*The*
# Product Safety Engineering Newsletter

Vol. 10, No. 2 - June 2014

IEEE PSES Product Safety Engineering Society

## What's Inside



## President's Message

Hello Fellow PSES Members!

I was glad to see so many of you at the 2014 ISPCE; it turned out to be a great event. Please see the ISPCE Article in this issue of the *PSEN* for more.

In my last column, I focused on member involvement, and I want to share some additional thoughts on that. The symposium is a great example of the many levels from which members can choose to be involved—examples include a short term contribution to facilitate a session at the symposium, which takes about two hours, to a long term contribution serving on the Technical Program Committee, which involves a year-long commitment of a few hours per month. Without the help of all the members who volunteered, no matter what amount of help they individually provided, we couldn't have put on the symposium. There were a number of members (over 30, not counting presenters) who were able to attend and help out at the actual event as well as those who were unable to attend but helped with preparations for the event. I would like to again say thank you to all who helped in any way to make it one of the best symposia ever!

We are already starting preparations for the 2015 symposium, so if you would like to get involved in some way, no matter how much, even if it is to share an idea, please contact our 2015 ISPCE Chair, John Allen at Jrallen@productsafetyinc.com.

Also, as I mentioned in my last column, we will be trying different ways to reach out with opportunities to get involved. One thing we did differently at the 2014 ISPCE was to have a member information table near the entrance to the general assembly room. Not only did we have information there, but we had at least one of our Board members there most of the time to answer questions and encourage members to get more involved. As a result we did get a number of sign-ups for different activities, including helping to form a virtual Chapter of the PSES—more on that in a future column. We will be following up directly with those who signed up at the ISPCE.

Continued on Page 3

*The*
**Product Safety Engineering Newsletter**



# Newsletter Committee



# Officers of the IEEE PSES

**Executive Committee**

| | | |
|---|---|---|
| President | Kevin Ravo | (14-15) |
| Past President | Elya Joffe | (14-15) |
| President Elect | TBD | (15) |
| Secretary | Daniece Carpenter | (NA) |
| Treasurer | Jan Swart | (NA) |
| Vice President - Communications | Dan Roman | (11-13) |
| Vice President - Member Services | Thomas Ha | (11-13) |
| Vice President - Technical Activities | Ivan Vandewege | (11-13) |
| Vice President - Conferences | Doug Nix | (11-13) |

**Directors At Large**

| Term Expires 12/14 | Term Expires 12/15 | Term Expires 12/16 |
|---|---|---|
| Paul Wang | Bill Bisinius | Silvia Diaz Monnier |
| Mike Nicholls | Grant Schmidbauer | Stefan Mozar |
| Steli Loznen | Kevin Ravo | Mark Maynard |
| Juha Junkkarinen | Rich Nute | Jack Burns |

**Ex Officio (without vote)**

Gold Member: TBD
Chapter Chairs
Standing Committee Chairs
IEEE HQ
IEEE TAB Division VI Director

# IEEE PSES Web Sites

http://www.ieee-pses.org/
http://psessymposium.org/
http://product-compliance.oc.ieee.org/
http://www.ieee-pses.org/emc-pstc.html
http://www.ieee-pses.org/newsletters.html
http://www.ieee-pses.org/pses.html

Continued from Page 1

However, we can always use even more help, so watch for additional opportunities that will appear in the *PSEN* or on the PSES website, and give one a try!

Starting in the next and subsequent newsletters, I will be sharing with you a little about the various activities of each of the officers of the Society—particularly areas where you can get involved. Hopefully this will provide some more insight into the activities of the Board and some ideas of ways you could get involved. I have to say that it is great to see different members getting involved in our various activities since they typically bring new ideas and energy. Getting involved at different levels is not only a great way to support the society, but also a great way broaden your own professional network as you interact with others in the society that you might not already know.

Finally, as always if you have any thoughts about ways we can provide more value to our members, please share those directly with me or any of the other Board Members. Just taking a few minutes to compose an email with an idea might be all it takes to help us develop the next new way to deliver more value to our members. This is even yet another way to get involved by contributing your great ideas!

Sincerely,

Kevin Ravo

# Editor Wanted

*Gary Weidner, our editor since the beginning, would like to step down (or retire as it were). At last year's symposium he received a service award thanking him for his volunteer work as Editor of our Newsletter all these years. He will be missed. Gary prepared this job description as we look for someone to take the reins. -D.R.*

**Do You Have What it Takes to do This Job?**

I've been editing the current incarnation of the *Product Safety Engineering Newsletter* since the first issue appeared in the fourth quarter of 2005. I'd like to turn the position over to someone else, so a few thoughts are gathered here in order to convey what is involved. Hopefully I've been of some use, but there's something that's been gnawing at me ever since that first issue. Let me explain.

Few people outside the editing trade are aware of what a periodical publication editor does. The work involves two activities, described below. Both of the activities are necessary for a successful publication, and neither is sufficient by itself.

***Editing*—**Yes, editors edit. But "wordsmithing" is not something that one can simply decide to do and jump into it. My observations indicate that this poses a delicate problem in the engineering community because:

(a) It seems that most engineers consider themselves to be good written communicators.

(b) Experience in the publishing field and with *PSEN* indicates that most engineers do not write well, let alone edit the writings of others.

If you've been involved in writing or editing, words like "Strunk & White" or "Chicago Manual of Style" are probably familiar to you.

***Mining for content*—**The other half of a typical periodical editor's work (and *PSEN* is typical is this regard) is to locate useful and interesting content. Intuition would seem to indicate that an editor sifts through a stream of submitted articles, then edits the best for publication. Wrong. Most successful publications receive submitted articles, but not nearly enough to feed the issue-after-issue conveyor belt. Mining for content involves serious time and effort devoted to networking.

What's been gnawing at me is that I've not been able to devote anywhere near an appropriate amount of time, effort, and sometimes expense, to mining for *PSEN* content. Our newsletter needs someone with demonstrable writing and editing skills who can also commit to mining for content. If that's true for you and you would like to investigate the *PSEN* Editor position, contact Dan Roman, VP-Communications, at dan.roman@ieee.org.

# Chapter and TAC Safety Probes

**To see current chapter information and people looking to start chapters please go to the Chapter page at: http://www.ieee-pses.org/Chapters/index.html**

**Technical Activity Committee information can be found at: http://www.ieee-pses.org/technical.html**

## Central Texas Chapter

Meeting Date: 4/15/2014

Topic: " How Wearable Electronics Intersect with 'The Cloud' and Internet of Things"

Speaker: Joseph Wei, Senior IEEE Member, founder of SJW Consulting, Inc.

Meeting opened with general announcements. As Mr. Wei had already been patiently waiting on the phone for several minutes his presentation began immediately afterwards. He covered many facets of wearable technology, including the various uses seen today and where it may possibly be headed in the future. During the presentation he answered several questions about the effects of securing all this additional data and commented on the legal ramifications. We all shared some laughs as some of the potential uses seemed rather strange in light of what is available today. After ending his presentation he took several questions from the group and explained some of the terminology used when presenting the topic.

## Information Technology TAC

The IT TAC has 17 active members and meets for one hour every month by teleconference to discuss technical items of interest to our members. Current topics include the status of the new IT safety standard IEC 62368-1, issues with India certifications, and changes to IEC standards that may have impact to IT products. Persons wishing to join this TAC should contact Gary Schrempp at gary_schrempp@dell.com.

## Forensics and Failure Analysis TAC

-The Forensics and Failure Analysis Technical Committee (FFATC) is considering a name change to simply “Failure Analysis Technical Committee” (FATC).

-The FFATC is working on updating its website under the PSES site.

-We are actively recruiting technical papers for next year’s symposium in Chicago, IL. Please consider sharing your interesting and unusual observations and findings from your failure analyses! The deadline for Paper and Presentation Submission: December 15, 2014. So plenty of time for reflection on your experiences to share!

-We encourage professionals with an interest in failure analysis to join the leadership of this technical committee. Please contact Daren Slee on our Linkedin group “Forensics and Failure Analysis” under the PSES if you would like to contribute! Along these lines, the discussion had at May’s symposium in San Jose amongst the leadership of the TCs and Local Chapters of the PSES was productive for seeding ideas for the Society moving forward. One of these was encouraging Local Chapters to reach out to the TCs for content for their meetings. It would also be helpful if Local Chapter members could join one or more TCs along their lines of interest (including FA) to pump the cross-production between the Chapters and TCs.

-Please keep in mind that our primary purpose as the PSES is “Product Safety”, not necessarily electrical safety. So keep those ideas involving

Continued on Page 7

## Seeking Collaborators

Looking for volunteers to create a spreadsheet with the world wide requirements for electronic products. The intent would be to have it broken up by industrial verses consumer, appliance verses ITE, and any other classes of devices. The list would include WEEE, RoHS, REACH, Safety, EMC and so on. As the IEEE PSES now has a number of members in a lot of countries, it is something we should be able to put together. If you think this is a good idea and would like to be part of the task group please drop me an email at: j.bacher@ieee.org.

Continued from Page 5

product safety rolling in, even without an electrical component.

-Recruit members of your contact list to present Webinars hosted by the FFATC. Again, contact Daren Slee if you'd like to present on a topic. Presentations can be advertised on our Linkedin group. This is an opportunity to warm up potential technical paper topics!

## Telecom Safety TAC

Don Gies attended the US TAG Meeting in San Jose, CA 12-16 May 2014. The IEEE TSTC proposal on battery cabinet ventilation, amended per recommendations from US TAG Meeting in Melbourne, FL, was accepted in principle at MT2 Meeting for IEC 60950-22, Second Edition. The proposal for Clause 11 of IEC 60950-22, Second Edition is to refer compliance to IEC 62368-1, Annex M, which in turn will be modified in accordance with the proposal. This way, criteria will apply to both indoor and outdoor equipment, as well as be documented in an active standard going forward. There will be a requirement for vent holes. For boost charge the holes need to be 8x larger than for float. IEC 60940-22 will point to IEC 62368-1 Annex M for the procedure on how to do the test. Added a 1.5 kV withstand for outside DC mains. Denmark asked for 2.5 kV, but that was rejected.

