The Probability Circular Ruler “PCR” (Process Safety Metrics)

Roberto Fernández Blanco
DASIS Corp., Buenos Aires, Argentina; robertofblanco@gmail.com (for correspondence)

Published online 21 March 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/prs.11817

The explanation of process safety protection layers and related probability of failure does not need to be complicated. This article shows visuals that can be used to explain the complexity of safety layers and their relationship to reduce the risk of an overall incident. It is proposed that the “Swiss Cheese Model” be replaced with a more realistic probability wheel referred to as the probability circular ruler, leading to usable information to be included in the P&ID as tagging labels with safety data of the process protecting device. © 2016 American Institute of Chemical Engineers Process Saf Prog : 124–136, 2016

Keywords: process safety management; probability of failure on demand; Swiss cheese model; probability circular ruler; risk reduction factor; safety integrity level; HIRA; layer of protection; inherently safer design

INTRODUCTION

In order to improve safety, one needs to be able to quantify a measured element against others or against an established standard reference.

Based on my method of “Visualizing the Concepts,” I reintroduce a process safety metric tool that I proposed in 1998 to substitute the “Swiss Cheese Model” (Figure 1) with a model of successive “Probability Circular Rulers, or **PCR**, with “**U**” numbers (their respective quantity of pockets), PCRs I used when the “SIL/RRF Graph” was developed [1] to replace the conventional Safety Integrity Level (SIL) tables.

This article discloses the significant role played by the PCR tool when mainly used as a Probability of Failure on Demand Wheel (PFD wheel) to depict and show a better understanding of the integrity of protection devices, instruments, Safety Instrumented Functions (SIF) and/or any type of Layers of Protection (LOP).

WE CANNOT PREVENT WHAT WE CANNOT IMAGINE

[*My quotation from my presentation in the 2013, 5th LACPS, Cartagena, Colombia*]:

It is very excruciating to be a witness or to be involved in a catastrophic “Incident Outcome” resulting in destructive consequences with loss of life or injuries. Moreover, the contamination of the environment causes public outrage. Assets are destroyed, production capability is impacted with market loss, in addition to damaged reputation, fines, litigation costs, repair costs, legal prosecutions, and the burden of guilt for an accident that could have been prevented.

This article is intended for technicians, engineers, supervisors, or managers who are working in the field with dangerous processes on a daily basis and who, however, do not specialize in process safety. This article will help professionals to go deeper into process safety science in an easy and understandable way to allow them to more efficiently recognize and identify hazards and their associated risks.

THE SWISS CHEESE MODEL

In an attempt to try to prevent, stop, and/or attenuate a hazardous process incident propagation and its consequences, successive LOPs (Figure 5; defensive trenches, barriers, safeguards, Instrumented Protective Systems/SIF and, Independent Protection Layers [IPL]) are installed. But, LOP have the undesirable possibility of failing with different degrees of probability.

Since the 1990s, process safety experts refer to the “Swiss Cheese” Model (Figure 1) to exhibit how LOP can fail and allow incident propagation.

According to this model, every LOP is represented as a slice of Swiss cheese where the cheese holes represent the barriers fail conditions and their inability to stop the incident propagation.

Successive barriers (slices of Swiss cheese) are installed to stop the incident from escalating, but, if the holes of the successive barriers are aligned, the incident, depicted here as a light beam, will continue its path going through the holes of the successive slices until it strikes one of the LOPs capable of stopping it. Otherwise, the Incident will continue up to its natural final incident outcome with damaging consequences.

However, this model does not give much understanding to people involved on a daily basis with hazardous processes and provides very little visualization of the Probability of Failure (PF) of every LOP and the accumulation when successive LOP fail.

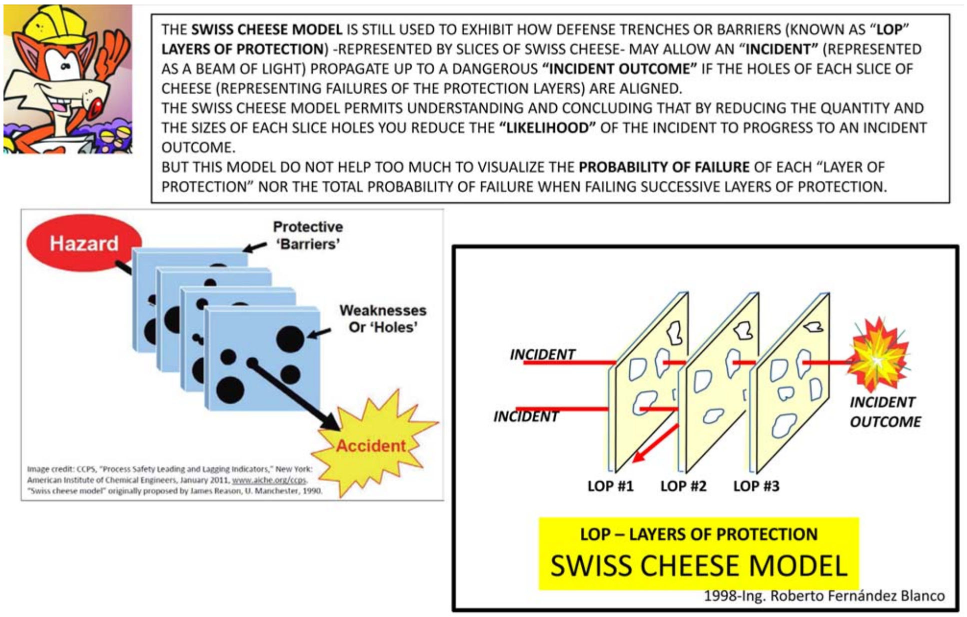
REINTRODUCING THE PCR

In this article, I follow up on my proposal of replacing the Swiss Cheese Model with a more consistent model, the Probability Wheel (like a roulette wheel) that I have given the name of the **PCR** (Figure 2) and used in 2005 to create the above mentioned SIL/RRF Graph [1].

How the PCR Works

Essentially, one imagines a roulette wheel with a quantity of “**U**” pockets of equal width successively numbered having only the pocket number “1” drilled with a hole or opening (Figure 3).

A light beam representing the incident propagation can only cross a wheel barrier and continue its way to the next one when it strikes the drilled pocket #1 of the respective



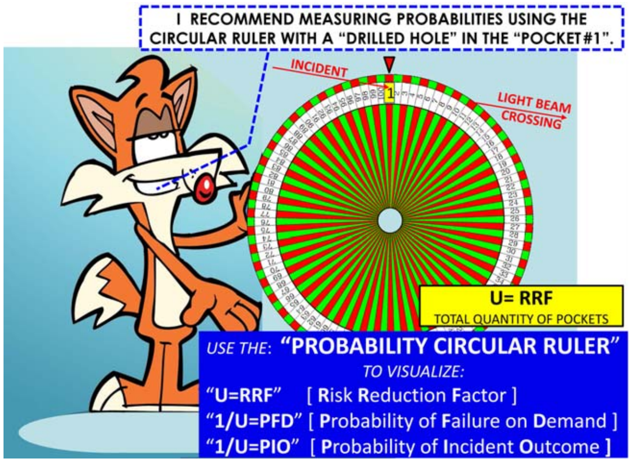
THE **SWISS CHEESE MODEL** IS STILL USED TO EXHIBIT HOW DEFENSE TRENCHES OR BARRIERS (KNOWN AS "**LOP**" **LAYERS OF PROTECTION**) -REPRESENTED BY SLICES OF SWISS CHEESE- MAY ALLOW AN "**INCIDENT**" (REPRESENTED AS A BEAM OF LIGHT) PROPAGATE UP TO A DANGEROUS **"INCIDENT OUTCOME"** IF THE HOLES OF EACH SLICE OF CHEESE (REPRESENTING FAILURES OF THE PROTECTION LAYERS) ARE ALIGNED.

THE SWISS CHEESE MODEL PERMITS UNDERSTANDING AND CONCLUDING THAT BY REDUCING THE QUANTITY AND THE SIZES OF EACH SLICE HOLES YOU REDUCE THE **"LIKELIHOOD"** OF THE INCIDENT TO PROGRESS TO AN INCIDENT OUTCOME.

BUT THIS MODEL DO NOT HELP TOO MUCH TO VISUALIZE THE **PROBABILITY OF FAILURE** OF EACH "LAYER OF PROTECTION" NOR THE TOTAL PROBABILITY OF FAILURE WHEN FAILING SUCCESSIVE LAYERS OF PROTECTION.

Image credit: CCPS, "Process Safety Leading and Lagging Indicators," New York: American Institute of Chemical Engineers, January 2011, www.aiche.org/ccps. "Swiss cheese model" originally proposed by James Reason, U. Manchester, 1990.

Figure 1. Swiss Cheese Model. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]



I RECOMMEND MEASURING PROBABILITIES USING THE CIRCULAR RULER WITH A "DRILLED HOLE" IN THE "POCKET#1".

USE THE: **"PROBABILITY CIRCULAR RULER"**
TO VISUALIZE:
"U=RRF" [Risk Reduction Factor]
"1/U=PFD" [Probability of Failure on Demand]
"1/U=PIO" [Probability of Incident Outcome]

Figure 2. Probability circular ruler. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

barrier when being in the upper position in coincidence with the reference arrow (Figures 3).

This depicts a Probability of "**P = 1/U**" (the #1 on the total "U" pockets) for the LOP failing to stop or mitigate the Incident.

When the drilled pocket #1 of all the successive LOPs are aligned (the upper position in Figures 4 and 6), all the LOPs are in a failed condition and the incident progresses up to the natural incident outcome.

Once familiarized with the image of the **PCR** of "**U**" pockets with the"1" drilled, it will be easy to represent and visualize:

a. The "**P**robability of **F**ailure on **D**emand **PFD = 1/U**" of every LOP (Figure 6), that of a complete SIF loop (Figures 18a–18d), that of a single safety protecting device or instrument, or that of any safety procedure;
b. The **P**robability of every **I**ncident **O**utcome (**PIO** = **1/U**) at the end of every branch (scenario) of an Event Tree Analysis (**ETA**) diagram (Figure 19);
c. Any other Probability application, Fault Tree Analysis (**FTA**) diagram, for example, (Figure 20).
d. The "**U**" pockets of the **PCR** will directly indicate the **R**isk **R**eduction **F**actor **RRF = 1/PFD = U** of any barrier.
e. Overall risk reduction is the product of each RRF.

Figures 5–7 permit the comparison of one set of LOPs represented by both models, with the "Swiss Cheese slices" model and with the PCRs model.

