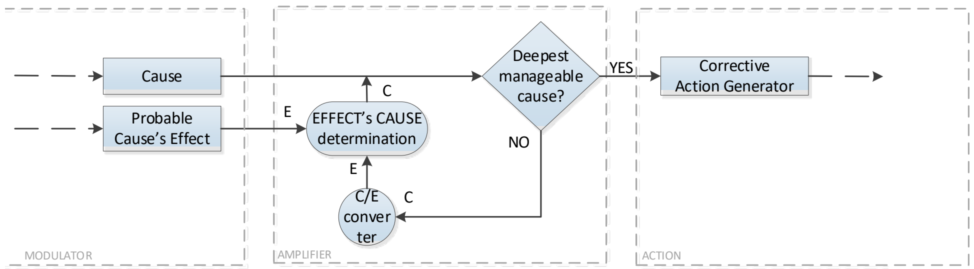


Figure 7, Amplification of Weak or Hidden Warning Signals

In addition to different types of "Causes", such as Root Cause, Direct Cause, Apparent Cause or Contributing Cause, it is important to recognise the Probable Cause too (fig 2 and 4). Many times, guided by Cause Analysis procedure, and requested by authority or required by legal requirements, some Facts are not required to be deeper examined although they are indicating existence of other important causes. Although not investigated yet, it can be assumed by our best judgement why these Facts exist. Since these causes are not proved, we can call them Probable Causes (Stručić, 2017). In figure 7, a Fact generated by a Possible Cause is presented as an Effect. Needless to say this Effect is a Warning Signal too. It is also important to note that the module, which processes other causes, processes Probable Cause too, but since it is just assumed, one step back is needed to extract its Effect and process it through an "Amplifier".

6.5.2 Elements of Amplifier

The purpose of good event analysis is to prevent recurrence of event i.e. to find the proper cause and enable its elimination. Therefore, the question "Deepest Manageable Cause?" is used in subchapter 6.5.1 to emphasise the main characteristic of the hunted cause - it examines the cause and compares the implied action based on that cause to the ability of the Organisation to efficiently implement that specific action. If this action is too demanding: e.g. exceeding the Organisation's resources; cannot be arranged due to external subject's unavailability or just missing external approval, then the corresponding cause should be further examined. Furthermore, the same should be done to "Shallow" causes which produce work requests usually "just to fix the problem" (Ziedelis 2014).

To examine or re-examine cause, the other fictional element "Cause/Effect converter" (C/E) is used to transform cause into effect. Since every cause is an effect of another deeper cause, investigating a "new" effect should result in a new finding which represents the deeper cause of an examined deviation. Deeper cause emphasizes the nature of the weaker cause and should easily prescribe appropriate action. If not, the process of "amplification" has to be repeated.

For Effect's Cause determination, it is essential to determine why the effect occurred which is done by use of different RCA tools (Ziedelis and Noel 2011). To simplify the approach, 5-Why's RCA tool could be used as good example. Thus, Effect's Cause element provides answer to question "what is the cause of this effect?" i.e. "Why does this effect exist?". In this illustration, the Amplifications Module should be used five times to get the positive passage through "Deepest Manageable Cause?" element.

Some critics emphasize the weakness of 5-Why's tool mainly because one "Why's" wrong answer could mislead investigator. To avoid this trap, one can use the Five-by-Five tool principle (Bill-Willson Net, March 2019, www.bill-willson.net/b73) in which five questions are defined to help in defining the right answer to each Why:

- What is the proof that this cause exists?
- What is the proof that this cause led to the stated effect?
- What is the proof that this cause actually contributed to the analysed problem?
- Is anything else needed for the stated effect to occur?
- Can anything else lead to the stated effect?

The other trap is that one effect could have more causes. Thus, they should be considered too. This would add parallel amplification loops and amplify additional hidden deficiency signals of Organisation.