In the June TAC meeting Al Martin described protection of DC feeds to radio equipment at the top of towers.

a. What protection is typically installed on equipment that will be located at the top of towers, and is any consideration given to the height of the tower?

b. What lightning waveshape is considered when designing protection for equipment to be located at tower tops?

c. Is there any information about the failure of installed protection to protect equipment located at tower tops?

Joe Randolph was congratulated for his "Best Paper" Lightning Surge Damage to Ethernet and POTS Ports Connected to Inside Wiring at the ISPCE 2014 Conference in San Jose.

# Safety Principles

**Safety principles for system design and engineering products**[1]

*by Joseph Homer Saleh[2*] & Francesca M. Favarò*

**Introduction**

With the introduction of the IEC 62368 guide, product safety standards are undergoing a shift in perspective based on the establishment of Hazard-Based Safety Engineering (HBSE). This shift emphasizes the importance of safety in the early design stages through the identification of potentially hazardous energy sources, and the implementation of different types of safeguards designed to protect against, contain, or mitigate such hazards. HBSE principles rely on the idea that harm to humans/property is based on energy transfer mechanisms from the hazardous energy sources to these entities [IEC 62638-1]. The prevention of such transfers through the establishment of safeguards helps ensure the safety of the product (and its handling). As such, one of the pillars of HBSE and the new product safety standards is in the idea of safeguards and their use against hazardous energy sources.

It is interesting to note that this energy basis of injury has a long tradition in epidemiology: it was first advocated by Gibson [1964] and it became a pillar of the epidemiology of injury prevention with the work of Haddon [1980]:

"*Man…responds to the flux of energies which surround him…mechanical, thermal, and chemical. Some limited fields and ranges of energy produce stimuli for the sense organs; others induce physiological adjustments; still others produce injuries. …Injuries to a living organism can be produced only by some energy interchange*." [Gibson, 1964]

Haddon expanded on this energy basis of injuries, and he devised the safety strategies that are intrinsically related to this perspective:

"*A major class of [adverse] phenomena involves the transfer of energy in such ways and amounts, and at such rapid rates that inanimate and animate structures are damaged. The harmful interactions with people and properties of…projectiles, moving vehicles, ionizing radiation, conflagrations…illustrate this class of phenomena*." [Haddon, 1980]

This energy model of accident and injury led Haddon to propose a set of safety strategies to guide the development of injury control mechanisms and safety interventions (e.g., reduce the amount of hazard/energy brought into being in the first place; reduce the rate of release of energy; separate in time and space energy source from vulnerable items and individuals; etc.; more details in [Saleh et al., 2014a]). In short, the foundation of the new IEC 62368 Standard resides in part in this Gibson/Haddon energy model of injury.

---

[1] This work is an abridged and modified version of an article published by the authors in the *Journal of Loss Prevention in the Process Industries*, 29 (2014) 283–294 and titled, "System safety principles: A multidisciplinary engineering perspective".

[2] [*] Corresponding author

Continued on Page 9

Continued from Page 8
Moreover the idea of safeguards in HBSE and IEC 62368 is related to the notion of safety barriers and defense-in-depth, a safety principle first conceived of in the nuclear industry in the 1950s and later adopted under various names in other hazardous industries. Defense-in-depth, as we will discuss shortly, consists in the design and implementation of multiple safety barriers, technical, procedural, and organizational, whose objectives are first to prevent accident initiating events from occurring, second to block accident sequences from escalating, and third to mitigate adverse consequences of the accident—an uncontrolled release of energy—should the previous barriers fail.

The purpose of this brief starter is first to recognize the intellectual debt that HBSE and the IEC 62368 Standard owe to both the Gibson/Haddon energy model of injury and the safety principle of defense-in-depth. Second, it is meant to invite more cross-talk between the different communities of system safety professionals, injury epidemiologists, and product safety professionals, as there are many synergies between their respective areas of interests, and the tools and frameworks in one area may be helpful in another. An interdisciplinary dialog between these different safety communities can enrich the perspectives of everyone involved, and ultimately it will further advance the common safety agenda and our shared end-objective, which is to help build a safer society, whether in the workplace, during commute, at home, or while handling any engineering product.

Going back to the idea of safety principles, while in the past we resorted to a proliferation of detailed safety measures (tactics) in specific areas and industries, today's tendency strives to define high-level safety principles or strategies that are independent of particular instantiations, and from which specific safety measures can be derived and adapted to a particular context or hazard. The HBSE process for example illustrates this shift in perspective, moving from prescriptive detailed rules to general models of safety (and accident occurrence). There are several system safety principles, in addition to the one leveraged in the HBSE and IEC 62368 Standard. These principles are framed at a high level of abstraction, and we believe they ought to be intrinsic to the intellectual toolkit of any safety professional. In the following sections, we introduce a set of five safety principles: (1) the fail-safe principle; (2) the safety margins principle; (3) the un-graduated response principle; (4) the defense-in-depth principle; and (5) the observability-in-depth principle. These principles can fulfill an important role in safety training and education, and they ought to be carefully considered in any design endeavor before they are ruled out if not applicable. All these safety margins principles can also be implemented in a variety of ways, and they require creativity and technical ingenuity to conceive and design in different contexts and for handling different types of hazards.

**System Safety Principles**

The safety principles that follow are related to the notions of hazard level and hazard escalation. In a system context, the first notion reflects the extent of energy involved and the closeness of an accident to being released—closeness in both a temporal and causal sense [Saleh et al., 2014a]. The second notion of hazard escalation introduces a dynamics to the problem and reflects whether an accident sequence has further advanced, was blocked, or was de-escalated. The further an accident sequence has advanced for a given energy source, the more hazardous the situation is.

***The Fail-Safe Principle***

The fail-safe principle imposes, or is defined by, one particular solution to the problem of how a local failure affects the system hazard level. Consider a function performed or implemented by a particular component in a system. The failure of this component or termination of its function can propagate and affect the system in different ways. For example it can lead to a cascading failure (domino

Continued on Page 10

Continued from Page 9

effect), which would result in a complete system failure or accident (e.g., nodes in an electric power grids operating at maximum capacity). It can also remain confined to the neighborhood of the failed component and hence have a limited impact at the system hazard level. Specifically, the fail-safe principle requires that the failure of an item in a system or termination of its function should result in operational conditions that (i) block an accident sequence from further advancing, and/or (ii) freeze the dynamics of hazard escalation in the system, thus preventing potential harm or damage (Figure 1). Conversely, if the fail-safe principle is not implemented, the component's failure would aggravate a situation by further escalating the hazard level, thus initiating an accident sequence or leading to an accident (Figure 1). This principle can be implemented in a variety of ways. For example, air brakes on trucks are maintained in the open position by pressure in the lines; should the pressure drop because of leakage or any other failure mechanism, the brakes will be applied. Another example of the implementation of the fail-safe principle is the "dead man's switch" for train operators: should they fall asleep or become unconscious, the device is no longer held down, and as a result the brakes are applied. More complex implementations of the fail-safe principle can be found in nuclear reactors where self-shutdown is initiated if critical operating conditions are reached. While there may be situations or items for which the fail-safe principle is incompatible with their design or is simply not implementable, it is nevertheless important that this principle always be considered and carefully assessed in any design endeavor before it is ruled out.

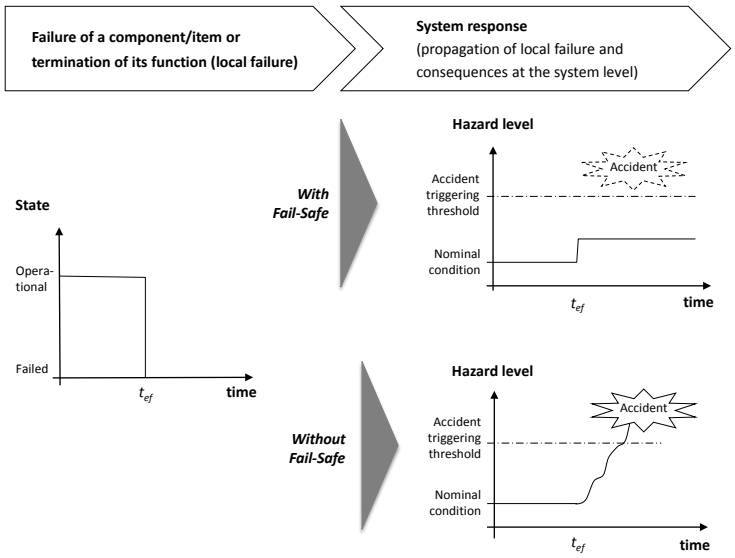



Figure 1: Illustrative comparison of system behavior over time following a local failure, both with the implementation of the fail-safe principle and without it ($t_{ef}$ is the time of occurrence of the failure of the component/function of interest)

### *The Safety Margins Principle*

The adoption of safety margins is a common practice in civil engineering where structures are designed with a safety factor to account for larger loads than what they are expected to sustain, or weaker structural strength than usual due to various uncertainties. The importance of safety margins for structures such as bridges and levees, which have to cope with the uncertainty of operational and environmental conditions such as wind force and wave height, is easy to understand. The idea of safety margins in civil engineering is an instantiation of a broader safety principle, which we refer to by the same name. The safety margin principle extends beyond civil engineering and is more diverse in its implementation than the particular form it takes for structures. It requires first an estimation of a critical hazard threshold for accident occurrence, and an understanding of the dynamics of hazard escalation in a particular situation. For example, methane in coalmines enters an "explosive range"

Continued on Page 11

Continued from Page 10

when its concentration in the mine atmosphere reaches between five and 15 percent [Saleh and Cummings, 2011]. Reaching the five percent threshold for example can be considered a critical hazard threshold in the mine. The safety margin principle requires that features be put in place to maintain the operational conditions and the associated hazard level at some "distance" away from the estimated critical hazard threshold or accident-triggering threshold (Figure 2). For instance, in the coal mine example, a safety margin can be established with respect to the risk of methane explosion by maintaining methane concentration below say three percent in the mine atmosphere, two percentage points below the critical hazard level. The difference between the operational upper limit (below three percent) and the boundary of the explosive range (five percent, the triggering threshold) is a particular form of safety margin in this context. Safety margins are one way for coping with uncertainties in both the critical hazard threshold and in our ability to estimate and manage the operational conditions in a system, such that their associated hazard level does not intersect with the real (but unknown) critical hazard threshold.