The "**U**" of every LOP can automatically envision the respective **PFD** (and Integrity level) and allows the visualization of the magnitude of the Consequence after the successive wheels (LOPs) stating the respective partial Risk Severity Level (**RSL**) which is changing when the Incident propagates unabated through the different LOPs, bearing in mind that any failing LOP involves an additional cost in the process operation.

The PCR model with its "U" number, properly supported with a technical description of the hazard and its incident and consequences, will permit a quick view of the weaker LOPs, which should be improved in their RRF and where it will be convenient to include an additional LOP with an appropriate RRF. It will also permit the comparisons of the effectiveness of different types of barriers, mechanical, chemical, instrumented and/or procedural, implemented for similar applications in different locations, resulting in a reasonable good metric tool to indicate the safety integrity performance of the different LOPs.

POSSIBILITY AND PROBABILITY

Possible is something that could happen (like a rain storm).

Probability is the chance (in percentage) that a possibility may occur.

Certainty means a probability of 100%.

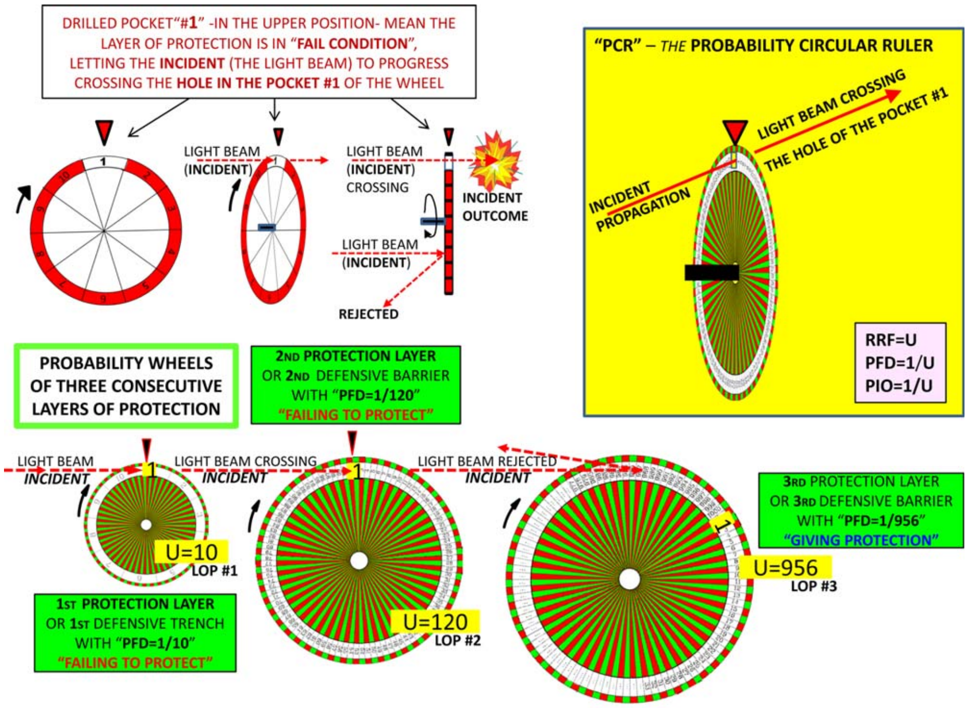

DRILLED POCKET"#1" -IN THE UPPER POSITION- MEAN THE LAYER OF PROTECTION IS IN "FAIL CONDITION", LETTING THE INCIDENT (THE LIGHT BEAM) TO PROGRESS CROSSING THE HOLE IN THE POCKET #1 OF THE WHEEL
LIGHT BEAM (INCIDENT)
LIGHT BEAM (INCIDENT) CROSSING
INCIDENT OUTCOME
LIGHT BEAM (INCIDENT)
REJECTED
"PCR" – THE PROBABILITY CIRCULAR RULER
LIGHT BEAM CROSSING THE HOLE OF THE POCKET #1
INCIDENT PROPAGATION
RRF=U
PFD=1/U
PIO=1/U
PROBABILITY WHEELS OF THREE CONSECUTIVE LAYERS OF PROTECTION
2ND PROTECTION LAYER OR 2ND DEFENSIVE BARRIER WITH "PFD=1/120" "FAILING TO PROTECT"
LIGHT BEAM INCIDENT
LIGHT BEAM CROSSING INCIDENT
LIGHT BEAM REJECTED INCIDENT
3RD PROTECTION LAYER OR 3RD DEFENSIVE BARRIER WITH "PFD=1/956" "GIVING PROTECTION"
U=10
LOP #1
U=120
LOP #2
U=956
LOP #3
1ST PROTECTION LAYER OR 1ST DEFENSIVE TRENCH WITH "PFD=1/10" "FAILING TO PROTECT"

Figure 3. "PCR"—Probability Circular Ruler Model. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

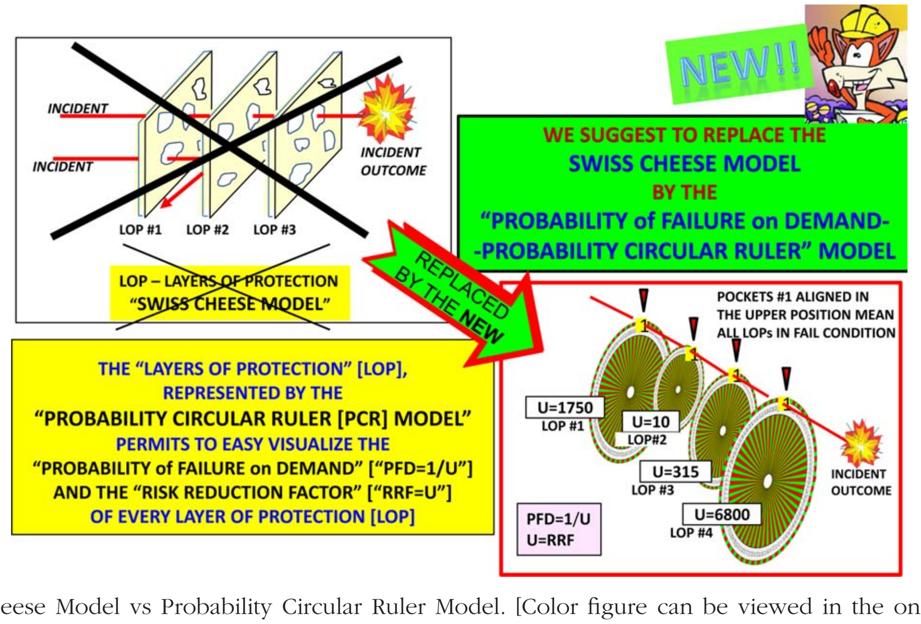

INCIDENT
INCIDENT
INCIDENT OUTCOME
LOP #1
LOP #2
LOP #3
LOP – LAYERS OF PROTECTION "SWISS CHEESE MODEL"
NEW!!
WE SUGGEST TO REPLACE THE SWISS CHEESE MODEL BY THE "PROBABILITY of FAILURE on DEMAND- -PROBABILITY CIRCULAR RULER" MODEL
REPLACED BY THE NEW
THE "LAYERS OF PROTECTION" [LOP], REPRESENTED BY THE "PROBABILITY CIRCULAR RULER [PCR] MODEL" PERMITS TO EASY VISUALIZE THE "PROBABILITY of FAILURE on DEMAND" ["PFD=1/U"] AND THE "RISK REDUCTION FACTOR" ["RRF=U"] OF EVERY LAYER OF PROTECTION [LOP]
POCKETS #1 ALIGNED IN THE UPPER POSITION MEAN ALL LOPs IN FAIL CONDITION
U=1750
LOP #1
U=10
LOP#2
U=315
LOP #3
U=6800
LOP #4
INCIDENT OUTCOME
PFD=1/U
U=RRF

Figure 4. Swiss Cheese Model vs Probability Circular Ruler Model. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

Probability means that—on average—one device of a total of "U" devices might fail at any time within certain period or number of operations. It may happen that the failing device is the one you have installed in your process.

RISK (PROBABILITY AND CONSEQUENCE)

To visualize a risk concept, we should start from the concept of a Hazard.

A ***Hazard*** is an inherent latent source of harmful and destructive potential energies resulting from flammables, explosives, toxics, corrosive materials, incompatible chemical material reactivity, runaway reactions, mechanical, kinetic and potential energies releases, radioactive emissions, etc., resident in the main containment and/or the ancillary components of a process.

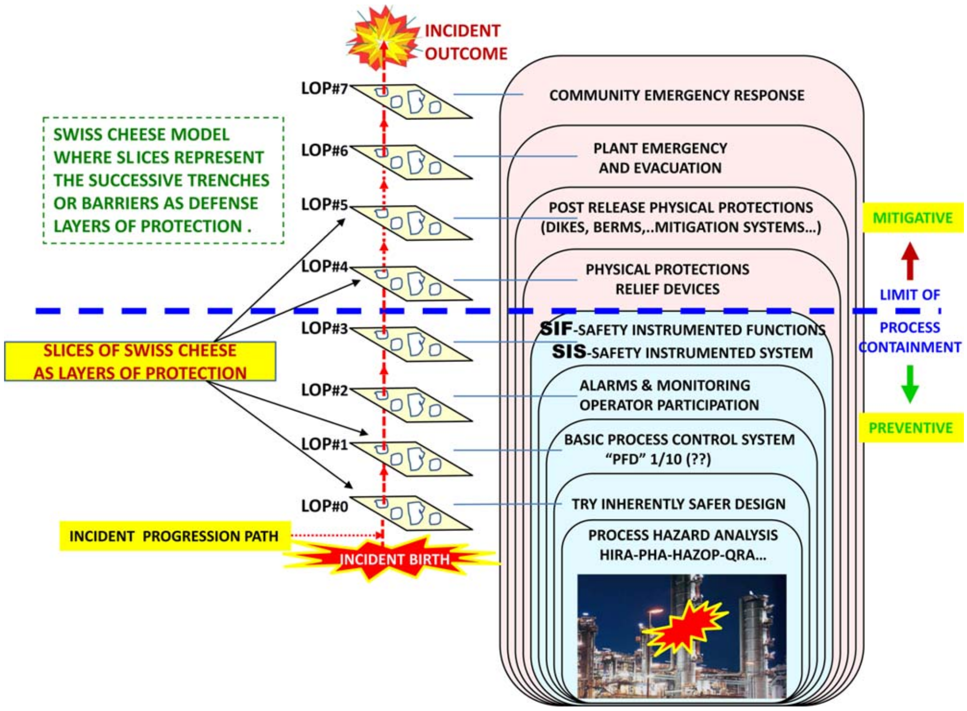

INCIDENT OUTCOME
LOP#7
LOP#6
LOP#5
LOP#4
LOP#3
LOP#2
LOP#1
LOP#0
SWISS CHEESE MODEL WHERE SLICES REPRESENT THE SUCCESSIVE TRENCHES OR BARRIERS AS DEFENSE LAYERS OF PROTECTION .
SLICES OF SWISS CHEESE AS LAYERS OF PROTECTION
INCIDENT PROGRESSION PATH
INCIDENT BIRTH
COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY AND EVACUATION
POST RELEASE PHYSICAL PROTECTIONS (DIKES, BERMS,..MITIGATION SYSTEMS...)
PHYSICAL PROTECTIONS RELIEF DEVICES
SIF-SAFETY INSTRUMENTED FUNCTIONS
SIS-SAFETY INSTRUMENTED SYSTEM
ALARMS & MONITORING OPERATOR PARTICIPATION
BASIC PROCESS CONTROL SYSTEM "PFD" 1/10 (??)
TRY INHERENTLY SAFER DESIGN
PROCESS HAZARD ANALYSIS HIRA-PHA-HAZOP-QRA...
MITIGATIVE
LIMIT OF PROCESS CONTAINMENT
PREVENTIVE

