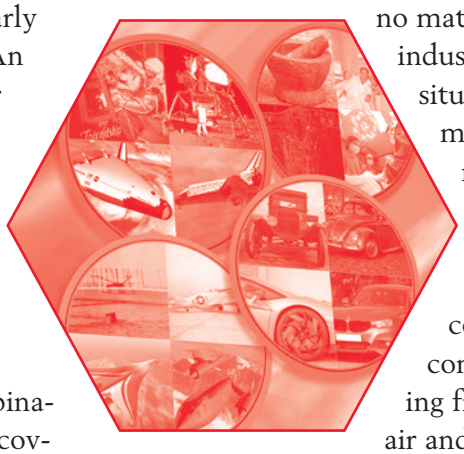
Disaster Prevention Through Intelligent Monitoring

by Dr. A.D. Painting (Attis Engineering Solutions Ltd) and Dr. D. Sanders (University of Portsmouth)

Despite various tools and systems that can monitor complex engineering environments, bad things still happen regularly in all types of engineering industries. An intelligent system designed to monitor certain indicators, regardless of engineering industry, that might predict catastrophes would ultimately reduce the potential for loss of human life and property.



In this article, 10 catastrophes were researched to identify their root causes and the various root cause combinations. These documented catastrophes covered a broad spectrum of engineering including oil, gas, nuclear, rail, air and space. The root causes identified in the investigation reports were grouped under 10 trait headings and their efficacy was tested using a qualitative fault tree of a credible catastrophic failure scenario. Each trait was adjusted to signify various levels of failure and fed into the prototype system representing the fault tree.

While near real-time monitoring and trend analysis was investigated and shown to support an intelligent system that might predict catastrophe, one of the surprising additional results from the research was highlighting the need to standardize the approach to investigative reports and audits of existing systems. Reporting in the same "technical language" and looking for specific condition levels for each of the traits could provide a true picture of asset condition and the required funding prioritization, as well as assisting the dissemination of findings to all engineering industries.

Introduction

Previous work [Ref. 1] highlighted several possible areas to investigate further, specifically the design and use of an intelligent monitoring system based on the measurement of common traits associated with catastrophes [Ref. 2].

Despite various tools and systems that can monitor complex engineering environments, bad things happen regularly in all types of engineering industries. An intelligent system that could monitor certain indicators no matter the complexity of the engineering industry, and could predict the potential situations that may lead to catastrophic mishaps, and could reduce loss of human life and property.

Ten high-profile catastrophes were researched to identify their root causes and the various root cause combinations These catastrophes encompassed a broad spectrum of engineering fields including oil, gas, nuclear, rail, air and space. The results demonstrated that each of the catastrophic mishaps was attributed to a combination of several minor failures. There were no examples of catastrophes occurring due to single-point failures.

The research set out to capture all the failure types and to simplify the list into a manageable number that could be readily monitored in any engineering industry.

The intelligent system was tested using a relatively simple fault tree representing a plausible catastrophic mishap in a maritime infrastructure environment. This led to some surprising results and byproducts to the initial research intention.

The choice of catastrophic disasters included five from the oil and gas industry and five disparate disasters. All of the disasters were well defined and fully investigated, providing the appropriate level of detail for the research. The choice consisted of:

- BP Texas City [Ref. 3]
- Piper Alpha [Ref. 4]
- Buncefield [Ref. 5]
- Texaco Refinery [Ref. 6]
- BP Deepwater Horizon [Ref. 7]
- Bhopal [Ref. 8]
- Chernobyl [Ref. 9]
- Challenger [Ref. 10]
- Royal Air Force Nimrod XV230 [Ref. 11]
- King's Cross Underground Fire [Ref. 12]

The development and testing of an intelligent monitoring system involved three main phases: the identification of common trait headings that would be applicable to all mishaps, the testing of a design based on a suitable root cause analysis tool, and various methods that could be used to provide a rudimentary predictive capability.