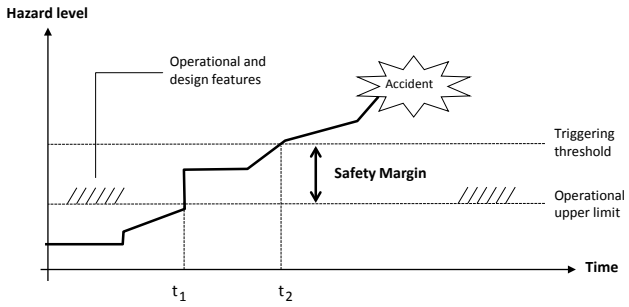



Figure 2: Illustration of the safety margins principle with a sample accident trajectory from a nominal operating condition to an accident. A larger margin makes it more likely that the system state will not reach the accident-triggering threshold, or that a longer time window is available to detect a system state that has crossed the operational upper limit (for nominal conditions) and abate the hazardous situation before an accident is triggered.

### *The Un-graduated Response Principle*

The use of force in a military or law enforcement context is governed by a set of rule whose principal tenet is that of a *graduated response*, namely that if force is deemed necessary, it ought to be applied gradually in relation to the extent of a demonstrated belligerence, as a last resort, and only the minimum force necessary to accomplish the mission should be used [CJCSI, 2005]. The opposite of this tenet holds for dealing with safety issues, and the corresponding principle we refer to as the un-graduated response or rules of engagements with technological hazards. This principle for accident prevention and mitigation articulates a hierarchy of preferences for safety interventions. It posits that the first course of action to explore for accident prevention is the possibility of eliminating a hazard all together. We refer to this course of action as "kill first" or the use creativity and technical ingenuity as a first resort to eliminate the hazard, regardless of the extent of its *belligerence* (use of lethal force against hazards). For example, if a heat source or electric wires are in the vicinity of flammable material, the hazard can be controlled or the probability of an accident reduced by using proper wire isolation and placing the wires within fireproof protective jackets. But this particular hazard, the co-location of the electric wires and flammable material, can be eliminated by re-routing the wires through another location—the preferred course of action by virtue of this safety principle.

Continued on Page 12

Continued from Page 11

If the hazard cannot be eliminated, the second course of action is to control it or reduce its likelihood of escalating into an accident. Figuratively, if "kill first" is not feasible, then proceed to "apprehend and (heavily) restrain". A third and concurrent course of action is to devise ways to mitigate the consequences or minimize the damage should the hazard escalate into an accident (Figure 3). Similar preferences are also included in the HBSE process for the design of safeguards, where the hierarchy of protection should be first to eliminate the hazard, then guard against it, and finally warn about it and rely on personal responsibility for avoidance [Lanzisero, 2010]. As with the previous safety principle, all these courses of action can be achieved in a number of ways. The efficiency of each mean ought to be examined, and its cost and benefit carefully assessed to guide decision-making with respect to the implementation of this principle.

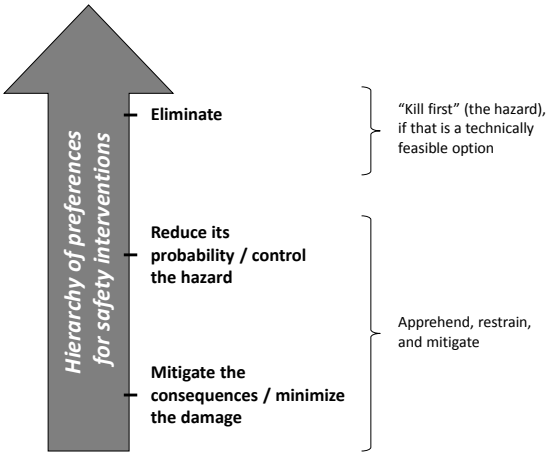



Figure 3: Illustration of the hierarchy of preferences for safety interventions by virtue of the un-graduated response principle

### *The Defense-in-Depth Principle*

Defense-in-depth derives from a long tradition in warfare by virtue of which important positions were protected by multiple lines of defenses (e.g., moat, outer wall, inner wall). As noted in the Introduction, defense-in-depth was first conceptualized in the nuclear industry, and it is adopted under various names in other industries. Defense-in-depth has several foundational pillars: (i) multiple lines of defenses or safety barriers should be placed along potential accident sequences; (ii) safety should not rely on a single defensive element (hence the "depth" qualifier in defense-in-depth); (iii) the successive barriers should be diverse in nature and include technical, operational, and organizational safety barriers. In other words, defense-in-depth should not be conceived of as implemented only through physical defenses.

The various safety barriers have different objectives and perform different functions. The first set of barriers, or line of defense, is meant to prevent an accident sequence from initiating. Should this first line of defense fail in its prevention function, a second set of safety defenses should be in place to block the accident sequence from further escalating. Finally should the first and second lines of defense fail, a third set of safety defenses should be in place to contain the accident and mitigate its consequences. This third line of defense is designed and put in place based on the assumption that the accident will occur, but its potential adverse consequences should be minimized. These three lines of defenses constitute defense-in-depth and its three functions, namely prevention, blocking

Continued on Page 13

Continued from Page 12
further hazardous escalation, and containing the damage or mitigating the potential consequences (Figure 4). Accidents typically result from the absence, inadequacy, or breach of defenses. The notion of a safety barrier is the embodiment of the "defense" part of defense-in-depth in the sense that defenses are realized through barriers deliberately inserted along potential accident sequences and prior to their initiating events. It can be seen that the previous safety principles overlap to some extent with defense-in-depth. For example, the implementation of a fail-safe mechanism, or the establishment of a safety margin, can be considered as different forms of barriers in the layout of defense-in-depth. And the un-graduated response principle reflects to some extent the different functions of the multiple lines of defenses (their "depthness"). Indeed the safety principles are not mutually exclusive, and this overlap is useful, as it provides us with an opportunity to emphasize certain foundational ideas in system safety and the need to include them in safety training and education.

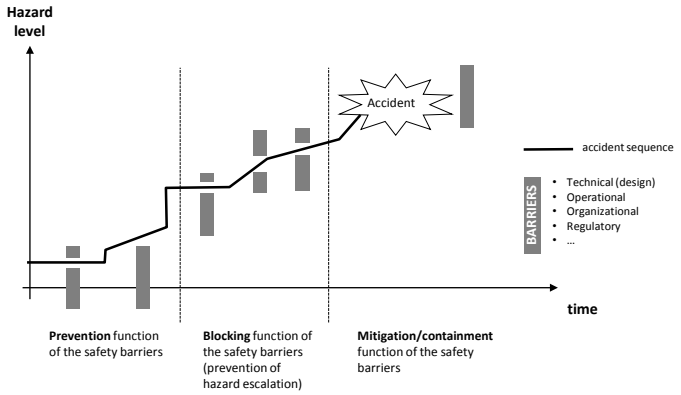



Figure 4: Illustration of the defense-in-depth safety principle, along with a hypothetical accident sequence

### *The Observability-in-Depth Principle*

Observability-in-depth plays a distinctive role in system safety, and it contributes to accident prevention in a fundamentally different way than the previous principles. This principle does not affect or intervene directly in an accident sequence, but it scans and monitors for hazard escalation and advancement of accident sequences in real-time, bringing an online mindset (i.e., during system operation) to accident prevention. Its significance is best motivated by considering situations in which this principle is NOT implemented. Violations of the observability-in-depth principle highlight not the causal chain of an accident sequence—why the accident happened—but the causal factors that failed to support accident prevention—why blocking the accident sequence did not happen. There are several mechanisms in the design of complex systems that can contribute to concealing the occurrence of hazardous events (e.g., redundant component failures or build-up of latent failures) and the transition of the system to an increasingly hazardous state, which make "systems more…opaque to the people who manage and operate them" [Reason, 1997]. As a result, system operators may be left blind to the possibility that hazard escalation is occurring, thus decreasing their situational awareness and shortening the time they have to intervene before an accident is released.

Operators make decisions during system operation, which are based on and affect the hazard level in a system. If the system conditions/states are not carefully monitored and reliably reported, there

Continued on Page 14

Continued from Page 13

is a distinct possibility that the hazard level *estimated* by the operators will diverge from the *actual* hazard level reached by the system (Figure 5). The gap between these two quantities can result in the operators making flawed decisions, which in turn can compromise the safe operation of the system or fail to check the escalation of an accident sequence (e.g., no action when an intervention is warranted; see for instance [Saleh et al., 2014b]). Observability-in-depth is characterized by the set of provisions, technical and operational, designed to enable the monitoring and identification of emerging hazardous conditions and accident pathogens. It requires that all safety-degrading events or states that safety barriers are meant to protect against be observable. This implies that various features be put in place to observe and monitor for the system state and breaches of any safety barrier, reliably providing this feedback to the operators. Observability-in-depth seeks (i) to minimize the gap between the actual and the estimated hazard levels, and (ii) to ensure that at the hazard levels associated with the breaching of various safety barriers, these two quantities coincide (i.e. no line of defense should conceal the fact that the system has breached any other safety barrier and has reached a hazardous state the engineers and system designers meant to protect against). The "depth" qualifier in observability-in-depth has both a causal and a temporal dimension, and it characterizes the ability to identify adverse states and conditions far upstream (early) in an accident sequence. It reflects the ability to observe emerging accident pathogens and latent failures before their effect becomes manifest on the system's output or behavior, or before an increasingly hazardous transition occurs in an accident sequence.