Figure 5. "Layers Of Protection" seen with the Swiss Cheese Model. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

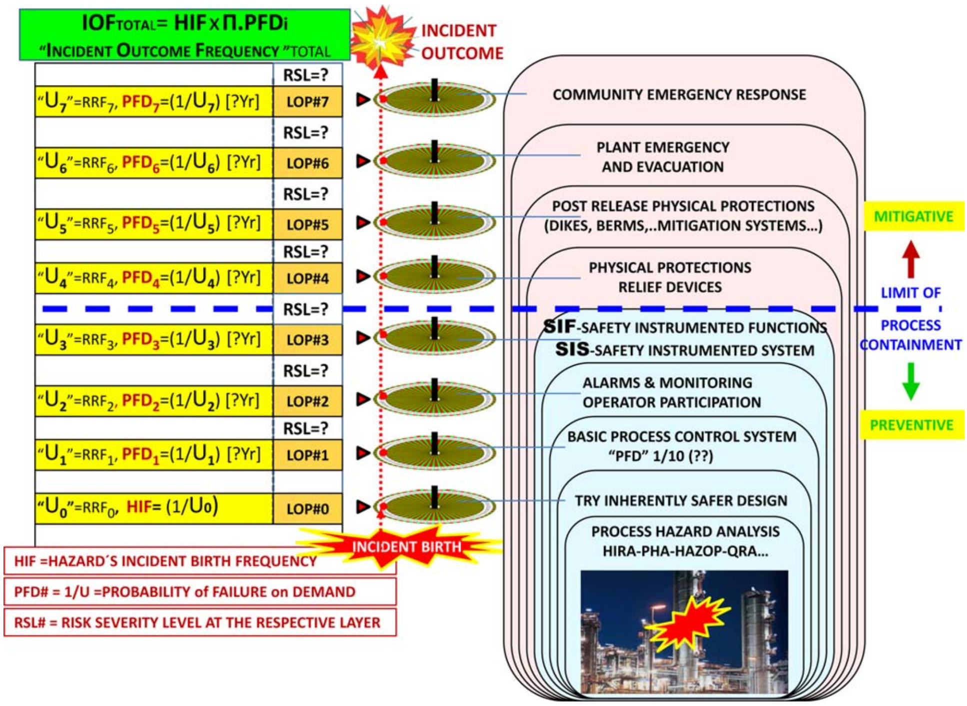

IOFTOTAL= HIF x Π.PFDi
"INCIDENT OUTCOME FREQUENCY "TOTAL
RSL=?
"U7"=RRF7, PFD7=(1/U7) [?Yr]
LOP#7
RSL=?
"U6"=RRF6, PFD6=(1/U6) [?Yr]
LOP#6
RSL=?
"U5"=RRF5, PFD5=(1/U5) [?Yr]
LOP#5
RSL=?
"U4"=RRF4, PFD4=(1/U4) [?Yr]
LOP#4
RSL=?
"U3"=RRF3, PFD3=(1/U3) [?Yr]
LOP#3
RSL=?
"U2"=RRF2, PFD2=(1/U2) [?Yr]
LOP#2
RSL=?
"U1"=RRF1, PFD1=(1/U1) [?Yr]
LOP#1
"U0"=RRF0, HIF= (1/U0)
LOP#0
HIF =HAZARD'S INCIDENT BIRTH FREQUENCY
PFD# = 1/U =PROBABILITY of FAILURE on DEMAND
RSL# = RISK SEVERITY LEVEL AT THE RESPECTIVE LAYER
INCIDENT OUTCOME
INCIDENT BIRTH
COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY AND EVACUATION
POST RELEASE PHYSICAL PROTECTIONS (DIKES, BERMS,..MITIGATION SYSTEMS...)
PHYSICAL PROTECTIONS RELIEF DEVICES
SIF-SAFETY INSTRUMENTED FUNCTIONS
SIS-SAFETY INSTRUMENTED SYSTEM
ALARMS & MONITORING OPERATOR PARTICIPATION
BASIC PROCESS CONTROL SYSTEM "PFD" 1/10 (??)
TRY INHERENTLY SAFER DESIGN
PROCESS HAZARD ANALYSIS HIRA-PHA-HAZOP-QRA...
MITIGATIVE
LIMIT OF PROCESS CONTAINMENT
PREVENTIVE

Figure 6. "Layers Of Protection" seen with the Probability Circular Ruler Model. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

In our Visualization Method, we represent (Figure 8) a Hazard as the caged fierce tiger as depicted on the cover page of *Process Safety Progress*, September 2014 issue [1].

A **Hazard** is a source of **Danger**. The Hazard can develop into a dangerous situation that exposes people, the environment, properties, and production assets to the harmful and uncontrollably destructive power released from the Hazard.

An ***Incident*** is the unwanted, sudden, unexpected, and uncontrollable release of the harmful and destructive

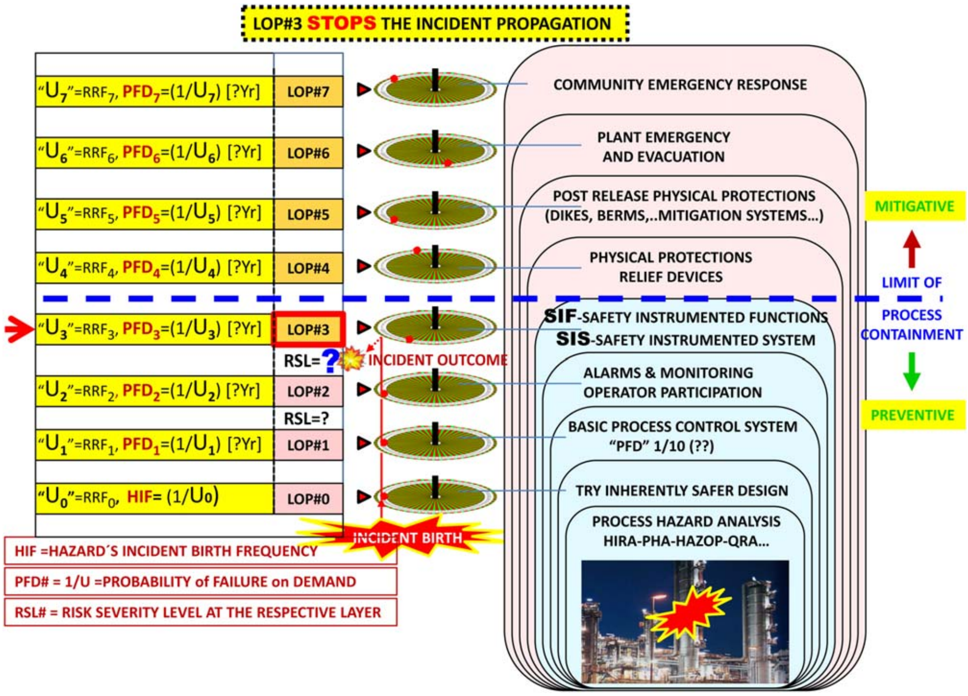

LOP#3 STOPS THE INCIDENT PROPAGATION
"U7"=RRF7, PFD7=(1/U7) [?Yr]
LOP#7
"U6"=RRF6, PFD6=(1/U6) [?Yr]
LOP#6
"U5"=RRF5, PFD5=(1/U5) [?Yr]
LOP#5
"U4"=RRF4, PFD4=(1/U4) [?Yr]
LOP#4
"U3"=RRF3, PFD3=(1/U3) [?Yr]
LOP#3
RSL=?
INCIDENT OUTCOME
"U2"=RRF2, PFD2=(1/U2) [?Yr]
LOP#2
RSL=?
"U1"=RRF1, PFD1=(1/U1) [?Yr]
LOP#1
"U0"=RRF0, HIF= (1/U0)
LOP#0
INCIDENT BIRTH
HIF =HAZARD´S INCIDENT BIRTH FREQUENCY
PFD# = 1/U =PROBABILITY of FAILURE on DEMAND
RSL# = RISK SEVERITY LEVEL AT THE RESPECTIVE LAYER
COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY AND EVACUATION
POST RELEASE PHYSICAL PROTECTIONS (DIKES, BERMS,..MITIGATION SYSTEMS...)
PHYSICAL PROTECTIONS RELIEF DEVICES
SIF-SAFETY INSTRUMENTED FUNCTIONS
SIS-SAFETY INSTRUMENTED SYSTEM
ALARMS & MONITORING OPERATOR PARTICIPATION
BASIC PROCESS CONTROL SYSTEM "PFD" 1/10 (??)
TRY INHERENTLY SAFER DESIGN
PROCESS HAZARD ANALYSIS HIRA-PHA-HAZOP-QRA...
MITIGATIVE
LIMIT OF PROCESS CONTAINMENT
PREVENTIVE

Figure 7. "Layers Of Protection" seen with the Probability Circular Ruler Model. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

