ENGINEERS AUSTRALIA

# OPPORTUNITY

**QUARTERLY NEWSLETTER** - April 2020 Vol 5. Issue 1

## In This Issue


| | |
|---|---|
| From the Editor's desk | 1 |
| Changes in IEC 61511-1 Ed 2 | 2 |
| Covid-19 Bowtie | 2 |
| The Safety Valve and Murphy's Law | 3-4 |
| Technical Sessions | 5 |


## From the Editor's Desk

Since our last newsletter the Covid-19 lockdown has had a significant impact on how we communicate with each other. Meetings using video telephony technologies have recently become far more common. Some RES chapters have been organising webinars for quite a while and others are just beginning to offer this type of service. Keep a look out for these in the weekly EA event alerts at https://www.engineersaustralia.org.au/Conferences-And-Events

There are also interesting discussions and event announcements in the Risk Engineering Society's LinkedIn group. At the moment, not surprisingly, many of the discussions centre on the issue of the impact of the corona virus on the industries where we work, or where we would be working if we were not in lockdown mode. Please sign up to this discussion group so that you are kept informed and contribute. If you have a LinkedIn account you can access the group at https://www.linkedin.com/groups/3751665/

In this newsletter Raj Sreenevasan from WA summarises changes made from edition 1 to edition 2 of the standard IEC 61511-1 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements. We have included links to a novel Risk Management Bow Tie for analysing some Covid-19 risks from the CCPS and Energy Institute. Derek Viner has provided the next instalment of his Safety Valve series of articles. We also include summaries of technical events held by a couple of chapters.

We hope you enjoy the newsletter. Please send articles of around 600 words for the next edition and also any comments you may have about current risk engineering issues where you work, live or visit. In the next issue we are particularly keen to include articles about managing risks for engineering projects and operations during the Covid-19 crisis. Case studies would be great! You can send your submissions to the joint editors Kevin Foster kevinjfoster@bigpond.com and Bronwyn Brookman Smith bronwyn@riskconsult.com.au

Kevin

RES is a Technical Society of Engineers Australia.

For Engineers Australia members, please remember to nominate your membership of RES when you renew your membership. NB: Non EA members can also join RES.

RISK ENGINEERING SOCIETY

# Safety Update

## Changes in IEC 61511-1 Ed 2

Many of you will be aware of the significant differences between Editions 1.0 and 2.0 of IEC 61511-1. Like you, I have followed the changes and implemented IEC 61511-1 Ed 2 clauses for safety instrumented systems. Whilst Ed 2.0 has not yet been published as a standard by IEC, the secretariat did a commendable job in publishing a Technical report (IEC 61511-4:2020).

In Australia we have adopted IEC 61511-1 Ed 2.0 (RLV) (Red Line Version) as our standard (AS IEC 61511-1:2018). Unlike other jurisdictions, Australian gas regulations (AS 3814:2018 Commercial Gas Fired Appliances) references the AS IEC 61511-1:2018 and hence it becomes mandatory to abide by the standard. It is no longer a ”recognized and generally accepted good engineering practice”

Because of this unique regulatory relationship, I have provided my interpretation of the changes. However, thes new 45 page technical report makes it easy to understand rationale behind the changes.

In summary, Ed 1 addressed the requirements relating to avoidance and control of systematic errors that occurred during design and engineering of independent safety functions up to SIL 3. Ed 2 addresses current practice of sharing automation system across multiple safety functions. It also provides guidance on how to avoid misinterpreting Ed 1 requirements, focusing design efforts on holistic functional safety management rather than limiting the efforts to calculations.

https://www.linkedin.com/posts/raj-sreenevasan-00061270_iec-61511-42020-activity-6648564348216188928-zgMf

Raj Sreenevasan

**Additional Resources on the changes**

Exida has released a webinar on the differences:

https://www.exida.com/Webinars/Recordings/iec-61511-whats-new-in-edition-two

Technical papers and presentations are also available:

https://www.icheme.org/media/11752/hazards-26-paper-15-iec-61511-functional-safety-in-the-process-industry-the-long-awaited-iec-61511-edition-2-and-what-it-means-for-the-process-industry.pdf