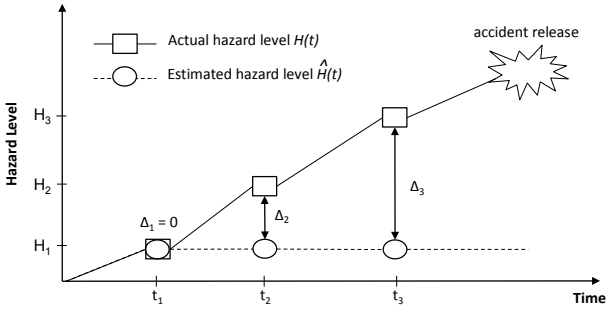



Figure 5: Hazard escalation over time and the violation of the observability-in-depth principle. The figure shows how underestimating the actual hazard level (ovals) can lead to an accident occurring seemingly without warning (rectangles). The gap between the these two quantities (Δ) represents a loss of situational awareness [Saleh et al., 2014b].

It is worth clarifying that observability-in-depth is an important complement to defense-in-depth: the former prevents the latter from devolve into a defense-blind safety strategy, and the latter (along with risk analysis tools), guides the establishment of provisions for monitoring safety functions and barriers. It introduces an online (real-time) mindset into risk analysis and management, and it supports the development of a "living" or online quantitative risk assessment. In short, observability-in-depth can help conceive of a dynamic defense-in-depth safety strategy in which some defensive resources, safety barriers and others, are prioritized and allocated dynamically in response to emerging risks.

Continued on Page 14

Continued from Page 14

## Conclusion

The high-level system safety principles discussed in this work are domain-independent, technologically agnostic, and broadly applicable across industries. Although this set of five safety principles is not meant to be exhaustive, we believe most detailed safety measures (tactics) derive from or relate to these principles. The translation of these safety principles into specific design features and safety measures requires detailed knowledge of the system under consideration, as well as creativity and technical ingenuity to conceive and implement in various context and for handling different risks.

We hope this work serves an educational role, for example in safety training. We believe these principles are a useful addition to the intellectual toolkit of engineers, decision-makers, and anyone interested in safety issues, and they can provide helpful guidelines during system design and risk management efforts. We also hope that this work invites more cross-talk between the different communities of system safety professionals, injury epidemiologists, and product safety professionals. An interdisciplinary dialog between these different safety communities, as noted previously, can enrich the perspectives of everyone involved, and ultimately it will further advance the common safety agenda and our shared end-objective, which is to help build a safer society, whether in the workplace, during commute, at home, or while handling any engineering product.

*Joseph Homer Saleh (404-385-6711; e-mail: jsaleh@gatech.edu) and Francesca M. Favarò are with the School of Aerospace Engineering, Georgia Institute of Technology.*

*References*

International standard IEC 62638-1 – Audio/video, information and communication technology equipment – Part 1: Safety Requirements, Edition 2.0, 2014-02.

Gibson, J. J. (1964). "The contribution of experimental psychology to the formulation of the problem of safety brief for basic research" *In*: Haddon Jr, W, *et* al., (eds). Accident research: methods and approaches. Harper & Row, New York.

Haddon Jr, W. (1980). "Advances in the epidemiology of injuries as a basis for public policy." *Public Health Reports*, Vol. 95, Issue 5, pp. 411–421.

Saleh, J. H., Marais, K. B., Favarò, F. M. (2014a) "System safety principles: A multidisciplinary engineering perspective" Journal of Loss Prevention in the Process Industries, Vol. 29, pp. 283–294.

Saleh, J. H., and Cummings, A. M. (2011). "Safety in the mining industry and the unfinished legacy of mining accidents: Safety levers and defense-in-depth for addressing mining hazards". *Safety Science*, Vol. 49*,* Issue 6, pp. 764-777.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B (2005). "*Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces"*.

Lanzisero, T. (2010). "Applied Safety Science and Engineering Techniques (ASSET™): Taking HBSE to the next level". In *Product Compliance Engineering (ISPCE), 2010 IEEE Symposium,* pp. 1-6.

Continued on Page 17

# 2015 IEEE Symposium on Product Compliance Engineering

Sponsored by the IEEE Product Safety Engineering Society

May 18-20, 2015
Chicago, IL, USA
www.psessymposium.org

## Call for Papers, Workshops, and Tutorials

**ORGANIZERS**

**General Chair**
John Allen
Jrallen@productsafetyinc.com

**Technical Program Chair**
Tom Burke
thomas.m.burke@ieee.org

**Technical Program Co-Chair**
Dwayne Davis
dwayned@asresearch.com

**Conference Management**
Conference Catalysts, LLC

The IEEE Product Safety Engineering Society seeks original and unpublished papers, presentations, workshops and tutorials on all aspects of product safety and compliance engineering including, but not limited to:

**EMC Compliance**

- Electromagnetic emissions, electromagnetic immunity, regulatory, and introductory topics (for safety engineer & compliance engineers)

**Energy Storage**

- Battery and energy storage designs, applications, manufacturing, testing and standards, including emerging chemistries, fuel cells, electrochemical capacitors (ultra-and super-capacitors), etc.

**Forensics**

- The latest findings in failure analysis
- General tools, techniques and best practices used for quality failure analysis

**Hazard-based Safety Engineering & Safety Science**

- Theory and application of HBSE and related safety science disciplines
- New hazard-based standard for A/V, IT & Communication Technology Equipment, IEC 62368-1

**Innovation**

- Emerging uses of technology, and associated challenges with safety & compliance, such as associated with 'smart' devices, wearable electronics, wireless power transfer, driverless cars, modular data centers, 3D printing, liquid cooling, PEDs/aircraft, virtual reality, technology & seniors, unmanned aerial vehicles (UAVs, aka drones), etc.

**Leadership**

- Management strategies and techniques, and case studies
- Change leadership, team building, conflict resolution, time management
- Communication skills

**Medical Devices**

- IEC 60601-1, and collateral standards
- Risk Management process for medical devices

**Risk Analysis, Assessment & Management**

- Fundamentals and application of risk analysis, assessment and management, into both existing and new standards and applications

Continued from Page 15
Reason, J. T. (1997). “Managing the risks of organizational accidents”. Aldershot, Hants, England; Brookfield, Vt., USA: Ashgate.

Saleh, J. H., Haga, R. A., Favarò, F. M., Bakolas, E. (2014b). “Texas City Refinery Accident: Case Study in Breakdown of Defense-In-Depth and Violation of the Safety-Diagnosability Principle”. *Engineering Failure Analysis*, Vol. 36, pp. 121-133.

# Volunteer Positions Available

PSES members wanted to volunteer for small but important roles within the PSES organization. No in-person meetings required. E-mail and conference calls only. All it takes is a couple of hours a month to help improve and grow our organization.

- PSES Global Outreach Rep: Help establish the PSES Country Reps - the country reps will serve as a leader within each foreign country that currently has PSES members (make contact with our foreign membership). Work with the Chapter Coordinator to help the Country Reps start local chapters.
- PSES Strategic Partner Rep: Make contact with other societies and organizations that have Product Safety interest. Work to help integrate our safety content into their societies and organizations (i.e. PSES has partnered with the Consumer Electronics Society).
- PSES PR Rep: Prepare and issue press releases regarding our Symposium and other special events and activities. Invite news organizations and other interested parties to cover our events.
- PSES Marketing Team: Team members participate in plan review and refinement, and each member leads 1 item within the plan (work at your pace - pick an area that interests you - no marketing experience or background needed - many tasks are technically oriented that serve marketing purposes).

For more details, please contact Bill Bisenius at +1-919-469-9434.

We also are seeking volunteers for the Symposium Committee:

- Overall Planning Committee
- Technical Program Committee
- Marketing Committee
- Paper Presentations
- Local Symposium Support
- Session Moderators
- Track Chairs

See the Symposium website at: http://www.psessymposium.org/ or contact John Allen at Jrallen@productsafetyinc.com.

## Special Free Offer

Starting this past January, PSES members began receiving the award winning CE Magazine free of charge. CE Magazine is published by the IEEE Consumer Electronics Society and its mission is to educate, inform, and entertain members on technology, events, industry news, and general topics. This trial offer is for all of 2014.

The Product Safety Engineering Society and Consumer Electronics Society are considering an arrangement that would put feature technical articles relating to Product Safety and Compliance Engineering in CE Magazine. We would appreciate your feedback once you begin receiving the magazine. You can contact Dan Roman (dan.roman@ieee.org) or Kevin Ravo (Kevin.L.Ravo@ul.com).

## PSES Jobs Web Page

PSES has a web page for employers and job seekers at http://www.ieee-pses.org/jobs.html. Employers may post jobs seeking regulatory or compliance-related personnel free of charge. Job postings will remain on this web site for a period of 6 months but may be removed earlier by request of the employer.

Job postings **must** include the name and location of the employer and a method for an applicant to respond to the listing. We will **not** accept or post job listings from professional recruitment firms or job placement services working on behalf of a client that is not identified, and we will not include job listings for positions that require the candidate to pay a placement fee.

See http://www.ieee-pses.org/jobs.html for full posting policy and how to submit requests.

IEEE | PSES Product Safety Engineering Society

E-Mail List: http://www.ieee-pses.org/emc-pstc.html
Virtual Community: http://product-compliance.oc.ieee.org/
Symposium: http://psessymposium.org/

Membership: The society ID for renewal or application is "043-0431".

## *Advantages of Membership in the IEEE PSES*

*Makes you part of a community where you will:*

- Network with technical experts at local events and industry conferences.
- Receive discounts on Society conferences and symposiums registration fees.
- Participate in education and career development.
- Address product safety engineering as an applied science.
- Have access to a virtual community forum for safety engineers and technical professionals.
- Promotion and coordination of Product Safety Engineering activities with multiple IEEE Societies.
- Provide outreach to interested engineers, students and professionals.
- Have access to Society Publications.

# News and Notes

## *Compliance News Shorts*

June, 2014

***EU – New Radio Equipment directive (RED)***

Replacing the current Directive 1999/5/EC, R&TTE Directive, a new Radio Equipment Directive (RED), Directive 2014/53/EU, was published on April 16, 2014. This directive will be applicable from June 13, 2016.