6.5.3 Actions

In plain language the results of Condition/Deviation Report assessments are well defined causes of registered deviations and adverse conditions. They present vulnerabilities of the assessed Organisation and should be eliminated.

Regardless of deepness of retrieved causes, they should be well defined. This means that they should provide important information necessary to define effective corrective actions. If they are properly defined, definition of actions should be unambiguous.

E.g. production process in one NPP was stopped for some days because of failure of one safety control electronic circuit board. Further investigation found that one electrolytic capacitor failed because of aging. Extended/deeper investigation revealed that this model of circuit board is used in several other applications and that the manufacturer discontinued production, so it was no longer possible to replace the electronic control circuit boards, but this was not the case for the capacitor. Thus, an action plan was made to replace the same model capacitors in all circuit boards.

Actions defined this way should be reasonable and achievable on time, i.e. manageable by the Organisation. Some operating Organisations set requirements for corrective actions that have to be respected in a more popular way. E.g. in Organisations that use SMART approach (Specific, Measurable, Achievable, Relevant, Timely), typically the Corrective Action Program process enables the launch of corrective action when confirmation of all these requirements are achieved. Since it based on a defined problem's cause, it is obvious that the cause has to be well defined.

Furthermore, the Organisation should be motivated to perform even deeper investigation, even though this can bring Organisation to situation where it is unable to perform corrective action because it could be beyond the power of the Organisation or because of lack of resources (Roed–Larsen et al., 2005). Nevertheless, knowing more about the background of the problem could be an asset in Foresight in Safety. E.g. after defining actions to replace all affected capacitors in the safety electronic boards (because of ageing and inability of manufacturer to re-produce the same type of electronic board), extended investigation might reveal that the manufacturer is experiencing a survival risk due to a superior competitor. This might be important information for the Organisation because of difficult troubleshooting of possible other equipment failures with equipment produced by the same manufacturer. Thus, this information is not crucial for immediate action plan, but might be critically important to possible future decisions and negotiations outside the Organisation.

6.6 Conclusion

To truly understand the problems in our operating Organisation, they should be visualised to the level of plain clearness. Tools and processes explained in this chapter can help to understand those problems deeply enough and enable visualisation of their weak and faulted roots. Only in this state of understanding, are we able to obtain good qualitative insight of our vulnerabilities. With the knowledge and experience of design and operations we will then get all necessary elements for smart decisions in fighting discovered weaknesses.

This chapter tried to explain how registered anomalies in operating Organisation should be processed to reveal deeper causes i.e. to visualise warning signals and provide a clear basis for definition of a corrective action plan. The four phases of visualisation process consist of Detection, Acquisition, Modulation and Amplification of warning signals. Naturally, output of this process becomes an input for determination and implementation of corrective actions process – typically called Corrective Action Program.

The presented work mechanism of fictional electronic device illustrates main elements of an efficient EWS treatment process in an operating Organisation. This can be developed in more details by adding additional electronic elements e.g. “Noise filter” or “Screener discriminator” etc. But the intention of this chapter is, at the first place, to give operating Organisations interested in continuous safety improvement an idea about an alternative approach in fighting the problems.

In the context of Foresight in Safety, revealing weak and hidden signals of decreased safety enables stakeholders to foresee potential safety consequences and initiate timely actions. Thus, visualisation of hidden and weak signals has an important role in predicting possible incidents and accidents. Nevertheless, deeper investigation of causes than needed for efficient action plan definition, can bring additional information to decision makers and enable them to use this extra knowledge in future decisions and negotiations.