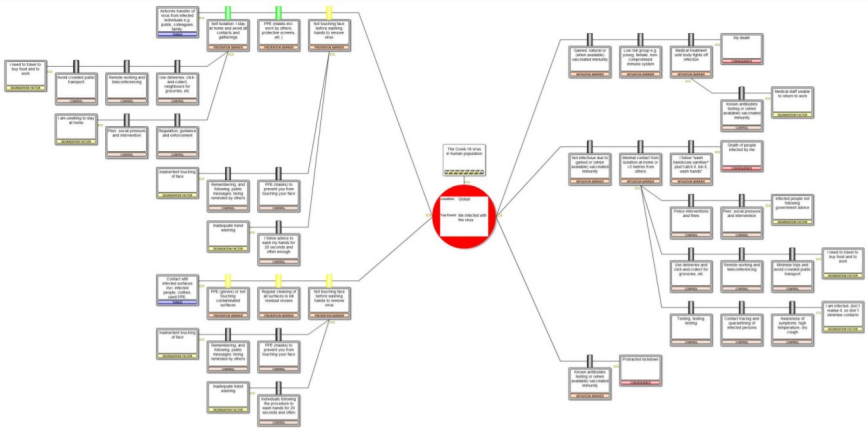
https://www.cheminst.ca/wp-content/uploads/2019/04/207-New-Updated-International-CSChE2017.pdf

## COVID-19 Bowties

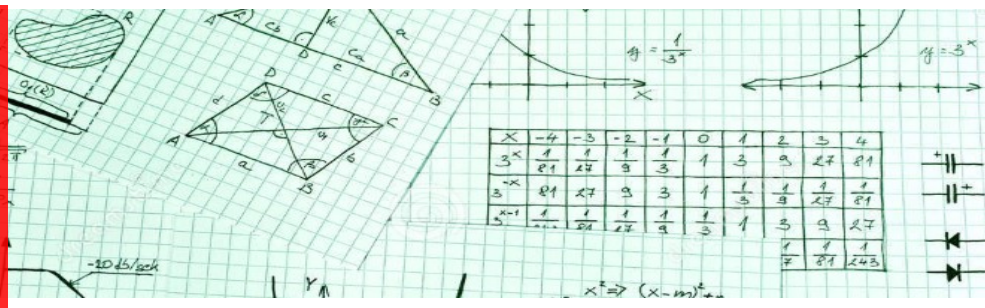
Bowties are becoming more prevalent as they visually depict the safeguards and barriers to prevent and mitigate an unwanted event.

The Centre for Chemical Process Safety (CCPS) and Energy Institute released “Bow Ties in Risk Management” in 2018. With the current Covid-19 situation, the books authors have released a monograph containing a bowtie for Covid-19.

https://www.aiche.org/sites/default/files/html/544481/BowTieforCOVID19-CCPSMonograph.html



# A Lesson for Engineers



## The Safety Valve and Murphy's Law

Since the founding of the RES (being one of those who called the Society's first meetings in the mid to late 1970s), I ponder how much progress has been made in developing and promoting the science and engineering of *risk* amongst the larger body of engineers. There are a few of us who regard ourselves as risk engineers, but I suspect there are very few engineers in more traditional fields of engineering (mining, chemical, civil, mechanical, electrical, structural, electronic, aeronautical) who have an improved understanding of risk, and the methods of risk engineering, as a result of the formation of a small specialist society such as ours.

There are however two fundamental aspects of risk, and its management, that are literally household words. One is the heading of my first article, the Safety Valve [Opportunity Vol 4 Issue 3 2019]. This small item of risk engineering would have come to prominence in the early days of steam and it remains in extended common use today - we talk of safety valves in social, psychological and political situations. So much so that we have almost forgotten its origin in stopping pressure vessels from exploding.

The second is good old Murphy's Law - *what can go wrong will* or variations on this. Wikipedia has a fascinating article on it, in which we read it could equally have come to be known as Strauss's law (US Atomic Energy Commission chairman - "If anything bad can happen, it probably will") or Reilly's law. Everyone knows it by the name of Captain Ed Murphy (an engineer working on research at what became the now famous US Edwards Airforce Base), originally reported as saying about someone: "if there is anyway to do it wrong, he will". The Wikipedia entry gives various versions of the law and even quotes a source that calls it the fourth law of Thermodynamics, probably tongue-in-cheek.