A copy of the Directive is available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_153_R_0002&from=EN%20

More information is available at http://ec.europa.eu/enterprise/sectors/rtte/documents/legislation/review/index_en.htm

**Vietnam – New Technical Standards**

Implemented on January 15, 2014, Vietnam's Type Approval Authority MIC (Ministry of Information and Communication) new Technical Regulations replace standards which impact RFID/SRD devices and radars previously approved under QCVN47:2011. A summary of the new standards in blue which replaces standard QCVN47:2011follows.

| No | Device name | Before 15-Jan-14 | After 15-Jan-14 |
|---|---|---|---|
| 1 | Wireless radio equipment using frequency modulation (FM) frequency band from 54MHz to 68 MHz | QCVN47:2011/BTTTT | QCVN70:2013/BTTTT |
| 2 | Radio equipment operating on 25MHz – 1GHz | QCVN18:2010/BTTTT<br>QCVN47:2011/BTTTT | QCVN18:2010/BTTTT<br>QCVN73:2013/BTTTT |
| 3 | Radio equipment operating on 1GHz – 40GHz | QCVN18:2010/BTTTT<br>QCVN47:2011/BTTTT | QCVN18:2010/BTTTT<br>QCVN74:2013/BTTTT |
| 4 | Data transmission equipment for low speed 5.8GHz specially used in the field of transportation | QCVN18:2010/BTTTT<br>QCVN47:2011/BTTTT | QCVN18:2010/BTTTT<br>QCVN75:2013/BTTTT |
| 5 | Data transmission equipment for high speed 5.8GHz specially used in the field of transportation | QCVN18:2010/BTTTT<br>QCVN47:2011/BTTTT | QCVN18:2010/BTTTT<br>QCVN76:2013/BTTTT |

***USA – FDA Draft Guidance on Social Media***

The FDA has published a Draft Guidance on how pharmaceutical companies should message on platforms such as Twitter.

Today, the FDA carefully controls the messaging for drugs requiring FDA clearance including labeling, advertisement and promotion. The regulations insure that the companies may not advertise the benefits without also disclosing the risks and side effects.

The Draft Guidance is available at http://www.fda.gov/downloads/Drugs/GuidanceCom-

Continued on Page 21


How do you turn 20 gigabytes of
streaming data into a faster qualifying time?
©2013 Dell Inc. All rights reserved.
Dell Intelligent Data Solutions help a Formula 1™ team gain an edge.
With an intelligent storage management platform, Dell helps an F1 team turn data into insights into a faster car. By analyzing data trackside, the team can make real-time decisions that improve the car's in-race performance. To see how we can help solve your most important business challenges, visit dell.com/domore
DELL
The power to do more

Continued from Page 19
plianceRegulatoryInformation/Guidances/UCM401087.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery

***EU – CENELEC vote on EN 62368***
The new hazard based safety standard, EN62368-1: 2013/FprAA:2014, Audio/Video, Information and Communication Technology Equipment – Part 1was adopted by CENELEC after a second formal vote. A 5 year transitional period from the current standards, EN 60065 and EN 60950-1, has been proposed.

***China – CNCA invitation for foreign certification providers***
With the issuance of Announcement 17 of 2014 on June 6, 2014, CNCA, the Certification and Accreditation Administration, invites testing and certification bodies to formally apply to become designated to perform work under the China Compulsory Certification (CCC) program.
Information on the Announcement is available at http://webstore.ansi.org/NewsDetail.aspx?NewsGuid=2078d6d7-83c2-4428-a517-3f74b1a88f35

Announcement 17 of 2014 is available in Chinese only at http://www.cnca.gov.cn/tzgg/ggxx/ggxx2014/201406/t20140606_20415.shtml

***USA – FCC Regulation Change for Wireless & Radio***
The FCC released a First Report and Order on April 1, 2014 allowing devices in the U-NII-1 band to operate with higher power, and to be used outdoors.
The docket is available at http://www.fcc.gov/document/5-ghz-u-nii-ro

***EU – Compliance with EN 300 328 v1.8.1***
Any new radio device placed on the market on or after the effective date of December 31, 2014 must meet the EN 300 328 v1.8.1 standard. After the effective date, the previous version of the standard will cease to offer presumption of conformity. Devices declared under the previous version will need to be retested.
This standard covers WiFi, Bluetooth, and other wideband transmitters operating in the 2.4 GHz band..

## *Environmental Directions*

***EU – Recast WEEE Directive***
The EU Commission recently published a new consolidated FAQ (Frequently Asked Questions) regarding the Directive 2012/19/EU. The EU Member States had until February 14, 2014 to enact the provision of the new requirements. Two main periods are included within the scope of the Directive:
A transition period from August 13, 2012 until August 13, 2018
An “open-scope” period from August 15, 2018 onwards.
The FAQ is available at http://ec.europa.eu/environment/waste/weee/pdf/faq_weee2.pdf

***Jordan – Energy Efficiency***
Approved on April 24, 2014, Technical Regulations on energy efficiency will require new labeling for some household appliances beginning July 1, 2014.

The Regulated Products are:

Continued on Page 22

Continued from Page 21

| *Product* | *Technical Regulation No.* |
|---|---|
| Air conditioner | No. 2108/2013 |
| Combined washer-dryer | No. 2097/2013 |
| Dishwasher | No. 2100/2013 |
| Electric lamps | No. 2092/2013 |
| Electric Oven | No. 2098/2013 |
| Clothes dryer | No. 2096/2013 |
| Refrigerator | No. 2101/2013 |
| Washing Machine | No. 2104/2013 |
| Television | No. 2105/2013 |

The energy label format specifies the energy efficiency class, rated from A, most efficient, to G, least efficient.

Resolution No. 1, 2014 states that non-compliant products may not be imported effective July 1, 2014.

***Malaysia – Energy Efficiency***

The Malaysian Suruhanjaya Tenega (Energy Commission) recently published guidelines for labeling of 4 types of appliances on their website at http://www.st.gov.my/ The affected products are:

Television
Refrigerator
Domestic Fan
Air Conditioner

Per the Electricity Regulation 1994, Amendments 2013, Regulation 101A (3), these products must bear the Energy Efficient Label before it can be sold.

# News to Know

***Recently Published IEC Standards***

IEC 60825-1 ed3.0 (2014-05) Safety of laser products - Part 1: Equipment classification and requirements

IEC 60300-1 ed3.0 (2014-05) Dependability management - Part 1: Guidance for management and application

IEC 60598-1 ed8.0 (2014-05) Luminaires - Part 1: General requirements and tests

IEC/TR 62914 ed1.0 (2014-05) Secondary cells and batteries containing alkaline or other non-acid electrolytes - Experimental procedure for the forced internal short-circuit test of IEC 62133:2012

IEC 61000-4-5 ed3.0 (2014-05) Electromagnetic compatibility (EMC) - Part 4-5: Testing

Continued on Page 23

Continued from Page 22
and measurement techniques - Surge immunity test

IEC 60730-2-22 ed1.0 (2014-05) Automatic electrical controls - Part 2-22: Particular requirements for thermal motor protectors

IEC/TS 62603-1 ed1.0 (2014-05) Industrial process control systems - Guideline for evaluating process control systems - Part 1: Specifications

***USA – National Electrical Safety Code (NESC)***

The NESC, published exclusively by the IEEE, is one of the oldest safety codes continuously in use. Originally published in August 1914, the NESC will celebrate its 100th anniversary this year.

A collaborative work, the NESC specifies best practices at both public and private utilities for electric supply and communication utility systems.

On September 1, 2014, the change proposal preprint for the 2017 Edition will be available, followed by an eight month commentary period.

More information on the history, anniversary, and the change proposal is available at http://standards.ieee.org/about/nesc/100/index.html

*Compliance News Shorts is Edited By Daniece Carpenter, Principal Regulatory Engineer*

***IEEE Electromagnetic Compatibility Magazine Volume 3 Quarter 1*** in their Twenty-Five Years Ago feature reprinted the following from their Winter 1989 newsletter:

A new Technical Committee was formed in August of 1988 in Seattle. The Product Safety Committee of the IEEE EMC Society was chaired by Richard Pescatore of Hewlett-Packard. The newsletter for the committee was being mailed to over 800 readers and four local groups (San Francisco, Portland/Seattle, Los Angeles, and Boston) are holding regular technical meetings.

# South Korean Fan Death Mystery

The South Korean Fan Death Mystery

*by Dr. Rob Long*


The idea that humans assess risk objectively, or just calculate risk based on some common criteria in a risk matrix (exposure, frequency, probability and consequence), is not supported by the evidence. It is often after the event that we articulate some rational explanation for our choice or risk ranking, but in reality that is not why we chose to undertake that task or take that risk in the first place.

One example of subjective risk attribution, that I hadn't heard but was totally intrigued by, is the genuine belief by South Koreans that fans left on overnight are very likely to kill you!

Nobody is saying that Koreans are dumb in their beliefs, but they behave as expected, and defend their beliefs, when knowledge presented and unquestioned throughout their life is challenged and said to be wrong.

Also, if you approach a Korean about this issue, their first instinct is to defend their culture to foreigners even though they may not agree with the belief themselves. But, even if you do convince a Korean that fan death is not true, it would be really hard for you to get them to actually overcome the deep subconscious fear and actually sleep in a sealed room with a fan on. They have been very well trained by the media, the government and their parents avoid the risk.

From Chapter 1 of Dr. Long's new book, "REAL RISK – Human Discerning and Risk" (download a free copy here):
A good example of just how risk is aggravated, yet not connected to reality or scientific evidence, is illustrated in a study of the fear of fans in South Korea or what is known as "fan death" myth.

It is a widely held belief in South Korea that a fan left on overnight in a closed room can kill you. This is why all fans in South Korea must be fitted with a timer.