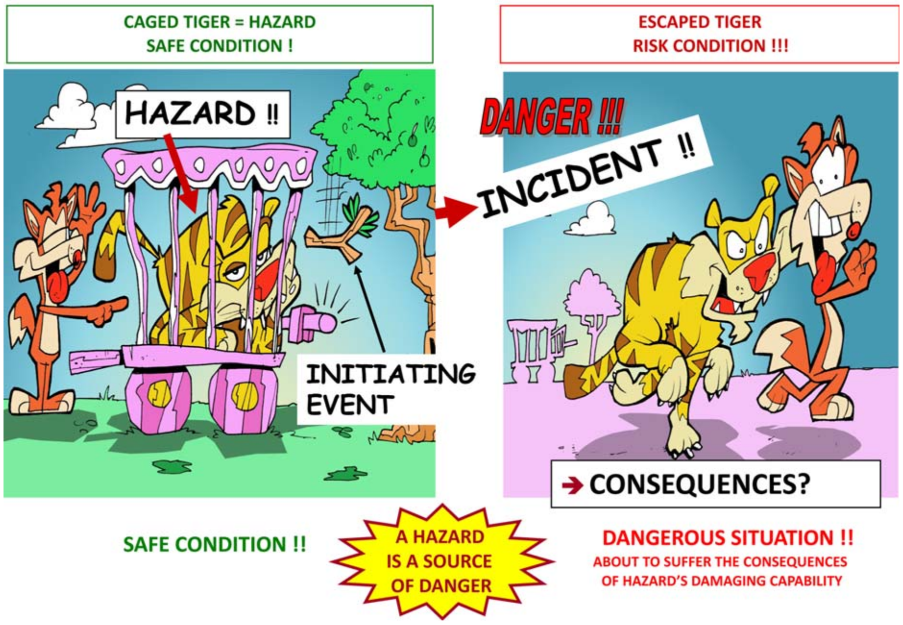


Figure 8. Hazard-initiating event—incident birth and propagation—incident outcome probability and consequences. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

potential energies or materials contained in the Hazard and liberated by an **Initiating Event**.

Each **Hazard** develops into its own **Incident** and each incident, once initiated, develops, progresses, propagates, escalates, and spreads choosing different possible paths and alternative scenarios. That outgrowth, depending on the circumstances or events, finds its way to a culmination, the **Incident Outcome.**

The visualization method represents the incident as a light beam traveling freely while the successive protection barriers are unable to stop its propagation.

The ***Incident Outcome***, with different degrees of Probability, may give place to different levels of collateral and/or final consequences that are proper to the chemical and physical natural characteristics of the participating components

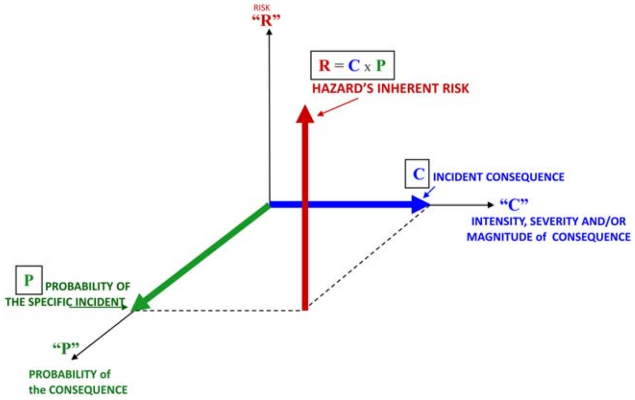

RISK
"R"
R = C x P
HAZARD'S INHERENT RISK
C INCIDENT CONSEQUENCE
"C"
INTENSITY, SEVERITY AND/OR MAGNITUDE of CONSEQUENCE
P PROBABILITY OF THE SPECIFIC INCIDENT
"P"
PROBABILITY of the CONSEQUENCE

Figure 9. Inherent risk, probability, and incident outcome consequence. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

(internal and/or external) and circumstances, capable of causing different degrees of damages and destruction to people, property, production, and/or the environment.

Risk is the "probable and harmful Consequence" of an **Incident Outcome** that may happen in a hazardous process impacting people, environment, properties, and/or production. We evaluate the level of the Risk with both parameters, its natural level of **Probability** times the **Magnitude** or **Severity** of its Consequences (Figure 9).

Tolerable Risk is the Maximum Tolerated Limit established as a target by authority of competence (Organization, Company Directives, Insurance Companies, the Law, etc.) to both, separately or in combination, the maximum level of **Probability** tolerated for the **Incident Outcome** and the maximum Magnitude tolerated for the resultant **Consequences**.

Risk Reduction is the RISK level reduction of the natural-spontaneous Incident Outcome (evaluated without any protection barrier) by reducing the magnitude of its consequences and/or by reducing the probability of the incident to progress up to its natural incident outcome.

If you are still able to redesign your process, you should first try to reduce the risk by reducing the natural level of consequences and/or the probability of the natural incident outcome by means of an **Inherently Safer Design** (ISD) [2].

Otherwise, the Risk reduction steps should be completed by implementing successive defense trenches or barriers known as **LOP,** with the objective of detecting and preventing, in an appropriate amount of time, the existence of an incident, and its propagation within its primary containment or attenuation in case the incident goes beyond the limits of the process.

Risk Reduction Factor (RRF). When a hazard is activated by an Initiating Event and the incident initiates its propagation, different successive LOPs are demanded to obstruct or contain it within the main containment of the process. Once gone beyond this limit, it must be restrained or mitigated (Figures 7 and 17).

Any successive barrier or LOP introduces an additional **RRF**. The magnitude of every RRF (the inverse of the PFD) depends on the Integrity of the respective LOP.

However, LOPs are not absolutely perfect, having a probability to fail. LOPs may fail in one or two of the following different ways: executing its protecting function when not necessary (known as **Probability of Failing Spuriously** [**PFS**]) and (the worst, dangerous, and unwanted) not executing the protective action when is demanded by the process (known as **PFD**).

The PFS of a LOP affect production and may create some undesirable and inconvenient situations (which may also give a place to hazardous conditions that must be considered at the design phase). But, the real concern is with the undetected **PFD** of the LOP, which makes this unresponsive when demanded for protection, leaving the process vulnerable.

The ***PFD*** of any LOP is a very important magnitude in process safety. It defines the concept of **Integrity** of the respective LOP and is directly related to the RRF as "**PFD = 1/RRF**".

The **PFD** denotes the possibility that any LOP "could" fail to stop an Incident propagation (pocket # 1 of its **PCR** in the upper position) (Figures 2–4).

In simple terms, if the LOP has a high PFD when demanded for protection by the process, its inverse, the RRF, will be low and insufficient to reduce the process risk up to or under the established tolerable risk level. This condition requires a redesigned LOP to lower its PFD or to add an improved LOP to get the required total risk reduction factor.

The greater the **RRF** required by the hazardous process to reach a "Tolerable" level, the lower the **PFD** of the respective layer of protection.

My SIL/RRF Graph, cited at the beginning of this article [1] permits a visualization of the relationship between PFD and RRF, also with the respective bands of Safety Integrity Level (SIL) for continuous, high, and low process demand modes.

The usual successive **LOPs** are the following (Figure 6):

- inherently safer designs (**ISD**);
- control instrumented system (**CIS**), also known as basic process control system (BPCS);
- monitoring/alarm systems and operator supervision;
- safety instrumented functions (**SIF**), integrated in a safety instrumented system (**SIS**);
- mechanical passive and active protecting devices (Relief valves, Rupture Disc, Dikes, etc.);
- mitigation devices;
- Emergency and Evacuation procedures; and
- Community Emergency procedures.

Essentially, for the field people, process safety means process risk reduction in all possible ways: Inherent Safer Designs, protecting devices, proper operation, proper procedures, proper testing, maintenance, etc.

RELIABILITY, INTEGRITY, AND DEPENDABILITY

Capable means having the ability and skill for doing a specific task no matter what.

We are using the term probability to value any kind of capability.

RELIABILITY is the probability (capability) that a device (LOP, Instrument, SIF, or Procedure) will properly perform the "intended" (desired, required, and expected) function it is requested to do (of course, under its stated operative conditions and limits and within the specified operating time).

In simple terminology, it should properly do the "task" it is requested and expected to do.

INTEGRITY is the Probability that a device (LOP, Instrument, SIF, or procedure) has the necessary strength, ability to respond, and hold up to achieve its intended function. This happens under the stated operative conditions and limits within the specified operating time.

For example, two men, one who is thin and one who is muscular, may have both the same capability for a specific task, but they will have not the same capability to support stressing conditions.

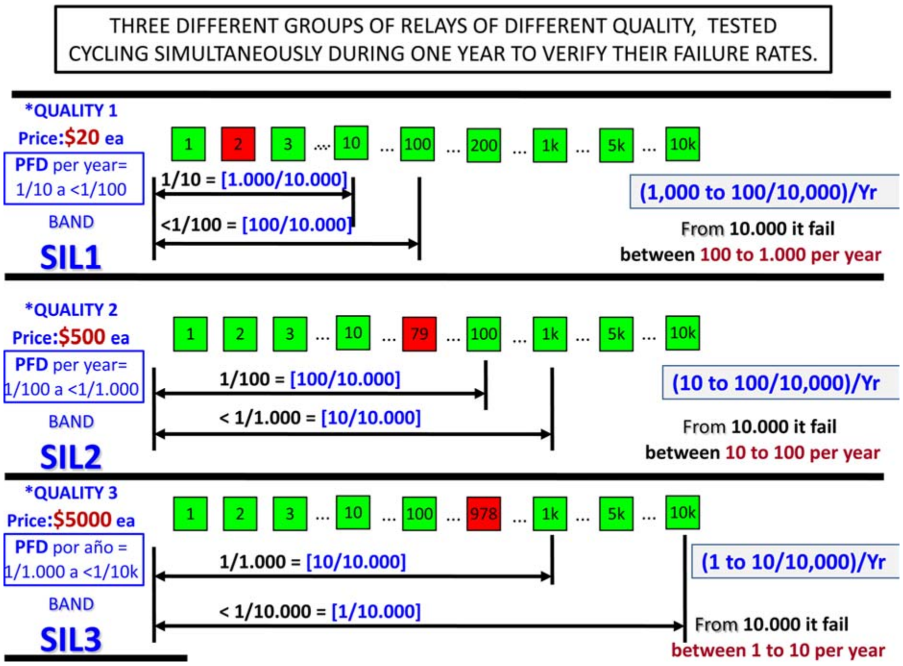

THREE DIFFERENT GROUPS OF RELAYS OF DIFFERENT QUALITY, TESTED CYCLING SIMULTANEOUSLY DURING ONE YEAR TO VERIFY THEIR FAILURE RATES.
*QUALITY 1
Price:$20 ea
PFD per year= 1/10 a <1/100
BAND
SIL1
1 2 3 ... 10 ... 100 ... 200 ... 1k ... 5k ... 10k
1/10 = [1.000/10.000]
<1/100 = [100/10.000]
(1,000 to 100/10,000)/Yr
From 10.000 it fail between 100 to 1.000 per year
*QUALITY 2
Price:$500 ea
PFD per year= 1/100 a <1/1.000
BAND
SIL2
1 2 3 ... 10 ... 79 ... 100 ... 1k ... 5k ... 10k
1/100 = [100/10.000]
< 1/1.000 = [10/10.000]
(10 to 100/10,000)/Yr
From 10.000 it fail between 10 to 100 per year
*QUALITY 3
Price:$5000 ea
PFD por año = 1/1.000 a <1/10k
BAND
SIL3
1 2 3 ... 10 ... 100 ... 978 ... 1k ... 5k ... 10k
1/1.000 = [10/10.000]
< 1/10.000 = [1/10.000]
(1 to 10/10,000)/Yr
From 10.000 it fail between 1 to 10 per year

Figure 10. Testing for failure rates. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

The difference resides in their PFD. The PFD by itself is the measure of the device capability (probability) to persist **Available**, ready to take care of a demand.