6.7 References

Bach B., NENE conference 2007, Slovenia Corrective Action Program at the Krško NPP - Trending and Analysis of Minor Events

Bill-Willson Net, March 2019, www.bill-willson.net/b73

Brainyquote.com, March 2020, https://www.brainyquote.com/quotes/humphrey_bogart_108860

ESReDA, 2015, A Case study analysis on dynamic learning from accidents — The ESReDA Cube, a method and metaphor for exploring a learning space for safety

International Atomic Energy Agency, 1997, Procedures for self-assessment of operational safety, IAEA-TECDOC-954

International Atomic Energy Agency, 2005, Effective corrective actions to enhance operational safety of nuclear installations, IAEA-TECDOC-1458

International Atomic Energy Agency, 2006, Application for Management System for Facilities and Activities, IAEA GS-G-3.1

International Atomic Energy Agency, 2012, Low Level Event and Near Miss Process for Nuclear Power Plants: Best Practices, SAFETY REPORT SERIES No. 73

International Atomic Energy Agency, 2013, Periodic Safety Review for Nuclear Power Plants for protecting people and the environment, IAEA No. SSG-25

International Atomic Energy Agency, 2014, Precursor analyses — The use of deterministic and PSA based methods in the event investigation process at nuclear power plants, IAEA-TECDOC-1417

International Atomic Energy Agency, 2015, Root Cause Analysis Following an Event at a Nuclear Installation: Reference Manual, IAEA TECDOC No. 1756

International Atomic Energy Agency, 2018, Operating Experience Feedback for Nuclear Installations, IAEA Safety Guide SSG-50,

International Atomic Energy Agency, March 2020, https://nucleus.iaea.org

International Atomic Energy Agency, November 2002, Self-assessment of Safety Culture in nuclear installations - Highlights and good practices, IAEA-TECDOC-1321

International Atomic Energy Agency, November 2006, Fundamental Safety Principles, IAEA Safety Standard No SF-1

Reason J., 1998, Achieving a safe culture: An International Journal of Work, Health & Organisations, Theory and practice, Pages 293-306

Roed–Larsen S., Stoop J.A., Funnemark E., Bolt E., 2005, Shaping public safety investigations of accidents in Europe, ISBN: 82-5150304-3

Strucic M., 53rd ESReDA Seminar, Ispra, Italy, November 2017, Use of Event and Causal Factor Short Cart Reports to Assess and Simplify Accident Reports

Stručić M., European Commission 2016, European Clearinghouse topical report: Events related to design deficiency, PUBSY No.: 105232

Strucic M., Kavsek D., Novak J., Dudas M., 6th International Conference on Nuclear Option in Countries with Small Grid, Dubrovnik 2006, Self-Assessment at Krško Nuclear Power Plant

USA Nuclear Regulatory Commission, March 2020, https://www.nrc.gov/reading-rm/basic-ref/glossary/corrective-action-program.html

Ziedelis S., European Commission 2014, Organizational and Management-Related Aspects in Nuclear Event Analysis, Topical Operational Experience Report

Ziedelis S., Noel M., 2011, Application and Selection of Nuclear Event Investigation Methods, Tools and Techniques, Final Technical Report

Ziedelis S., Noel M., Technical Report European Commission 2011, Comparative Analysis of Nuclear Event Investigation Methods, Tools and Techniques, EUR 24757

This chapter is extracted from the final technical report of the ESReDA Project Group *Foresight in Safety*. The full report is freely downloadable from the ESReDA web site and from the EU Joint Research Centre publications repository.

Bibliographic identifiers for the full report are indicated below.

PDF	ISBN	978-92-76-25189-7	ISSN	1831-9424	doi: 10.2760/814452	KJ-NA-30441-EN-N
Print	ISBN	978-92-76-25188-0	ISSN	1018-5593	doi: 10.2760/382517	KJ-NA-30441-EN-C

How to **cite this report**: ESReDA Project Group Foresight in Safety, *Enhancing Safety: The Challenge of Foresight*, EUR 30441 EN, Publications Office of the European Union, Luxembourg, 2020. ISBN 978-92-76-25189-7, doi: 10.2760/814452, JRC122252.

"Enhancing Safety: The Challenge of Foresight"

Edited by the ESReDA Project Group *Foresight in Safety*.

ESReDA
European Safety, Reliability & Data Association