Common Traits

The identification of common traits attributable to catastrophes involved the selection and research of the 10 catastrophic mishap investigation reports to identify the various root cause categories and combinations that led to each disaster. A total of 21 common root causes, occurring in various combinations, were associated with the 10 disasters. When these results were compared with the findings of research undertaken by the U.K. Health and Safety Executive (HSE) into 36 U.K. and international mishap case studies [Ref. 13], a total of 56 root cause headings were identified. In order to set up a monitoring system to measure these root causes, the number of headings had to be reduced to a manageable size. This was achieved using six headings already identified by the HSE in *HSG 254 - Developing Process Safety Indicators* document as high-risk areas [Ref. 14], and four additional engineering management headings that summarized the remaining ungrouped failure types. This resulted in a total of 10 trait headings:

- HSG254 Headings:
  - Plant change
  - Inspections and maintenance
  - Staff competence
  - Operating procedures
  - Emergency arrangement procedures
  - Permits to work

- Engineering Management Headings:
  - Safety management systems
  - Maintaining design intent
  - Product safety hazards
  - Finance

The grouping considered the full investigation description of each root cause rather than just the root cause title, due to some identified ambiguities and the initial 56 root causes were grouped under the 10 trait headings [Figure 1]. The full justification for the grouping of traits is captured in Ref. 15.

Intelligent Monitoring

To develop the intelligent monitoring system, it was first necessary to identify a root cause analysis tool that could be adapted to suit complex environments for the majority of, if not all, engineering industries. Several analysis tools were investigated and the most appropriate method to identify all events and sub-events that could lead to a catastrophe was identified as qualitative Fault Tree Analysis (FTA).

A qualitative fault tree was developed with the plausible catastrophic disaster of "Dry Dock (Lock) Failure" as the top event. While this was a simple representation, the need to overlay 10 traits per sub-event became too complex. So, instead of tracking 10 traits for each sub-event, they were summed together as a single "state" condition. The "state" was derived from individual trait weightings based on the significance of each trait, as identified in the grouping of the 56 root causes. This ensured that each trait had a relevant contribution to the single "state" condition for each sub-event.

The use of weightings to capture the overall trait state was acceptable when looking for slight variations or deviations in trait levels, but if a trait were to suddenly drop into a "fail" state, the significance of this instantaneous failure should override all other inputs to drive a suitable response to make the situation "Safe." This was achieved using a simple Boolean logic "if" statement. The prototype monitoring system was then tested using scenarios that included the deteriorating conditions of various trait headings over a 10-week period. A scenario representing a "Fail" condition for three traits: Staff competence, Operating procedures and Permits to work, for both Lock Drainage A and B Valves led to a "Fail" condition for "Lock Catastrophic Failure" [see Figure 2 showing a "Fail" conditions in red]. An occasional override condition of failure was tested at opportune moments to ensure that this Boolean function would drive the correct response and not get lost in the data being recorded.

As the scenario of sub-event "states" slowly deteriorated and as sudden failures were introduced, the fault tree highlighted these failures immediately, proving the combination and weightings of the 10 traits, as well as the override functions within the Boolean statements.

Predictive Capability

To provide advanced warning of impending disaster, there is a requirement to forecast the condition for