SILs are measures of device's **PFD**.

Within process safety science, four bands (levels) of PFD exist. They are known as SIL1, SIL2, SIL3, and SIL4. For better visualization, see the author's SIL/RRF Graph in Ref. 1.

DEPENDABILITY is what the user is asking for, that is, to be backed by devices and procedures with the adequate Integrity (Probability to not fail when demanded) accordingly with the process risk reduction required and also with the appropriate Reliability (capability to perform the required function).

PROCEEDING WITH THE PROCESS RISK REDUCTION

The necessary **RRF** needed to lower actual process risk has to be determined in reference to a pre-established Organization Risk Tolerance level.

This number is compared with the results of an adequate **PHA** and the calculated risk levels of the different scenarios of every "Hazard-Incident" pair, with

- **LOPA** (semiquantitative Layer Of Protection Analysis),
- or by using Quantitative Risk Assessment (**QRA**) assisted with a Fault Tree Analysis (**FTA**) and an Event Tree Analysis (**ETA**).

The difference signifies the needed protection layers.

The Center for Chemical Process Safety uses the acronym Hazard Identification and Risk Assessment (**HIRA**) to refer to the above task.

If you are still able to redesign your process, you should first attempt to reduce the risk by preventing hazardous initiating and/or enabling events by reducing the level of consequences and/or by reducing the probability of every incident outcome with an **ISD** [2].

If this is not possible or not adequate, the additional risk reduction steps should be done by implementing one or more appropriate LOPs.

As seen in Figures 6 and 7, the **PCR** with its "**U**" number will permit to visualize the PFD (or RRF) of every LOP. The above mentioned SIL/RRF Graph can be used effectively to fix and visualize the maximum permitted PFD (associated with the SIL level bands) of every implemented additional protecting barrier (LOP, SIF, device, or Procedure) included to protect the process against the respective linked "Hazard-Incident."

EXAMPLES OF PROBABILITY AND TIME AS RELATED TO PFD

The electromechanical relay (created about 1835) is a well-known electrically operated device used to switch contacts on and off to supply and interrupt power to other devices.

This electrical jewel is a very dependable and reliable device, with a high integrity level (very low PFD dangerous) that was extensively used from the 1920s to 1980s to integrate process protection systems. It is still used in small systems of fixed configurations that require limited commands and information to the operators. This is generally achieved by hardwired panels of lights, pushbuttons, and annunciators, like the burner management and safety systems (BMS) applied to command and protect small or medium size boilers.

Figure 10 show a (fictitious) test of 10,000 relays of three samples of different qualities (Samples S1, S2, and S3), all cycling at the same time (during 1 year), to determine their Probability of Failure "PF" within that year.

This information provides, with a probabilistic prediction, the PF of the different types of relays. This allows us to choose (and pay for) the proper relay to configure the most appropriate protection systems with the level of process risk that we want to prevent.

Relays can fail in two ways: by "not closing" (or not staying closed) the contacts when they must close or by "not opening" when they must open.

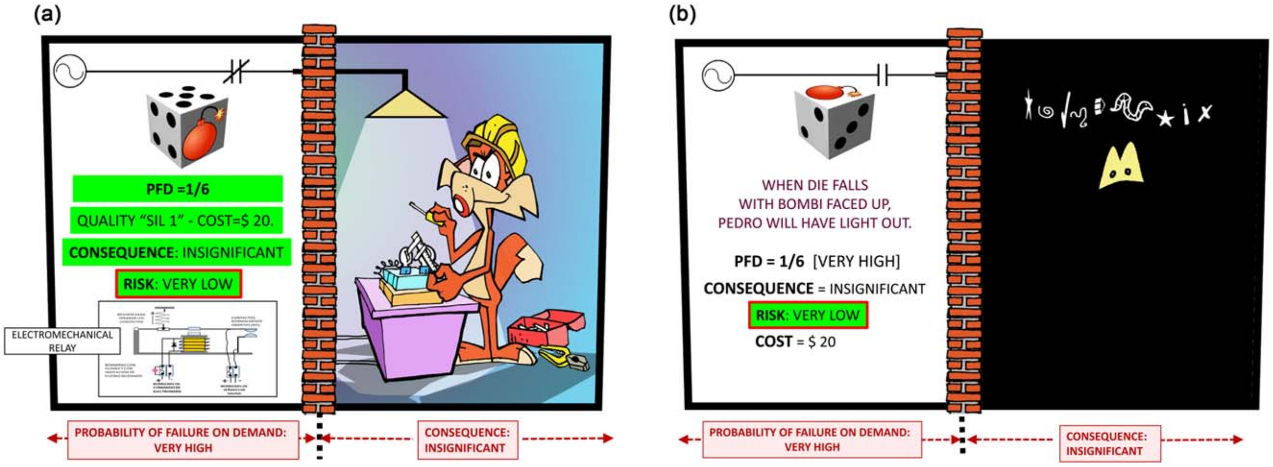

(a)
PFD =1/6
QUALITY "SIL 1" - COST=$ 20.
CONSEQUENCE: INSIGNIFICANT
RISK: VERY LOW
ELECTROMECHANICAL RELAY
PROBABILITY OF FAILURE ON DEMAND: VERY HIGH
CONSEQUENCE: INSIGNIFICANT
(b)
WHEN DIE FALLS WITH BOMBI FACED UP, PEDRO WILL HAVE LIGHT OUT.
PFD = 1/6 [VERY HIGH]
CONSEQUENCE = INSIGNIFICANT
RISK: VERY LOW
COST = $ 20
PROBABILITY OF FAILURE ON DEMAND: VERY HIGH
CONSEQUENCE: INSIGNIFICANT

Figure 11. (a) High probability, low consequence, low risk. (b) Low risk, a nuisance. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

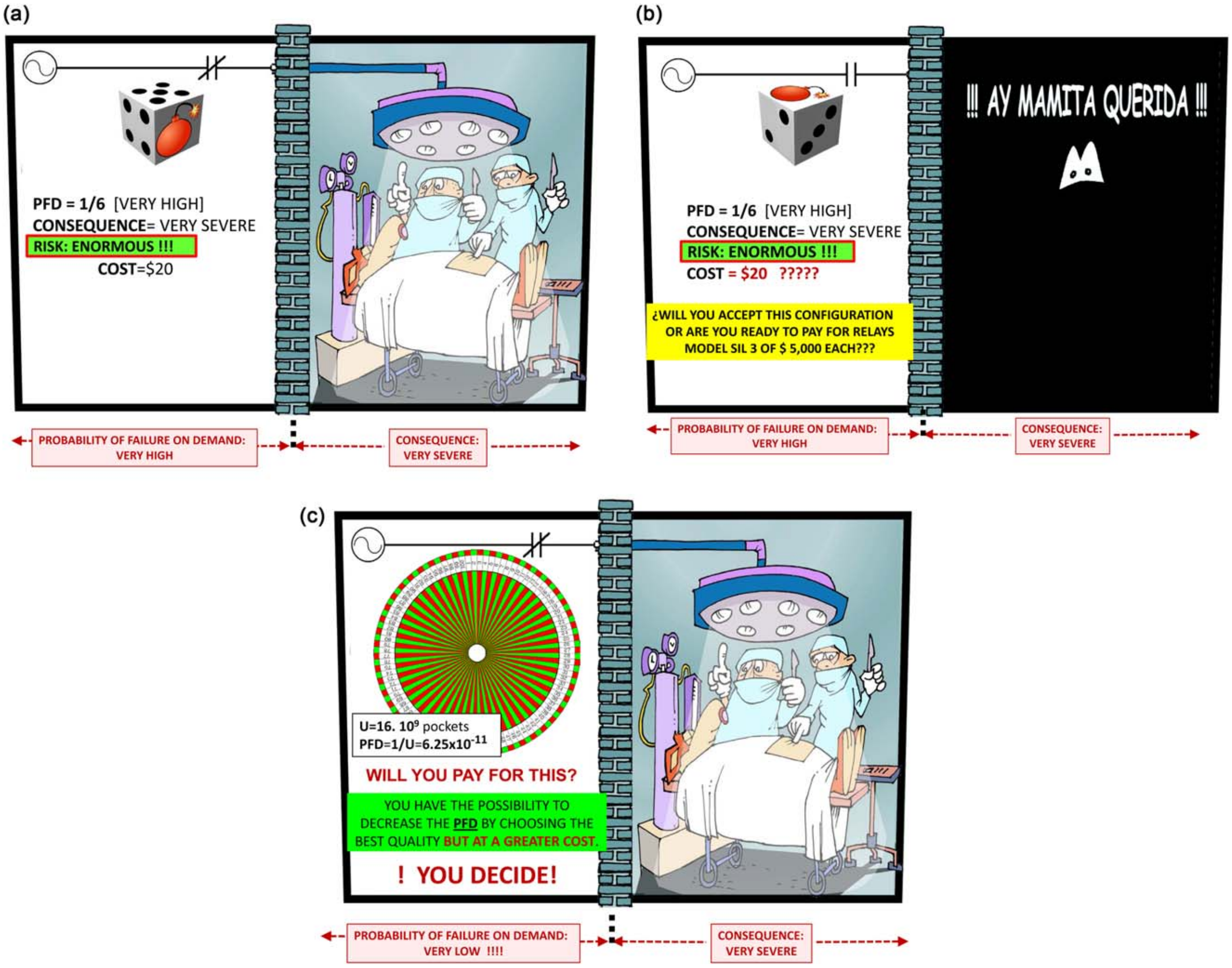
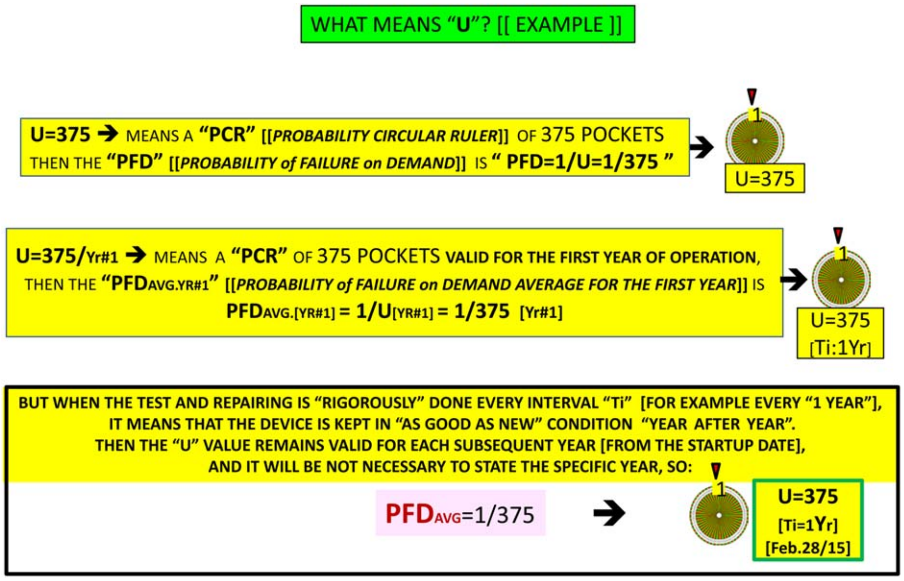