In other words, everybody at work, at home, amongst your friends, in the shops you visit, the aeroplanes in which you (used to) fly etc. know this adage and have no difficulty recalling or understanding it.

The saying is a statement of simple truth about the probability of things going wrong - if something is possible, then it is also probable (in the sense of having a probability associated with it). There are only two certain things in the world, death and taxes, so everything else we deal with is uncertain and hence subject to this simple principle. As engineers we are called on to design things to efficiently suit a required function, so it is natural for us to attend to what our designs are *intended* to do, often paying less attention to what they *could* do. The engineer must also attend to the adverse potential of their designs. This means risk engineering is something all designers should do and our role as professed risk engineers is to both promote the science and application of the subject and assist designers ourselves.

For example, when a vessel is pressurised there is a probability that the safety valve (SV) will fail to operate when called on to do so (SV failures per demand). If we include the probability of an overpressure situation arising (demands per pressurisation) and also the exposure (the number of times a year the vessel is pressurised, or the period of time in a year for which the vessel is pressurised) some very simple arithmetic allows us to calculate the frequency with which vessel overpressure is not relieved by the valve. The inverse of that of course is the Mean Time Between cases of unrelieved overpressure. The existing mathematics of reliability engineering is all we need to understand this.

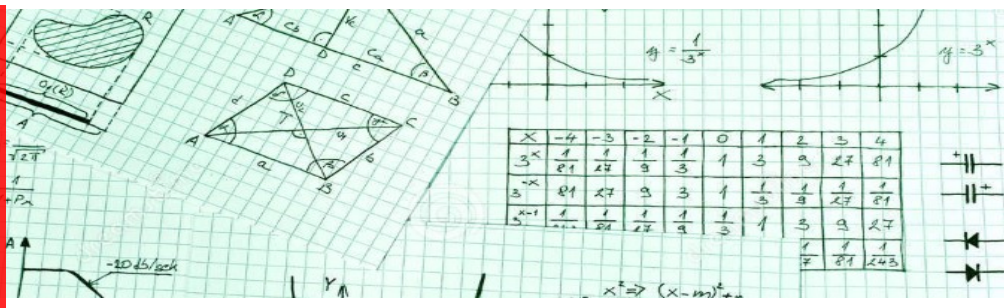
These calculations are useful in that they give the engineer a sense of perspective on the significance of the outcome when things go wrong, and make it possible to promote efficient control measures aimed at reducing the adverse effects, when it does happen.

The Time Sequence Model clearly and simply shows the logic of the process - there are reasons the *Event* can happen (called Event Mechanisms) and there are *Outcomes* after the *Event* has happened. As engineers we are mostly interested in the damaging potential of energy sources and the *Event* can be defined in this context - hence if an energy source exists it is only a matter of time before control over its damaging properties are lost and an *Outcome* with potential adverse *Consequence* occurs.

Logic, as well as moral duty, make it clear that the more extreme the Likely Worst Consequence of the *Outcome,* the more must be done to minimise this by controlling the *Outcome* process as well as directing it towards less damaging *Consequences*. Sometimes this means running around panicking and calling the emergency services, but the response should have been included in the design process and continue to be managed over the years in the operational phase.

The logic of this is not complex, so I'm sure you'll also feel frustration and curiosity when faced with reports of serious cases where this has not been taken into account in the system design. I'll mention three cases here. The first and last attracted a lot of publicity, the other comparatively little. The first case(s) really did kill a lot of people and happened in both 2015 and 2019. The second case nearly killed a lot of people. The third case killed two plane loads. There are relatively few examples (Exposure, maybe some hundreds) of the first case to be found in the world. The potential for (Exposure) in the second case exists one hundred thousand times every day and third case less than that as the case involves only one type of aircraft.