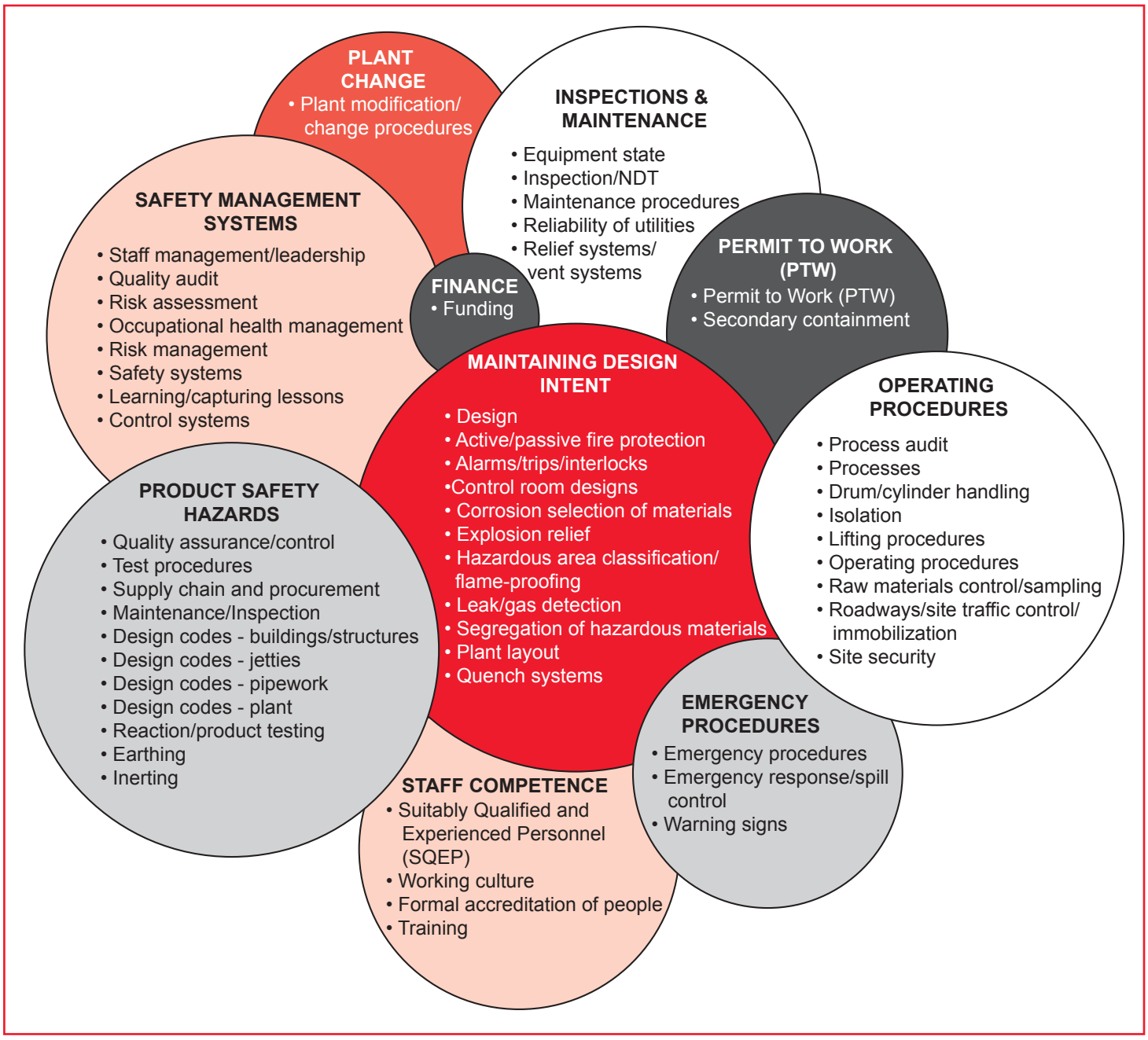


Figure 1 — Alignment with the 10 Trait Headings.

each trait several weeks into the future, based on the trend analysis of historic data. Several existing methods and toolsets provide trend analysis and prediction, including various database programs, Visual Basic (VB) programming and neural networks using data-mining software. All three of these methods were tested for simplicity of design, ease of build, user friendliness and accuracy of prediction. The research decided that simplicity to build was more important than accuracy, and so a Microsoft Excel database was chosen for the built-in straight-line trend analysis function and graphical representation.

Several trait value ranges were tested over a period of four weeks to test the accuracy of the prediction. Out of the set scenarios, some proved to be more accurate than others and the research concluded that a neural network based system would provide more accurate predictions [see Figure 3's example of a linear drop].