(a)
PFD = 1/6 [VERY HIGH]
CONSEQUENCE= VERY SEVERE
RISK: ENORMOUS !!!
COST=$20
PROBABILITY OF FAILURE ON DEMAND: VERY HIGH
CONSEQUENCE: VERY SEVERE
(b)
!!! AY MAMITA QUERIDA !!!
PFD = 1/6 [VERY HIGH]
CONSEQUENCE= VERY SEVERE
RISK: ENORMOUS !!!
COST = $20 ?????
¿WILL YOU ACCEPT THIS CONFIGURATION OR ARE YOU READY TO PAY FOR RELAYS MODEL SIL 3 OF $ 5,000 EACH???
PROBABILITY OF FAILURE ON DEMAND: VERY HIGH
CONSEQUENCE: VERY SEVERE
(c)
U=16. 10^9 pockets
PFD=1/U=6.25x10^-11
WILL YOU PAY FOR THIS?
YOU HAVE THE POSSIBILITY TO DECREASE THE PFD BY CHOOSING THE BEST QUALITY BUT AT A GREATER COST.
! YOU DECIDE!
PROBABILITY OF FAILURE ON DEMAND: VERY LOW !!!!
CONSEQUENCE: VERY SEVERE

Figure 12. (a) High probability, severe consequence, unacceptable high risk. (b) Enormous risk, scared. (c) Drastic probability reduction to feel safer and calm. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]



WHAT MEANS “U”? [[EXAMPLE]]

U=375 ➔ MEANS A “PCR” [[*PROBABILITY CIRCULAR RULER*]] OF 375 POCKETS THEN THE “PFD” [[*PROBABILITY of FAILURE on DEMAND*]] IS “ PFD=1/U=1/375 ” ➔ U=375

U=375/Yr#1 ➔ MEANS A “PCR” OF 375 POCKETS VALID FOR THE FIRST YEAR OF OPERATION, THEN THE “$PFD_{AVG.YR\#1}$” [[*PROBABILITY of FAILURE on DEMAND AVERAGE FOR THE FIRST YEAR*]] IS

$PFD_{AVG.[YR\#1]} = 1/U_{[YR\#1]} = 1/375$ [Yr#1] ➔ U=375 [Ti:1Yr]

BUT WHEN THE TEST AND REPAIRING IS “RIGOROUSLY” DONE EVERY INTERVAL “Ti” [FOR EXAMPLE EVERY “1 YEAR”], IT MEANS THAT THE DEVICE IS KEPT IN “AS GOOD AS NEW” CONDITION “YEAR AFTER YEAR”. THEN THE “U” VALUE REMAINS VALID FOR EACH SUBSEQUENT YEAR [FROM THE STARTUP DATE], AND IT WILL BE NOT NECESSARY TO STATE THE SPECIFIC YEAR, SO:

$PFD_{AVG}=1/375$ ➔ U=375 [Ti=1Yr] [Feb.28/15]

Figure 13. What means “U” **EXAMPLE++. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

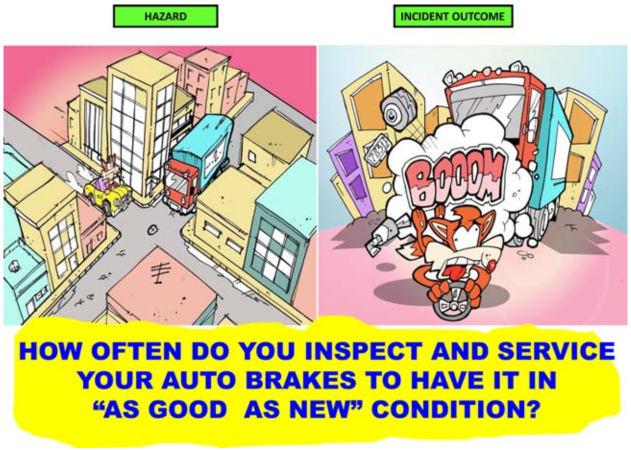

HAZARD
INCIDENT OUTCOME
BOOOM
HOW OFTEN DO YOU INSPECT AND SERVICE YOUR AUTO BRAKES TO HAVE IT IN “AS GOOD AS NEW” CONDITION?

Figure 14. Maintain brakes as good as new. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

WITH WHICH FREQUENCY YOU INSPECT AND SERVICE YOUR SAFETY EQUIPMENTS TO KEEP IT IN “AS GOOD AS NEW” CONDITION?
I THOUGHT, I BELIEVED... I AM SO SORRY...
TOO LATE !!

Figure 15. Maintain protection devices as good as new. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

Depending on the application, one of the above conditions will be dangerous and the other will be spurious and unwanted.

For fire suppression, the relays are integrated to operate as Energize To Trip in order to power the water deluge valve that will supply water to extinguish the fire.

In this case, the dangerous condition results when the contacts do not close when required to activate the valve.

For BMSs, the relays are configured to operate as De-energize To Trip in order to interrupt the power supply and deactivate the fuel shut off valves feeding the burners when a flameout occurs in the firebox.

In this application, a dangerous failure results when the contacts, which must be opened, remain closed.

Figures 11a, 11b, and 12a–12c show a greater understanding of the importance of paying higher cost to achieve a higher integrity (i.e., with lower dangerous PF on demand) depending on the type and level of risk of the application.

It becomes obvious that we are not going to require the same level of integrity for a relay to switch on or off a home bedroom light as we would for one required for a hospital surgical room.

We will consider now statistical figures of annual fatalities due to automobile accidents to estimate the probabilities of people suffering from those accidents.

Assuming that 45,000 fatalities occur within 1 year in a population of 45 million people means that the probability of a fatal car accident is “1 person per 1,000 per year” written as 1/1,000/year.

With this notation, we should be very careful to not misinterpret this figure as “1 fatal accident in 1,000 years,” which is obviously absurd.

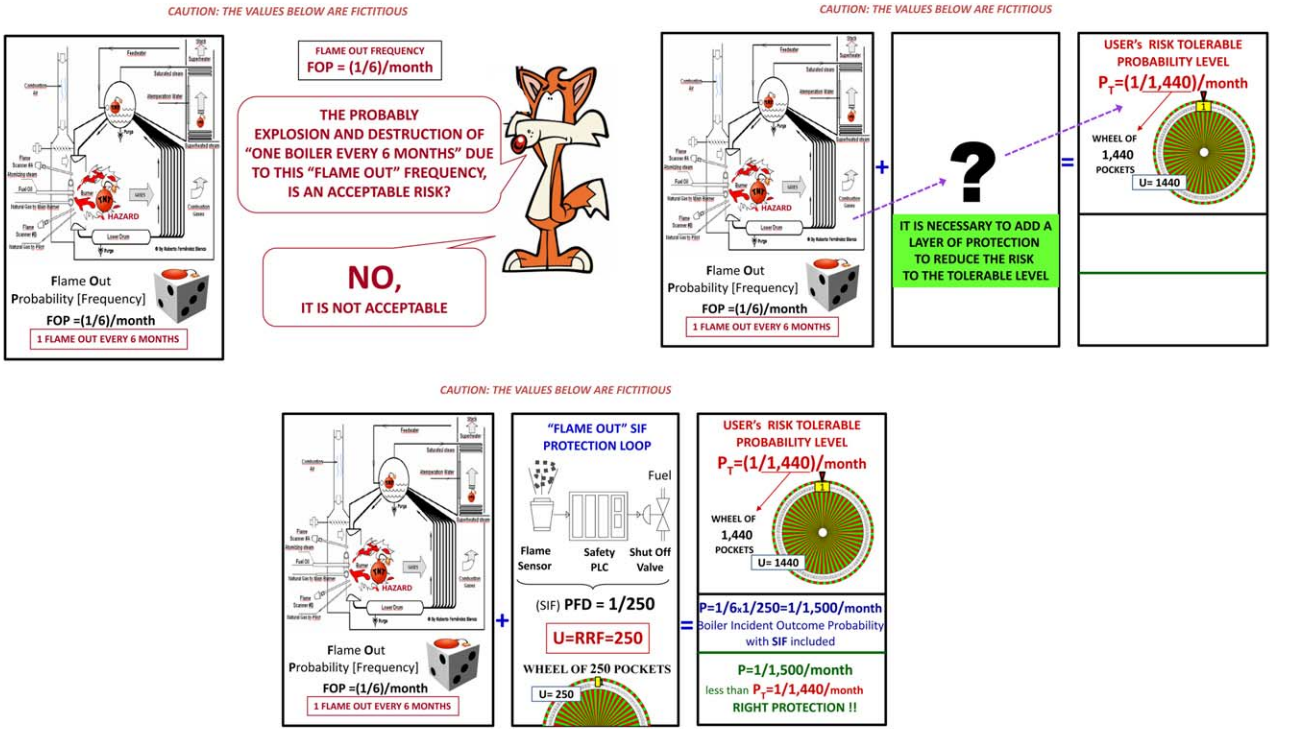

CAUTION: THE VALUES BELOW ARE FICTITIOUS
FLAME OUT FREQUENCY
FOP = (1/6)/month
THE PROBABLY EXPLOSION AND DESTRUCTION OF "ONE BOILER EVERY 6 MONTHS" DUE TO THIS "FLAME OUT" FREQUENCY, IS AN ACCEPTABLE RISK?
NO, IT IS NOT ACCEPTABLE
HAZARD
Flame Out Probability [Frequency]
FOP =(1/6)/month
1 FLAME OUT EVERY 6 MONTHS
CAUTION: THE VALUES BELOW ARE FICTITIOUS
+
?
IT IS NECESSARY TO ADD A LAYER OF PROTECTION TO REDUCE THE RISK TO THE TOLERABLE LEVEL
=
USER's RISK TOLERABLE PROBABILITY LEVEL
P_T=(1/1,440)/month
WHEEL OF 1,440 POCKETS
U= 1440
CAUTION: THE VALUES BELOW ARE FICTITIOUS
"FLAME OUT" SIF PROTECTION LOOP
Fuel
Flame Sensor
Safety PLC
Shut Off Valve
(SIF) PFD = 1/250
U=RRF=250
WHEEL OF 250 POCKETS
U= 250
P=1/6x1/250=1/1,500/month
Boiler Incident Outcome Probability with SIF included
P=1/1,500/month
less than P_T=1/1,440/month
RIGHT PROTECTION !!