# A Lesson for Engineers



## The Safety Valve and Murphy's Law (cont.)

**First case: Tailings dam failures in Brazil.** https://www.youtube.com/watch?v=sKZUZQytads. Whether the actual 'cause' (i.e. Mechanism) of the failure (the Event) is known or not, what is known is that such dams do fail (https://en.wikipedia.org/wiki/List_of_tailings_dam_failures). There is also engineering knowledge of Mechanisms (https://www.hindawi.com/journals/ace/2019/4159306/).

It is clearly not fanciful to imagine such dam failures. What is perplexing is that the designers were content to design and build dams with outflow paths that could produce such destruction and that Governments were content to approve the designs.

As a quick web search will show, the costs to the communities, the environment and the companies involved were nothing short of spectacular. Or is this just that people, companies, Governments etc. can't think past what is intended to happen? What I find disturbing (and unhelpful) is the way Governments subsequently assume that they are innocent and that massive punishment of the operator by imposing huge fines will somehow solve the problem.

**Second case: An airliner almost failed to achieve take-off** from Melbourne airport (https://en.wikipedia.org/wiki/Emirates_Flight_407). The flight failed to achieve take-*off safety speed* at the point along the runway when it should have, resulting in the need to apply emergency thrust. Damage was done to approach path lighting structures at the end of the runway and the aeroplane itself.

The Event is something that is possible. It occurred when the engines were assumed to be at the required take-off thrust levels - full power take-off settings are an exception these days. The inadequacy of the thrust only became evident towards the end of the take-off run when an attempted rotation failed to produce sufficient lift to allow the aircraft to become airborne. This is well into the Outcome pathway and it was only then that the flight crew became aware of the problem. How did they become aware? By realising that rotation had not lifted the aircraft off the runway. This is seat-of-the-pants stuff (and the year was 2009 and the technology the pinnacle of mankind's capability). But this was not a unique case (https://www.avweb.com/flight-safety/technique/when-engine-instruments-lie/). In this story the Captain thought they should have been going faster by the time they passed the terminal building and applied maximum thrust in time. Also seat-of-the-pants stuff. Whilst not a pilot, it is perplexing that all cases of pilots monitoring take off performance are by setting a thrust level based on take-off performance charts, assuming they have done the sums or entered data correctly and that the engines are doing what they are expected to do etc.. Note that up to the Emirates case at Melbourne airport there was no independent monitoring of acceleration achieved vs expected. That is, no attention paid by aeronautical engineers to designing the Outcome pathway. This case made manufacturers begin to design monitoring systems to give the flight crew information about what was actually happening vs. what they hoped was happening on the take off run.

The Mechanism here was an error entering fuel weight data. In 1979 an error in entering route data led to the crash of an Air New Zealand aircraft into Mt Erebus with the loss of all on board. This involved the same Mechanism type (data entry error) but different circumstances, i.e. the same Occurrence Process, different conditions and circumstances.

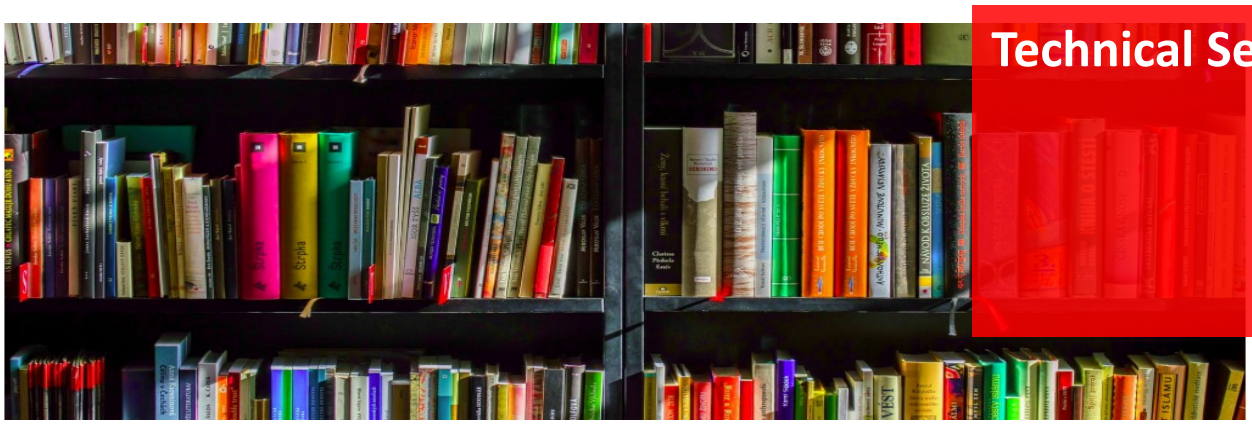
**Third case: Two Boeing 737Max cases of loss of control** and total loss. Following this in aviation newsletters, it appears that the plane relies on automated pitch control as the fundamental aerodynamics are unstable due to the relatively forward and upward location of the engines compared with the conventional underwing location. The conventional location maintains pitch stability while minimising the drag of the installation. The 737Max design incorporated unusual positioning, to allow bigger diameter engines on an old airframe.