Trait Criteria Selection

For the initial stages of the research, the trait condition was identified as a number between "0 = Fail" and "9 = Good," with "3" or below indicating a "Fail" condition, "6" and above indicating a "Good" condition and everything in between signifying a "Warning" condition. To standardize the measurement approach for all sub-event traits, there was a requirement to set scoring

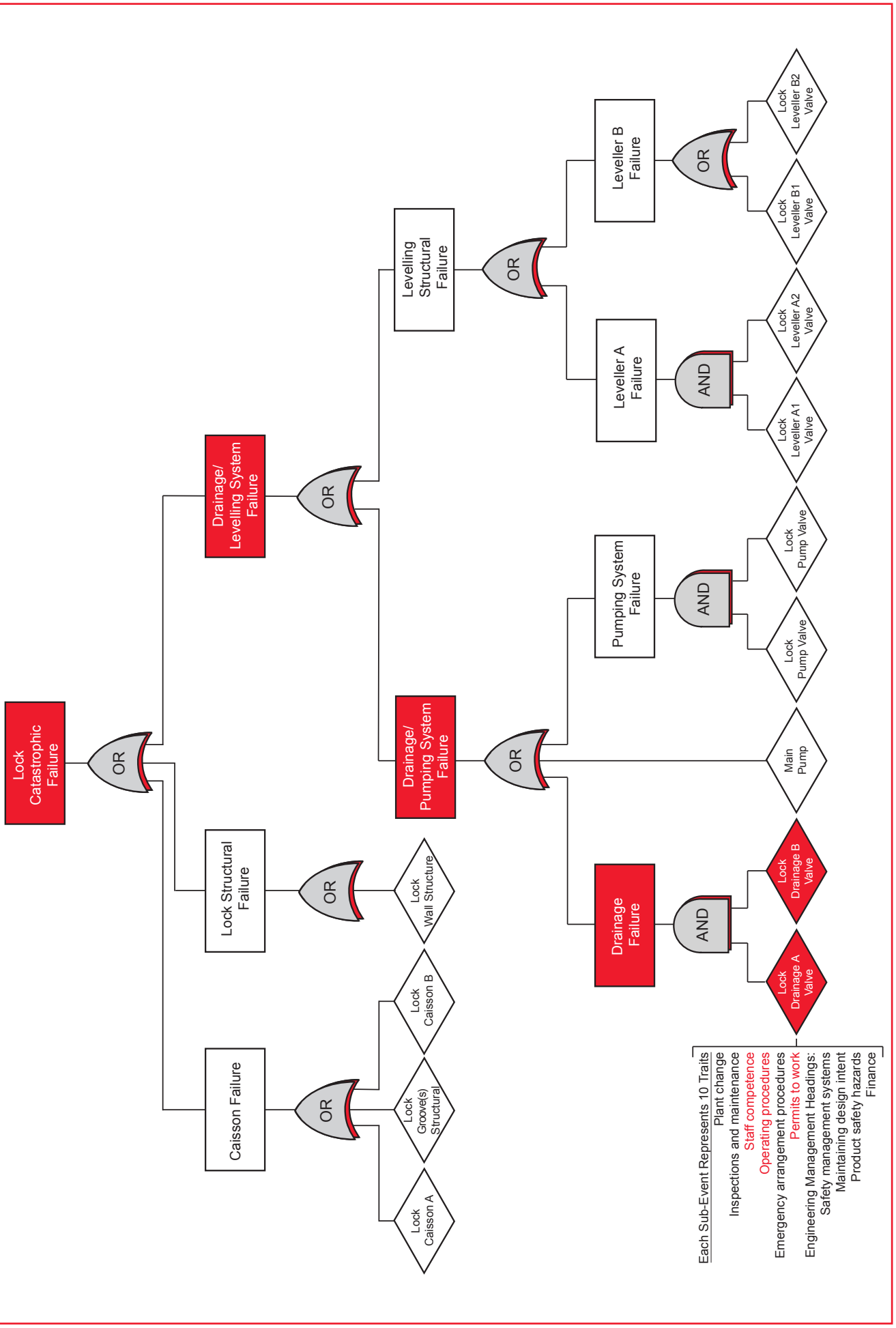


Figure 2 — Prototype Monitoring System.