Many scientific tests have proven that the [perceived] risks associated with electric fans are not real but, due to cognitive dissonance, the evidence is not believed. To make matters worse, the South Korean Consumer Protection Board (KCPB) has issued the following warning:

If bodies are exposed to electric fans or air conditioners for too long, it causes [the] bodies to lose water and [causes] hypothermia. If directly in contact with [air current from] a fan, this could lead to death from [an] increase of carbon dioxide saturation concentration [sic] and decrease of oxygen concentration. The risks are higher for the elderly and patients with respiratory problems. From 2003 [to] 2005, a total of 20 cases were reported through the CISS involving asphyxiations caused by leaving electric fans

***The Impact of Product Safety Myths***

*As product safety professionals, we are confronted with myths about product safety on a regular basis. People outside our profession often make comments that fly in the face of the science and engineering practice in our field, comments that are based in urban myths and misinformation.*

*Dr. Long's article takes a brief look at one of those myths, a myth with a specific social context that some of our members may have encountered. Understanding the origins of myths like this, and the impact that they can have on our profession is important. Have you dealt with a myth like this in your work? What impact did it have? How did you resolve the issue? We want to hear your stories about this challenge.*

*Doug Nix, Machine Safety Associate Editor*

Continued on Page 25

Continued from Page 24

and air conditioners on while sleeping. To prevent asphyxiation, timers should be set, wind direction should be rotated and doors should be left open.

*Dr. Rob Long is a social psychologist, principal and trainer at Human Dymensions PTY LTD.*
*10 Jens Place Kambah ACT 2902*
*mobile: 0424547115*
*e-mail: admin@humandymensions.com*
*web: www.humandymensions.com*

*Dr. Long's article is reprinted from his posting on safetyrisk.net with permision.*

# Interlock Architectures - Pt. 3

Editor's note—This is the third in a seven-part series of articles reprinted through the courtesy of Doug Nix from postings on the Machinery Safety 101 blog (http://machinerysafety101.com).

**Interlock Architectures – Pt. 3: Category 2**

by Douglas Nix

In the first two posts in this series, we looked at Category B, the Basic category of system architecture, and then moved on to look at Category 1. Category B underpins Categories 2, 3 and 4. In this post we'll look more deeply into Category 2.

Let's start by looking at the definition for Category 2, taken from ISO 13849-1:2007. Remember that in these excerpts, SRP/CS stands for Safety Related Parts of Control Systems.

**Definition**

**6.2.5 Category 2**

For category 2, the same requirements as those according to 6.2.3 for category B shall apply. "Well–tried safety principles" according to 6.2.4 shall also be followed. In addition, the following applies.

SRP/CS of category 2 shall be designed so that their function(s) are checked at suitable intervals by the machine control system. The check of the safety function(s) shall be performed

- at the machine start-up, and
- prior to the initiation of any hazardous situation, e.g. start of a new cycle, start of other movements, and/or
- periodically during operation if the risk assessment and the kind of operation shows that it is necessary.

The initiation of this check may be automatic. Any check of the safety function(s) shall either

- allow operation if no faults have been detected, or
- generate an output which initiates appropriate control action, if a fault is detected.

Whenever possible this output shall initiate a safe state. This safe state shall be maintained until the fault is cleared. When it is not possible to initiate a safe state (e.g. welding of the contact in the final switching device) the output shall provide a warning of the hazard.

For the designated architecture of category 2, as shown in Figure 10, the calculation of $MTTF_d$ and $DC_{avg}$ should take into account only the blocks of the functional channel (i.e. I, L and O in Figure 10) and not the blocks of the testing channel (i.e. TE and OTE in Figure 10).

The diagnostic coverage ($DC_{avg}$) of the total SRP/CS including fault-detection shall be low. The $MTTF_d$ of each channel shall be low-to-high, depending on the required performance

Continued on Page 27

Continued from Page 26

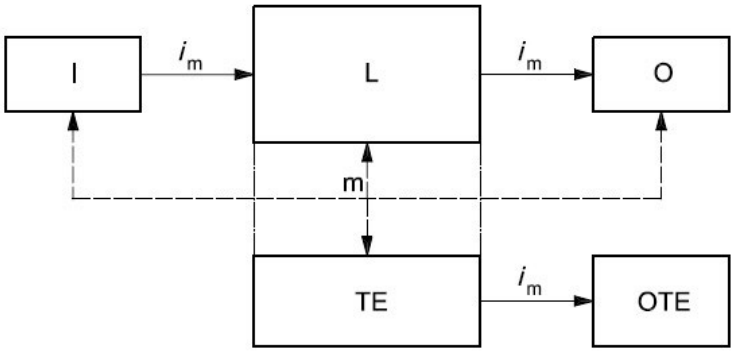
level ($PL_r$). Measures against CCF shall be applied (see Annex F).

The check itself shall not lead to a hazardous situation (e.g. due to an increase in response time). The checking equipment may be integral with, or separate from, the safety-related part(s) providing the safety function.

The maximum PL achievable with category 2 is PL = d.

NOTE 1 In some cases category 2 is not applicable because the checking of the safety function cannot be applied to all components.
NOTE 2 Category 2 system behaviour allows that
the occurrence of a fault can lead to the loss of the safety function between checks,
the loss of safety function is detected by the check.
NOTE 3 The principle that supports the validity of a category 2 function is that the adopted technical provisions, and, for example, the choice of checking frequency can decrease the probability of occurrence of a dangerous situation.

**Figure 1 - Category 2 Block diagram [1, Fig. 10]**




Dashed lines represent reasonably practicable fault detection.

**Key**

$i_m$ interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE

**Figure 10 — Designated architecture for category 2**

## Breaking it Down

Let start by taking apart the definition a piece at a time and looking at what each part means. I'll also show a simple circuit that can meet the requirements.

## Category B and Well-tried Safety Principles

The first paragraph speaks to the building block approach taken in the standard:

For category 2, the same requirements as those according to 6.2.3 for category B shall apply. "Well–tried safety principles" according to 6.2.4 shall also be followed. In addition, the following applies.

Systems meeting Category 2 are required to meet all of the same requirements as Cat-

Continued on Page 28

Continued from Page 27

egory B, as far as the components are concerned. Other requirements for the circuits are different, and we will look at those in a bit.

**Self-Testing Required**

Category 2 brings in the idea of diagnostics. If correctly specified components have been selected (Category B), and are applied following "well-tried safety principles," then adding a diagnostic component to the system should allow the system to detect some faults and therefore achieve a certain degree of "fault-tolerance" or the ability to function correctly even when some aspect of the system has failed.

Let's look at the text:

> SRP/CS of Category 2 shall be designed so that their function(s) are checked at suitable intervals by the machine control system. The check of the safety function(s) shall be performed
>
> - at the machine start-up, and
> - prior to the initiation of any hazardous situation, e.g. start of a new cycle, start of other movements, and/or
> - periodically during operation if the risk assessment and the kind of operation shows that it is necessary.
>
> The initiation of this check may be automatic. Any check of the safety function(s) shall either
>
> - allow operation if no faults have been detected, or
> - generate an output which initiates appropriate control action, if a fault is detected.
>
> Whenever possible this output shall initiate a safe state. This safe state shall be maintained until the fault is cleared. When it is not possible to initiate a safe state (e.g. welding of the contact in the final switching device) the output shall provide a warning of the hazard.

Periodic checking is required. The checks must happen at least each time there is a demand placed on the system, i.e. a guard door is opened and closed, or an emergency stop button is pressed and reset. In addition the integrity of the SRP/CS must be tested at the start of a cycle or hazardous period, and potentially periodically during operation if the risk assessment indicates that this is necessary. The testing frequency must be at least 100x the demand rate [1, 4.5.4], e.g., a light curtain on a part loading work station that is interrupted every 30 s during normal operation requires a minimum test rate of once every 0.3 s, or 200x per minute or more.

The testing does not have to be automatic, although in practice it usually is. As long as the system integrity is good, then the output is allowed to remain on, and the machinery or process can run.

**Watch Out!**

Notice that the words "whenever possible" are used in the last paragraph in this part of the definition where the standard speaks about initiation of a safe state. This wording alludes to the fact that these systems are still prone to faults that can lead to the loss of the safety function, and so cannot

Continued on Page 29

Continued from Page 28
be called truly "fault-tolerant." Loss of the safety function **should** be detected by the monitoring system and a safe state initiated. This requires careful thought, since the safety system components may have to interact with the process control system to initiate and maintain the safe state in the event that the safety system itself has failed. Also note that it is not possible to use fault exclusions in Category 2 architecture, because the system is not fault tolerant.

All of this leads to an interesting question: If the system is hardwired through the operating channel, and all the components used in that channel meet Category B requirements, can the diagnostic component be provided by a monitoring the system with a standard PLC?

The answer to this is **YES**. Test equipment (called OTE in the standard) is specifically excluded, and Category 2 DOES NOT require the use of well-tried components, only well-tried safety principles.

Finally, for the faults that can be detected by the monitoring system, detection of a fault must initiate a safe state. This means that on the next demand on the system, e.g., the next time the guard is opened, the machine must go into a safe condition. Generally, detection of a fault should prevent the subsequent reset of the system until the fault is cleared or repaired.

Testing is not permitted to introduce any new hazards or to slow the system down. The tests must occur "on-the-fly" and without introducing any delay in the system compared to how it would have operated without the testing incorporated. Test equipment can be integrated into the safety system or be external to it.

**One More "Gotcha"**

Note 1 in the definition highlights a significant pitfall for many designers: if **all** of the components in the functional channel of the system cannot be checked, **you cannot claim conformity to Category 2**. If you look back at Fig. 1, you will see that the dashed "m" lines connect all three functional blocks to the TE, indicating that all three must be included in the monitoring channel. A system that otherwise would meet the architectural requirements for Category 2 must be downgraded to Category 1 in cases where all the components in the functional channel cannot be tested. This is a major point and one which many designers miss when developing their systems.

**Calculation of $MTTF_d$**

The next paragraph deals with the calculation of the failure rate of the system, or $MTTF_d$.

> For the designated architecture of category 2, as shown in Figure 10, the calculation of MTTFd and DCavg should take into account only the blocks of the functional channel (i.e. I, L and O in Figure 10) and not the blocks of the testing channel (i.e. TE and OTE in Figure 10).

Calculation of the failure rate focuses on the functional channel, not on the monitoring system, meaning that the failure rate of the monitoring system is ignored when analyzing systems using this architecture. The $MTTF_d$ of each component in the functional channel is calculated and then the $MTTF_d$ of the total channel is then calculated by summing the failure rates of the individual functional blocks.