The automated pitch control relies, not surprisingly, on input from an angle of attack sensor. Angle of attack is closely related to fuselage pitch angle. Curiously, it appears the engineers designed the system to use only one of these sensors for this purpose. If the sensor fails (for instance a bird strike on the sensor) there is no input to the pitch controller. A natural response of pilots to autopilot pitch control error is to turn off the pitch function of the autopilot, but in the case of the 737Max this presents them with an aeroplane inherently unstable in pitch. Nothing I have read to date suggests the design engineers had designed Outcome pathway control measures as a back up to this apparently very obvious and possible Mechanism.

I should conclude by saying that this is by no means the case in the design of chemical process plant, where overpressure, underflow, reverse flow etc. sensitive designs are made as a matter of course. Perhaps there are other fields of engineering where this is also true, but why not in all fields? Does our profession lack routinely applied principles of design? I suspect as a generalisation, engineers of many or most disciplines are not taught the science of risk.

Always remember Murphy!

Derek Viner



# Technical Sessions

## Risk Engineering Research

The RES Queensland Chapter held an event in November 2019 showcasing Risk Engineering in Research Projects. Three research higher degree candidates from the University of Queensland spoke on their research projects.

Jaime Cadena Gomez gave a presentation on “Fire risk assessment for the retrofit of a high-rise building with a façade”. He highlighted the possibility of up to ±3 orders of uncertainty in the assessment, and compared the alternative methods of either preparing a damage model leading to an assessment of the potential for major loss; or a method of setting a maximum allowable level of damage in a fire leading to estimates of the potential for “surprise” results. Conclusions were drawn regarding the need to use only non-combustible façade materials in high-rise buildings.

John Lee discussed “The use of dynamic models to improve process safety”. He pointed out that there are weaknesses in current hazard analysis and control methods and that there is a large number of new risk management methods available that have not yet been generally adopted. John introduced the concept of using dynamic models to identify hazards not found using more traditional methods, and the use of languages such as T in conjunction with ISO15926 for data integration and Industry 4.0 to develop and maintain a digital meta-twin of a process plant that can be used for hazard identification and analysis.

Kourosh Parsa spoke about ”Methods to evaluate alarm system design and to prioritise and rationalise alarms to increase operator situation awareness and assist operator decision-making”. This covered the relevance of alarm systems and the challenges relating to human reliability when faced with the huge increase in the number of alarms typically occurring during abnormal situations. He discussed factors involved in good (and bad) alarm design, and described a procedure and system that could be used to improve alarm systems.

## Have We Time To Save Our Way of Life

RESWA joined with Sustainable Engineering Society in hosting a session on the risks of Climate Change. Delivered by David Rice, based on presentations delivered at the World Engineering Convention in Melbourne in 2019. Considering options for industry moving forward, the basic theme is that the economy is the only force powerful enough to make good the current damage to the environment that will be essential if we are to save something like our current way of life. This focused on issues that engineers can do via project evaluation.

**RES National Committee**

Geoff Hurst (President)

David Cox (Treasurer and QLD)

Pedram Daneshmand (Deputy President and NSW)

Subhash Dang (ACT)

Timothy Rigby (Victoria)

Kevin Foster (WA)

Andrew Dakin (EA) provides advice to the committee