principles. Therefore, a scoring criterion was developed for each of the 10 traits to ensure that the measured condition was both accurate and repeatable and that the data gained could be transferred to all engineering products, services and/or systems. The boundaries between "Good," "Warning" and "Fail" were chosen to signify the levels at which there would be a minor recoverable effect on the operational capability and the point at which there was no longer an operational capability [Table 1].

While the detailed scoring was appropriate for maritime engineering, using language, indicators and abbreviations relevant only to that environment, the principle behind the scoring could be transferable to any industry, with a small amount of tailoring to industry type.

Conclusions

The wealth of available catastrophic mishap investigations carried out by institutions and government bodies, such as the United Kingdom's Health and Safety Executive (HSE) and the United States' Chemical Safety Board (CSB), ensured an unbiased capture of the root causes associated with the 10 disasters discussed here. The investigations demonstrated several different processes used in the identification of root causes, and while each investigation identified root causes under various headings, they all confirmed that none of the disasters were caused by a single specific act or failure.

The research found several intelligent systems, such as condition-based monitoring systems, that captured fluid, vibration, light, heat and noise levels, as well as how these measurements provided warnings when compared against specific tolerances. However, there was no evidence of any research covering intelligent monitoring systems that specifically considered the measurement of common traits and overlaid this measurement onto a fault tree representing a catastrophic event.

While there was an abundance of information on the catastrophes, each investigation seemed to involve different techniques and question sets. There was no evidence of a consistent reporting format. One of the surprising consequences of this research found that a standardized approach to the investigation of disasters, based on a specific set of trait headings, would provide uniform findings in a format that could be compared to

Asset Information	State	Plant Change	Inspections and Maintenance	Staff Competence	Operating Procedures	Emergency Procedures	Permits to Work	Safety Management Systems	Maintaining Design Intent	Product Safety Hazards	Finance
Week 1	8	8	7	7	8	9	8	7	9	8	9
Week 2	8	8	7	6	8	9	8	7	9	8	9
Week 3	8	8	7	5	8	9	8	7	9	8	9
Week 4	7	8	7	4	8	9	8	7	9	8	9
Week 5	3	8	7	3	8	9	8	7	9	8	9

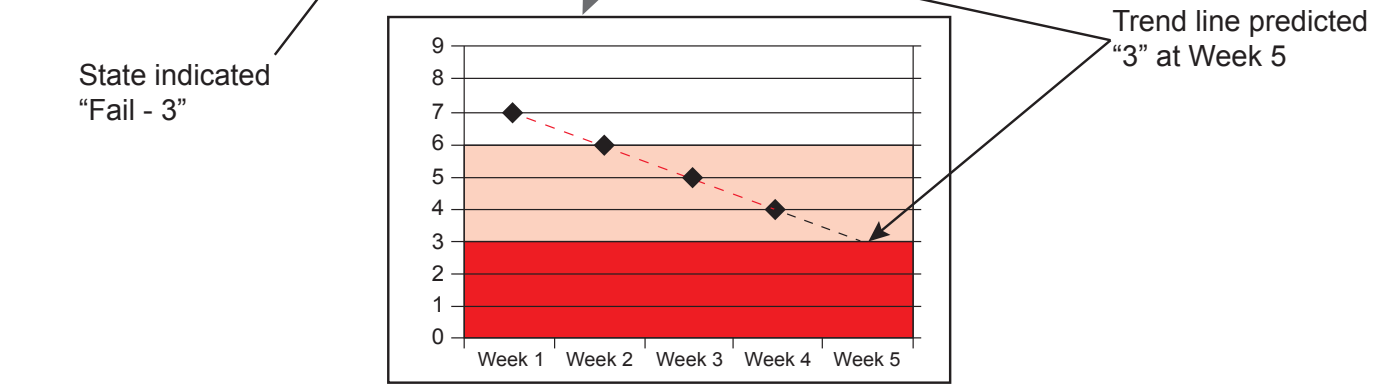


Figure 3 — Trend Analysis Inputs and Output.