Figure 16. (a) Unacceptable inherent boiler Probability of Flame Out [Fictitious]. (b) Layer of Protection required to reduce the risk. (c) Flame Out Layer of Protection [SIF]. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

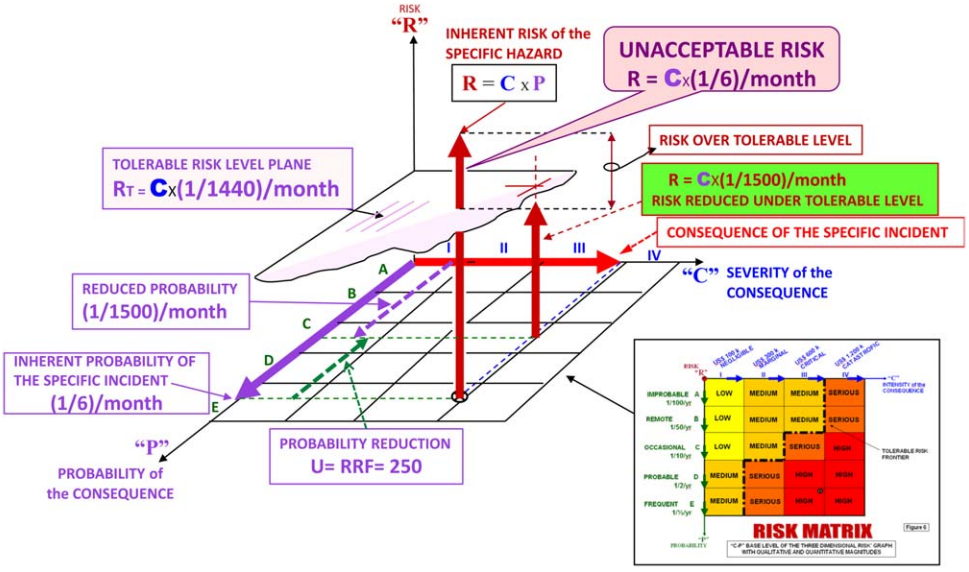

RISK
"R"
INHERENT RISK of the SPECIFIC HAZARD
R = C x P
UNACCEPTABLE RISK
R = Cx(1/6)/month
RISK OVER TOLERABLE LEVEL
TOLERABLE RISK LEVEL PLANE
RT = Cx(1/1440)/month
R = Cx(1/1500)/month
RISK REDUCED UNDER TOLERABLE LEVEL
CONSEQUENCE OF THE SPECIFIC INCIDENT
I
II
III
IV
"C" SEVERITY of the CONSEQUENCE
A
B
C
D
E
REDUCED PROBABILITY (1/1500)/month
INHERENT PROBABILITY OF THE SPECIFIC INCIDENT (1/6)/month
"P"
PROBABILITY of the CONSEQUENCE
PROBABILITY REDUCTION
U= RRF= 250
RISK "R"
US$ 100 k NEGLIGIBLE
US$ 300 k MARGINAL
US$ 600 k CRITICAL
US$ 1,200 k CATASTROFIC
"C" INTENSITY of the CONSEQUENCE
IMPROBABLE A 1/100/yr
REMOTE B 1/50/yr
OCCASIONAL C 1/10/yr
PROBABLE D 1/2/yr
FREQUENT E 1/½/yr
LOW
MEDIUM
SERIOUS
HIGH
TOLERABLE RISK FRONTIER
"P" PROBABILITY
RISK MATRIX
Figure 6
"C-P" BASE LEVEL OF THE THREE DIMENSIONAL RISK" GRAPH WITH QUALITATIVE AND QUANTITATIVE MAGNITUDES

Figure 17. Risk reduction. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

The safer way is to write a "PF per unit of time" (Failure frequency or Failure Rate) using parentheses. For example, (2/50,000)/year clearly means that from 50,000 equal devices in operation, two of them has the probability to fail "during this year."

Why Are We Emphasizing "This Year"?

Let us consider that this refers to a new automobile that you are purchasing. The auto manufacturer, an international and well-renowned company, has just released a new model with an estimation (backed by statistics) of a PF on Demand for the auto's brakes of "1 full brake failure", during the "first year" of use, in the total of the new 10,000,000 [[10^7]] cars sold.

As said before, if the notation is written to state "1/10,000,000/year," it is important to remember that this does not means the nonsense of 1/10,000,000 year (one total fail in 10,000,000 years), but means that 1 car's brake from 10,000,000 "could fail" during the "first year" of use.