The Diagnostic Coverage ($DC_{avg}$) is also calculated based exclusively on the components in the functional channel, so when determining what percentage of the faults can be detected by the monitoring

Continued on Page 36

# ISPCE 2014

We hope that those of you who attended the 2014 ISPCE in May enjoyed it and found it of value. In this article I will share some of the highlights from the Symposium for those who were unable to attend. There are also some additional pictures of the event on our web site at: http://ewh.ieee.org/soc/pses/symposium/2014/index.html and the program at: http://2014.psessymposium.org/sites/2014.psessymposium.org/files/ISPCE2014_Proceedings_web_v3.pdf.

We tried a number of different things this year based on feedback we have received from past Symposia. Most significant was the time of year. We moved it earlier in the year based on feedback that when it is later in the year, budgets often get tighter and it is more difficult to get funding for these types of activities.


We had two keynotes that focused more on technology developments such as 3D Printing for Keynote #1 and Wearable Technologies for Keynote #2. Both of these provided some background and insight into the technologies and hopefully got us all thinking about the safety and other compliance issues that will need to be addressed to bring these types of products to the market.


We had two demonstrations, again along the lines of current technology trends. One was the Google car that was on display. It certainly generated a lot of discussion about all of the potential safety issues that need to be addressed. The other demonstration was led by students from a local high school who demonstrated the robot they built as part of their participation in the FIRST Robotics program: http://www.usfirst.org/roboticsprograms/frc/. This also generated some lively discussion and was a great way to get young people involved in our event.


We also had a very diverse technical program; you can get an idea of the diverse content from the website: http://ewh.ieee.org/soc/pses/symposium/2014/index.html. You can also see the exhibitors who were involved as well as the companies who supported the event as Patrons.

For 2014 our Awards Ceremony [*Ed.-See article on following pages in this newsletter*] focused on a number of PSES members who actually helped get the society started, as well as some other awards recognizing contributions to the society, including the Chapter of the Year award that went to the San Diego Chapter for outstanding/best practices among all chapters of the PSES. See the program for a complete listing: http://2014.

Continued on Page 31

Continued from Page 30

psessymposium.org/sites/2014.psessymposium.org/files/ISPCE2014_Proceedings_web_v3.pdf

We alloted additional time for networking among the attendees and with the exhibitors who joined us. It was really great to see the number of people who remained in the general assembly room making the most of the networking time!

Finally, the best thing was the number of attendees who were at the symposium. It was the highest ISPCE attendance we have had to date! Additionally, a large number of attendees stayed for the final session where we did a de-brief of the symposium to learn how we might do things better for 2015. John Allen (Chair for the 2015 symposium) was there taking many notes and already thinking how we can use the feedback to make 2015 even better!

For those of you who were there, it was great to see you and I hope to see you again next year. For those who couldn't make it this year, I hope we will see you next year! If you are interested in doing a little more than just attending, check out the PSES website and consider delivering a paper or getting involved in some other way.

Sincerely,

General Chair – 2014 ISPCE

# History and Awards

Travelling in Time: History and the Future
Awards at ISPCE2014 in San Jose

by Murlin Marks, Life Senior Member

Our IEEE PSES is a time machine, looking back to our origins and forward to our opportunities. At our annual conference in San José in May, our Awards Ceremony honored our full decade as a society and our pre-history as TC-8 of the EMC Society. That adds up to a full quarter century. What will the next quarter century bring?

First, an overview of the fast-paced Awards Ceremony. As Awards Committee Chair I had been told to keep the ceremony short in consideration of the busy conference schedule.


Figure 1 – That's me and Kevin Ravo starting things off.

Rich Pescatore, Brian Claes, I (Murlin Marks), Jack Burns, and Richard Georgerian served as TC-8 Chairs, coordinating relations with IEEE and the EMCS, setting up workshops at EMCS symposia, and coordinating our chapters. At the beginning, we were told we needed members and an infrastructure to become an IEEE Society.

Figure 2 – Richard Georgerian and Kevin (That's Grant Schmidbauer to the left)
Richard served as TC-8 Chair during its final years, headed up our early Symposia, and is our official photographer. (This is one of the few photos he didn't take.)

Our newsletter is our oldest form of communicating with members. It was started in the pre-internet days that required tricky desktop publishing, collating hard copies, and (gasp!) sending issues through the mail.

Figure 3 – Kevin, John McBain, Roger Volgstadt and Ken (a.k.a. Kent) Warwick. John, Roger and Ken kept the newsletter "alive" for many years.

In the early 2000s, a steering committee was formed to take us through the steps to become an IEEE society. Jim Bacher, Jack Burns, Daniece Carpenter and Mark Montrose were the key people on that committee who had meetings with IEEE executives and committees and persevered the process of getting us off the ground.

Continued on Page 33

Continued from Page 32

Figure 4 – Kevin, Daniece Carpenter, Jack Burns, and Jim Bacher. They get the credit for getting us off the ground.

Awards were given to the Symposium Chairs: Henry Benitez, Bansi Patel, Richard Georgerian, Doug Nix, Steve Brody and Anna Klausterman. Dan Arnold received an award for his service as our first treasurer and treasurer for most of our conferences, Jan Swart for his service as treasurer and Daniece Carpenter as secretary.


Figure 5 – Mark Montrose and Henry Benitez, our first two presidents.

Figure 6 – Rich Nute and Gary Tornquist served as symposium Technical Committee Chairs. Rich also has written numerous technical articles in our newsletter.

Recognition Awards were given to Dell, Microsoft and UL for their support over the years.

Figure 7 – Bahman Mostafazadeh accepts the PSES Recognition Award for UL.

Chapter of the Year went to the San Diego Chapter.

Figure 8 – Leszek Langiewicz, San Diego Chapter Chair, receives the Chapter of the Year Award from Mike Nicholls, Chapter Chair Coordinator.

The Best Paper Award went to Joe Randolph for his paper, “Lightning Surge Damage to Ethernet and POTS Ports Connected to Inside Wiring”.

Continued on Page 34

Continued from Page 33

Figure 9 – Joe Randolph receives the Best Paper Award From Tom Burke, the ISPCE Technical Committee Chair.

That wraps up the awards for this year's conference. Grant Schmidbauer and Juha Junkkarinen are also on the Awards Committee. We will now accept nominations for awards to be given at our conference next year in Chicago. I am sure we missed some worthy people.

And to the future—
What has the future to do with the past and our awards?

First, all our members have the opportunities to get involved just as our awardees have done. If you have a local chapter, find out how you can help. Probably every one of our members has some special area of expertise that can serve as the basis for a chapter presentation. Chapters can also set up workshops, judge science fairs, have tours and do outreach at local colleges. Help with the various society committees, e.g. marketing or membership. Get involved with our annual conferences. Write papers and articles. For the novices, we have a webinar on writing papers and getting published within IEEE. For our experienced member, there is the opportunity to mentor those who are less experienced. It is gratifying to see novices develop areas of skills and expertise and become the experts themselves.

Second, a professional society builds prestige within the profession. That's why our society awards are important.

Chapters! Please keep the Chapter of the Year Award in the back of your minds as you work through the year's activities. When we were TC-8 of the EMC Society, I observed the sometimes cut-throat (well, almost) competition between chapters for the honor of winning Chapter of the Year. It's a win-win to build chapter activities to boost the competition for the Chapter of the Year. There's still time in 2014 to build great programs for this year's award. Please work with Mike Nicholls to a) have the best possible program, and b) to fill out the CotY nomination form.

Your Awards Committee needs your input for achievement and recognition awards. Who has done great things within your chapter? Who has taken on a special task? Who has accomplished something special within the product safety/compliance engineering realm? We will send our reminders from time to time, but please help us build recognition in our profession. That's our future! Then you will look back fondly on what you have done for your colleagues and your profession. I know I do.

Figure 10 – Old timers?? Mark Montrose, Roger Volgstadt, Ken Warwick, Brian Claes and John Mcbain. See if you can recognize some of them in the early Newsletters.

**Hewlett-Packard Company** is a multinational information technology corporation headquartered in Palo Alto, California, USA. The company was founded in a one-car garage in Palo Alto by Bill Hewlett and Dave Packard in 1939. Since then HP becomes one of the world's largest information technology companies, operating in nearly every country, supplying not just hardware and software, but also a full range of services to design, implement, and support IT infrastructure.

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. The world’s largest technology company, HP brings together a portfolio that spans printing, personal computing, software, services and IT infrastructure at the convergence of the cloud and connectivity, creating seamless, secure, context-aware experiences for a connected world.

HP's Imaging and Printing Group is the leading imaging and printing systems provider in the world for printing and scanning devices, employing Inkjet and LaserJet technologies in variety of products, All-in-One multifunction printer/scanner/faxes, Large Format Printers, Digital Press, Photosmart digital cameras and photo printers, a photo sharing and photo products services.

HP's Personal Systems Group one of the leading vendors of personal computers ("PCs") in the world. PSG includes business and consumer PCs and accessories, handheld computing, and digital "connected" entertainment.

HP’s Enterprise Business incorporates HP Technology Services, Enterprise Services, Enterprise Security Services, Software Division, and Enterprise Servers, Storage and Networking Group. The Enterprise Servers, Storage and Networking Group oversee "back end" products like storage and servers.

Continued from Page 29
equipment, only faults in the functional channel are considered.

This highlights the fact that a failure of the monitoring system cannot be detected, so a single failure in the monitoring system that results in the system failing to detect a subsequent normally detectable failure in the functional channel will result in the loss of the safety function.

**Summing Up**
The next paragraph sums up the limits of this particular architecture:

> The diagnostic coverage (DCavg) of the total SRP/CS including fault-detection shall be low. The MTTFd of each channel shall be low-to-high, depending on the required performance level (PLr). Measures against CCF shall be applied (see Annex F).

The first sentence reflects back to the previous paragraph on diagnostic coverage, telling you, as the designer, that you cannot make a claim to anything more than LOW DC coverage when using this architecture.