Table 1 — Traits Boundary Conditions.

Traits	Boundaries	
	"Good" and "Warning"	**"Warning" and "Fail"**
Plant Change	The condition of the asset (sub-event) being considered that would not adversely affect the operational requirements of the business.	The condition of high-impact assets (sub-events) that would affect the operational effectiveness of the business.
Inspections and Maintenance	The reduced level of maintenance and inspections that would not adversely affect the business due to built-in redundancy and the ability to hire in equipment if operational requirements demand.	The reduced level of maintenance and inspection that would have a detrimental effect on the operational effectiveness of the business.
Staff Competence	The reduced level of staff competence that would not adversely affect the day-to-day operation of the business.	The minimum staff competence level that would have a detrimental effect on the operational effectiveness of the business.
Operating Procedures	The reduced level of suitable operating procedures that would not adversely affect the day-to-day operation of the business.	The reduced level of operating procedures that would have a detrimental effect on the operational effectiveness of the business, due to a lack of ability to undertake critical procedures.
Emergency Procedures	The minimum level of practiced emergency procedures that would not adversely affect the day-to-day operation of the business.	The level of practiced emergency procedures that would have a detrimental effect on the operational effectiveness of the business, due to loss of ability to undertake critical procedures safely.
Permits to Work	The restricted capability of "permit to work" system that would not adversely affect the day-to-day operation of the business.	An identified "permit to work" system failure that would have a detrimental effect on the operational effectiveness of the business, through loss of ability to undertake critical operationally essential procedures.
Safety Management Systems	A small number of safety management system issues that would not adversely affect the day-to-day operation of the business.	The level of safety management system failures that would have a detrimental effect on the operational effectiveness of the business, due to the loss of ability to manage critical operations.
Maintaining Design Intent	The minimum level of available design information that would not adversely affect the day-to-day operation of the business.	The level and impact of reduced design information and auditable documentation that would have a detrimental effect on the operational effectiveness of the business.
Product Safety Hazards	A small number of product safety hazards that would not adversely affect the day-to-day operation of the business.	The level and complexity of product safety hazards that would have a detrimental effect on the operational effectiveness of the business.
Finance	The level of reduced funding that would not adversely affect the day-to-day operation of the business. Possibly some minor mitigations and/or systems out of service.	The level of funding deficit and systems with reduced or no capability that will have a detrimental effect on the operational effectiveness of the business.

other disasters across all types of engineering industry. This, in turn, would ensure that any guidance from government and professional bodies, if produced in a standardized reporting format, could be targeted at specific industries more appropriately and effectively.

The research of predictive tools identified various techniques that could be employed to predict the future state of a system, based on the trend analysis of historic data and using formulas to calculate the next expected value on a graph or table. Although the use of trend analysis to predict the probability of future states within systems was common, there was no evidence of trend analysis being applied to a system that monitored traits in order to identify patterns that might indicate the potential of a catastrophic mishap.

While the tests and the scoring were specific to the maritime engineering industry, the naming of the 10 traits and the principle of monitoring these traits could easily be transferable to all high-risk operations in all engineering industries, including oil, gas, nuclear, rail, air, space and maritime engineering.

Ultimately, if the funds are not available to install an intelligent monitoring system to predict potential catastrophic mishaps, all is not lost. A temporary solution using a standardised question set, covering the 10 trait headings and agreed boundaries between "Good," "Warning" and "fail," would ensure that the business was made aware of any issues and had enough warning to prioritize effort in reducing the risk.

If investigations used the same heading criteria to capture root causes, these could be readily disseminated to all industries in a format that would assist safety engineers and safety professionals to take actions to ensure similar failures would not happen to them. This advanced knowledge would allow businesses to prioritize funding based upon the levels of risk.