This raises an interesting question, since Figure 5 in the standard shows columns for both $DC_{avg}$ = LOW and $DC_{avg}$=MED. My best advice to you as a user of the standard is to abide by the text, meaning that you cannot claim higher than LOW for $DC_{avg}$ in this architecture. This conflict will be addressed by future revisions of the standard.

Another problem raised by this sentence is the inclusion of the phrase "the total SRP/CS including fault-detection," since the previous paragraph explicitly tells you that the assessment of $DC_{avg}$ "should" only include the functional channel, while this sentence appears to include it. In standards writing, sentences including the word "shall" are clearly mandatory, while those including the word "should" indicate a condition which is advised but not required. Hopefully this confusion will be clarified in the next edition of the standard.

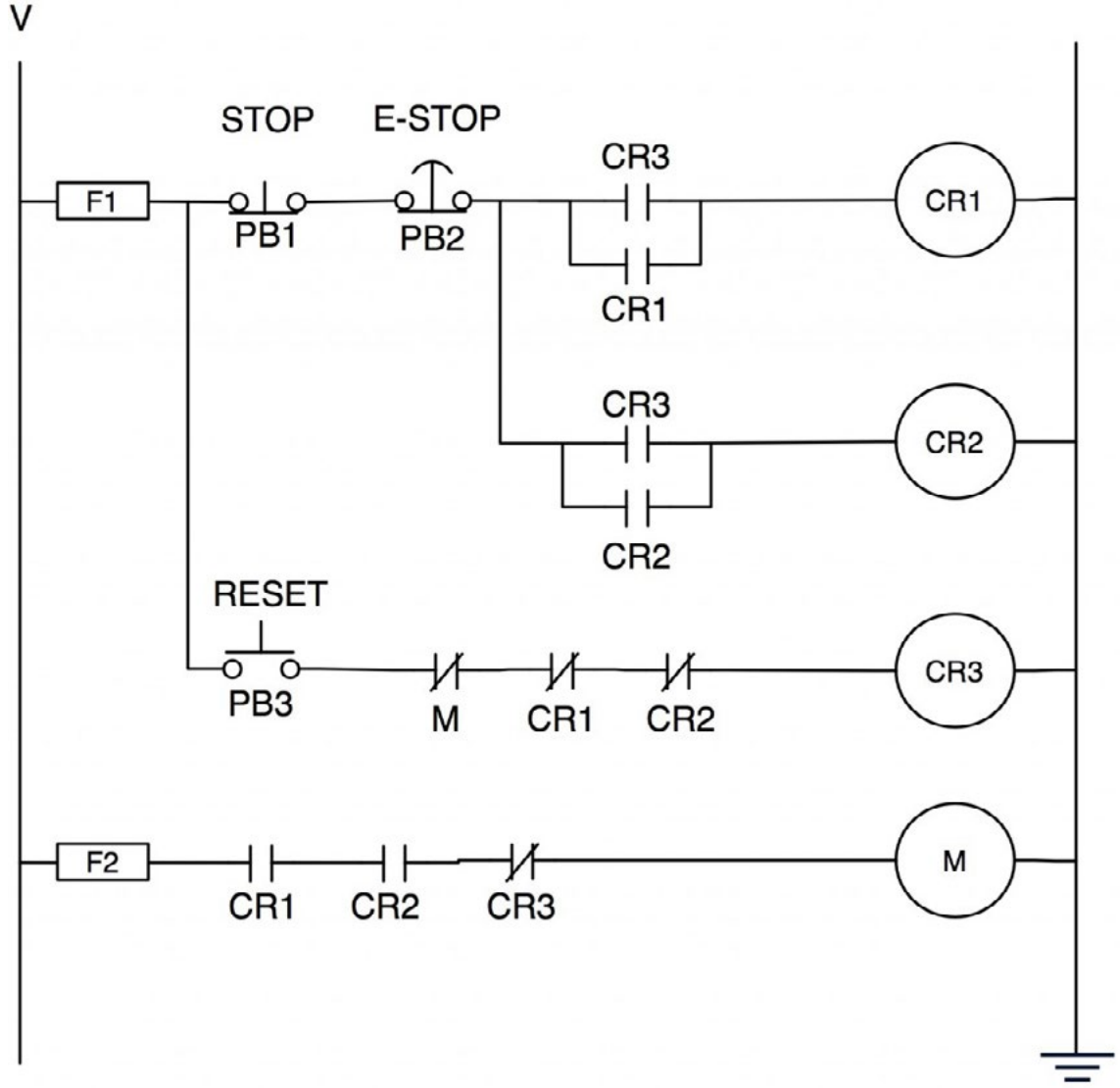
$MTTF_d$ in the functional channel can be anywhere in the range from LOW to HIGH depending on the components selected and the way they are applied in the design. The requirement will be driven by the desired PL of the system, so a $PL_d$ system will require HIGH $MTTF_d$ components in the functional channel, while the same architecture used for a $PL_b$ system would require only LOW $MTTF_d$ components. Finally, applicable measures against Common Cause Failures (CCF) must be used. Some of the measures given in Table F.1 in Annex F of the standard cannot be applied, such as Channel Separation, since you cannot separate a single channel. Other CCF measures can and must be applied, and so therefore you must score at least the minimum 65 on the CCF table in Annex F to claim compliance with Category 2 requirements.

**Example Circuit**
Here's an example of what a simple Category 2 circuit constructed from discrete components might look like. Note that PB1 and PB2 could just as easily be interlock switches on guard doors as push buttons on a control panel. For the sake of simplicity, I did not illustrate surge suppression on the relays, but you should include MOV's or RC suppressors across all relay coils. All relays are considered to be constructed with "force-guided" designs and meet the requirements for well-tried components.

Continued on Page 37

Continued from Page 36

**Figure 2 - Example Category 2 circuit from discrete components**




How the circuit works:

1. The machine is stopped with power off. CR1, CR2, and M are off. CR3 is off until the reset button is pressed, since the NC monitoring contacts on CR1, CR2 and M are all closed, but the NO reset push button contact is open.

2. The reset push button, PB3, is pressed. If both CR1, CR2 and M are off, their normally closed contacts will be closed, so pressing PB3 will result in CR3 turning on.

3. CR3 closes its contacts, energizing CR1 and CR2 which seal their contact circuits in and de-energize CR3. The time delays inherent in relays permit this to work.

4. With CR1 and CR2 closed and CR3 held off because its coil circuit opened when CR1 and CR2

Continued on Page 38

Continued from Page 37

turned on, M energizes and motion can start.

In this circuit the monitoring function is provided by CR3. If any of CR1, CR2 or M were to weld closed, CR3 could not energize, and so a single fault is detected and the machine is prevented from re-starting. If the machine is stopped by pressing either PB1 or PB2, the machine will stop since CR1 and CR2 are redundant. If CR3 fails with welded contacts, then the M rung is held open because CR3 has not de-energized, and if it fails with an open coil, the reset function will not work, therefore both failure modes will prevent the machine from starting with a failed monitoring system, if a "force-guided" type of relay is used for CR3. If CR1 or CR2 fail with an open coil, then M cannot energize because of the redundant contacts on the M rung.

This circuit cannot detect a failure in PB1, PB2, or PB3. Testing is conducted each time the circuit is reset. This circuit does not meet the 100x test rate requirement, and so cannot be said to truly meet Category 2 requirements.

If M is a motor starter rather than the motor itself, it will need to be duplicated for redundancy and a monitoring contact added to the CR3 rung.

In calculating $MTTF_d$, PB1, PB2, CR1, CR2, CR3 and M must be included. CR3 is included because it has a functional contact in the M rung and is therefore part of the functional channel of the circuit as well as being part of the OT and OTE channels.

Watch for the next installment in this series where we'll explore Category 3, the first of the "fault tolerant" architectures.

*Doug Nix, C.E.T., SM-IEEE is Managing Director at Compliance InSight Consulting Inc. in Kitchener, Ontario, Canada.*

# New PSES Members

## from 24 March 2014 through 21 June 2014

Our new members are located in the following countries: Australia, Canada, Chile, China, Hong Kong, India, Mexico, New Zealand, Peru, Singapore, United Kingdom, USA, and Zambia.

Alex Mathew Chettiath
Ali Aaron Kani
Alvaro Gonzalo Alvarez
ARUL MUTHIAH MANICKAVASAGAM
Arvin Singh
Clive Thomas
Dave Tillman
Dmitry L Gringauz
Donald L Hildebrand
Douglas C Massey
Douglas E Norman
Douglas L Datwyler
Erick Latvala
Erick Ortega
Frederick Germond
Gary Paul Shimko
Gary T Smullin
Gregg Jordan
James Timothy Millican
Jose A Molina
KAMONO NAMANTEMBA
Ken Budoff
Louis Le
Michael Berthiaume
Michael G Turco
mohammed Abid A Aldhahri
Paul David Evers
Radney Brian Pepito Minerva
Rakan Bejad Ali Alharbi
Rakesh Vazirani
Rob Klein
Rony Jean-Gilles
Saqib Ali
SARTHAK KUMAR SAHU
Simon Rate
Steven A Zilber
tongxun luo
VICTORIA A HAILEY
Wael Almazeedi

# Institutional Listings

We invite applications for Institutional Listings from firms interested in the product safety field. An Institutional Listing recognizes contributions to support publication of the IEEE Product Safety Engineering Newsletter. To place ad with us, please contact Jim Bacher at j.bacher@ieee.org

The Product Safety Engineering Newsletter is published quarterly during the last month of each calendar quarter. The following deadlines are necessary in order to meet that schedule.

Closing dates for submitted articles:

1Q issue: February 1
2Q issue: May 1
3Q issue: August 1
4Q issue: November 1

Closing dates for news items:

1Q issue: February 15
2Q issue: May 15
3Q issue: August 15
4Q issue: November 15

Closing dates for advertising:

1Q issue: February 15
2Q issue: May 15
3Q issue: August 15
4Q issue: November 15

*The*
**Product**
**Safety**
**Engineering**
**Newsletter**

Gary Weidner
GW Technical Services Inc.
2175 Clarke Drive
Dubuque, IA 52001-4125

**CHANGE SERVICE REQUESTED**