A last word from the authors: Identify an area within your industry, score each of the 10 traits using the coarse measurement of "Good," "Warning" and "Fail," and see what the exercise tells you about the potential for failure.

About the Authors

Dr. Andrew Painting is the Director of the Attis Engineering Solutions Ltd. safety engineering consultancy and a Fellow of the Safety and Reliability Society. He spent 11 years before that working within Portsmouth dockyard, initially leading a team of safety engineers and finally as the Chief Engineer for the Naval base. Prior to that, he spent 23 years as a submariner in the Royal Navy. After 18 years of hands-on engineering, he started his academic training with a BSc in mechatronics and artificial intelligence, then earned an MSc in occupational and environmental health and safety management. Finally, he was awarded a Ph.D. for the design of "An Intelligent Monitoring System to Predict Catastrophic Incidents."

Dr. David Sanders leads the Systems Engineering Research Group and is the Engineering Research Degrees Coordinator at the University of Portsmouth. He is a Fellow of the Institution of Mechanical Engineers, Institution of Engineering Technology and the Higher Education Academy. His areas of research within the systems engineering research group include automation and robotics, computing and electronics, and environmental systems."

References

1. Painting, A. D. *Engineering Governance Model & Monitoring System Report*. Fleet Support Limited (FSL) Technical Services, Portsmouth, 2008.
2. Painting, A. D., and D. Sanders. "Engineering Governance through the Provision of Intelligent Monitoring Systems," *Journal of System Safety*, Vol. 47, No. 1 (2011):15-21.
3. Baker, J. A., N. Leveson, F.L. Bowman, S. Priest, G. Erwin, I. Rosenthal, S. Gorton, P. Tebo, D. Hendershot, D. Wiegmann and L. Duane Wilson. *The Report of the BP U.S. Refineries Independent Safety Review Panel*, 2007.
4 . Cullen, T. *The Public Inquiry Into the Piper Alpha Disaster*, HM Stationary Office, 1990.
5. Buncefield Major Incident Investigation Board. *The Buncefield Incident - The Final Report of the Major Incident Investigation Board (Vol. 1)*. Crown Copyright, 2008.
6. Health and Safety Executive. *The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July, 1994*. Crown Copyright, 1997, retrieved December 19, 2012, from www.icheme.org/communities/special-interest-groups.
7. Oil Spill Commission. *BP Deepwater Horizon Oil Spill and Offshore Drilling*, 2011. Retrieved October 20, 2011 from www.oilspillcommission.gov.
8. Rosencranz, A. "Bhopal, Transnational Corporations, and Hazardous Technologies," *Ambio*, Vol. 17, No. 5 (1998): 336-341.

9. World Nuclear Association. *Chernobyl Accident 1986*, retrieved May 10, 2012 from world-nuclear.org/info/chernobyl/inf07.html.
10. National Aeronautics and Space Administration (NASA). *Report of the Presidential Commission on the Space Shuttle Challenger Accident*, 1986, retrieved January 28, 2013 from science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html.
11. Haddon-Cave, C. *The Nimrod Review*, The Stationary Office, London, 2009, retrieved November 14, 2010.
12. Fennell, D. *Investigation into the King's Cross Underground Fire*. The Stationary Office Books, London, 1988, retrieved February 4, 2013, from www.railwaysarchive.co.uk/documents/DoT_KX1987.pdf
13. U.K. Health and Safety Executive (HSE). *Case Studies, 2004*. Retrieved March 24, 2012, from www.hse.gov.uk/comah/sragtech/casestudyind.htm.
14. U.K. Health and Safety Executive (HSE). *HSG 254 Developing Process Safety Indicators,* Crown Copyright, 2006.
15. Painting, A. D. *An Intelligent Monitoring System to Predict Potential Catastrophic Incidents.* University of Portsmouth, Portsmouth, U.K., 2014.