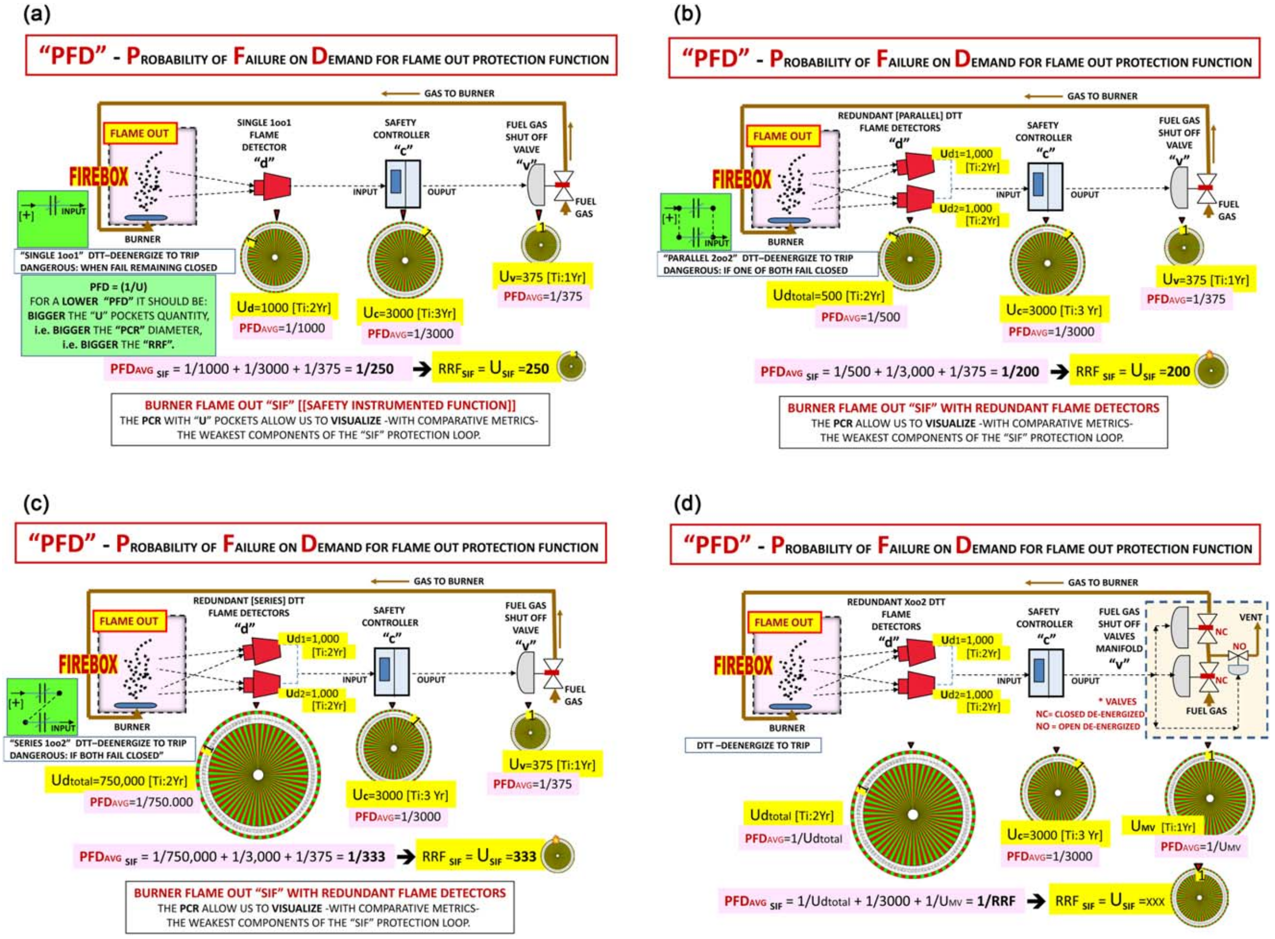

(a)
"PFD" - PROBABILITY OF FAILURE ON DEMAND FOR FLAME OUT PROTECTION FUNCTION
GAS TO BURNER
FLAME OUT
FIREBOX
SINGLE 1oo1 FLAME DETECTOR "d"
SAFETY CONTROLLER "c"
FUEL GAS SHUT OFF VALVE "v"
INPUT
OUPUT
FUEL GAS
BURNER
"SINGLE 1oo1" DTT–DEENERGIZE TO TRIP DANGEROUS: WHEN FAIL REMAINING CLOSED
PFD = (1/U) FOR A LOWER "PFD" IT SHOULD BE: BIGGER THE "U" POCKETS QUANTITY, i.e. BIGGER THE "PCR" DIAMETER, i.e. BIGGER THE "RRF".
Ud=1000 [Ti:2Yr]
PFDAVG=1/1000
Uc=3000 [Ti:3Yr]
PFDAVG=1/3000
Uv=375 [Ti:1Yr]
PFDAVG=1/375
PFDAVG SIF = 1/1000 + 1/3000 + 1/375 = 1/250 → RRF SIF = USIF =250
BURNER FLAME OUT "SIF" [[SAFETY INSTRUMENTED FUNCTION]]
THE PCR WITH "U" POCKETS ALLOW US TO VISUALIZE -WITH COMPARATIVE METRICS- THE WEAKEST COMPONENTS OF THE "SIF" PROTECTION LOOP.
(b)
"PFD" - PROBABILITY OF FAILURE ON DEMAND FOR FLAME OUT PROTECTION FUNCTION
GAS TO BURNER
REDUNDANT [PARALLEL] DTT FLAME DETECTORS "d"
Ud1=1,000 [Ti:2Yr]
Ud2=1,000 [Ti:2Yr]
SAFETY CONTROLLER "c"
FUEL GAS SHUT OFF VALVE "v"
FLAME OUT
FIREBOX
INPUT
OUPUT
FUEL GAS
BURNER
"PARALLEL 2oo2" DTT–DEENERGIZE TO TRIP DANGEROUS: IF ONE OF BOTH FAIL CLOSED
Udtotal=500 [Ti:2Yr]
PFDAVG=1/500
Uc=3000 [Ti:3 Yr]
PFDAVG=1/3000
Uv=375 [Ti:1Yr]
PFDAVG=1/375
PFDAVG SIF = 1/500 + 1/3,000 + 1/375 = 1/200 → RRF SIF = USIF =200
BURNER FLAME OUT "SIF" WITH REDUNDANT FLAME DETECTORS
THE PCR ALLOW US TO VISUALIZE -WITH COMPARATIVE METRICS- THE WEAKEST COMPONENTS OF THE "SIF" PROTECTION LOOP.
(c)
"PFD" - PROBABILITY OF FAILURE ON DEMAND FOR FLAME OUT PROTECTION FUNCTION
GAS TO BURNER
REDUNDANT [SERIES] DTT FLAME DETECTORS "d"
Ud1=1,000 [Ti:2Yr]
Ud2=1,000 [Ti:2Yr]
SAFETY CONTROLLER "c"
FUEL GAS SHUT OFF VALVE "v"
FLAME OUT
FIREBOX
INPUT
OUPUT
FUEL GAS
BURNER
"SERIES 1oo2" DTT–DEENERGIZE TO TRIP DANGEROUS: IF BOTH FAIL CLOSED"
Udtotal=750,000 [Ti:2Yr]
PFDAVG=1/750.000
Uc=3000 [Ti:3 Yr]
PFDAVG=1/3000
Uv=375 [Ti:1Yr]
PFDAVG=1/375
PFDAVG SIF = 1/750,000 + 1/3,000 + 1/375 = 1/333 → RRF SIF = USIF =333
BURNER FLAME OUT "SIF" WITH REDUNDANT FLAME DETECTORS
THE PCR ALLOW US TO VISUALIZE -WITH COMPARATIVE METRICS- THE WEAKEST COMPONENTS OF THE "SIF" PROTECTION LOOP.
(d)
"PFD" - PROBABILITY OF FAILURE ON DEMAND FOR FLAME OUT PROTECTION FUNCTION
GAS TO BURNER
REDUNDANT Xoo2 DTT FLAME DETECTORS "d"
Ud1=1,000 [Ti:2Yr]
Ud2=1,000 [Ti:2Yr]
SAFETY CONTROLLER "c"
FUEL GAS SHUT OFF VALVES MANIFOLD "v"
VENT
NC
NO
NC
FUEL GAS
* VALVES NC= CLOSED DE-ENERGIZED NO = OPEN DE-ENERGIZED
FLAME OUT
FIREBOX
INPUT
OUPUT
BURNER
DTT –DEENERGIZE TO TRIP
Udtotal [Ti:2Yr]
PFDAVG=1/Udtotal
Uc=3000 [Ti:3 Yr]
PFDAVG=1/3000
UMV [Ti:1Yr]
PFDAVG=1/UMV
PFDAVG SIF = 1/Udtotal + 1/3000 + 1/UMV = 1/RRF → RRF SIF = USIF =XXX

Figure 18. (a) Simplex flame out SIF. (b) Flame out SIF with redundant detectors 2oo2. (c) Flame out SIF with redundant detectors 1oo2. (d) Burner flame out "SIF" with redundant flame detectors and three valves shut-off manifold. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

This demonstrates the convenience of claiming the PF on demand per unit of time by writing it using parentheses and stating that this figure is "only valid" for the first year [year #1] of use of the new automobile, that is, $(1/10^7)$/year#1.

After a first year of use, the brakes will be worn making the PF on Demand "PFD" to be greater for the second year, even greater for the third year, and so on.

The PFD of any device in use (and wear) increases with time.

For a second year using the automobile in similar operating conditions, the auto company statistics state that the PFD increases to (25/10,000,000)/year#2 = (1/400,000)/year#2 meaning this that, for the second year of use, 25 cars out of 10,000,000 may have a total brake failure.

As everyone knows, to keep the brakes in "as good as new" (AGAN) condition requires a periodical full maintenance (inspection, verification, repairing, and testing).

Then, if you strictly repeat every year this full maintenance up to the "as good as new" condition, you will be able to continue using the initial PFD $= 10^7$/year figure for any following period Ti of 1 year.

So, you can now state, in your P&ID drawings or LOP diagrams, the "U" number together with the "Ti" Time interval and the date of the device start up in order to repeat every period Ti (1 year in this case) its maintenance to as good as new condition.

The notation could be as follows: [U $= 10^7$][Ti = 1 year] [08/may/15] (Figure 21).

But, if you do the repairs to "as good as new" condition every 2 years, then you must use the more conservative value of the second year, PFD = (1/400,000)/year#2 as valid for "any period Ti of 2 years."

The notation will be: [U $= 4 \times 10^5$] [Ti = 2 years][23/june/15] and you will work just with a PFDavg = 1/400,000.

Then, to be able to work with a "valid PFD average," it is necessary to have stated the "U" value together with the "startup date" and the "Time Interval Ti" when the full maintenance to "as good as new" condition must be repeated and recorded (Figure 13).

This is what must be done with any protecting device in any dangerous process plant (Figures 14 and 15).

WEAR OUT DATE

Any layer of protection has a period of "Safety-Related Useful Time" in which its Failure Rate remains relatively constant and the LOP, with its proper maintenance, is considered dependable in terms of integrity [availability] and reliability.

After this period, it becomes a final period where the equipment, having been subject to the process operating stress, starts to become weakened enough with the components becoming distressed, aged, weathered, and doing the failure rate to start to increase more significantly affecting the reliability and integrity of the device.

This stage is known as the "wear out or dying time frame," in which it is recommended to replace the entire unit

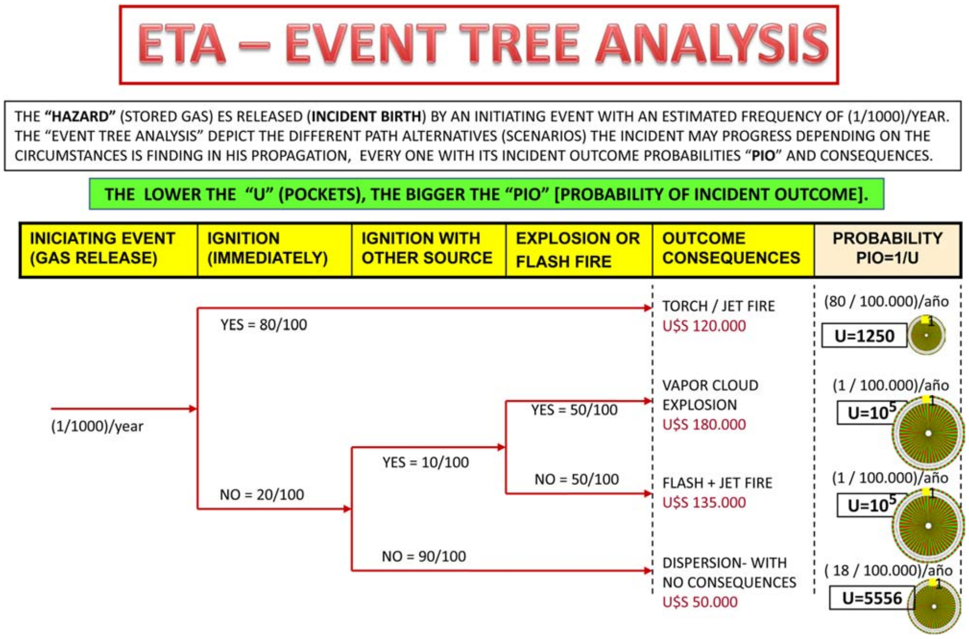

ETA – EVENT TREE ANALYSIS
THE "HAZARD" (STORED GAS) ES RELEASED (INCIDENT BIRTH) BY AN INITIATING EVENT WITH AN ESTIMATED FREQUENCY OF (1/1000)/YEAR. THE "EVENT TREE ANALYSIS" DEPICT THE DIFFERENT PATH ALTERNATIVES (SCENARIOS) THE INCIDENT MAY PROGRESS DEPENDING ON THE CIRCUMSTANCES IS FINDING IN HIS PROPAGATION, EVERY ONE WITH ITS INCIDENT OUTCOME PROBABILITIES "PIO" AND CONSEQUENCES.
THE LOWER THE "U" (POCKETS), THE BIGGER THE "PIO" [PROBABILITY OF INCIDENT OUTCOME].
INICIATING EVENT (GAS RELEASE)
IGNITION (IMMEDIATELY)
IGNITION WITH OTHER SOURCE
EXPLOSION OR FLASH FIRE
OUTCOME CONSEQUENCES
PROBABILITY PIO=1/U
(1/1000)/year
YES = 80/100
NO = 20/100
YES = 10/100
NO = 90/100
YES = 50/100
NO = 50/100
TORCH / JET FIRE
U$S 120.000
VAPOR CLOUD EXPLOSION
U$S 180.000
FLASH + JET FIRE
U$S 135.000
DISPERSION- WITH NO CONSEQUENCES
U$S 50.000
(80 / 100.000)/año
U=1250
(1 / 100.000)/año
U=10^5
(1 / 100.000)/año
U=10^5
(18 / 100.000)/año
U=5556

Figure 19. Probability circular ruler with "U" applied to visualize every "PIO"—probability of incident outcome. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

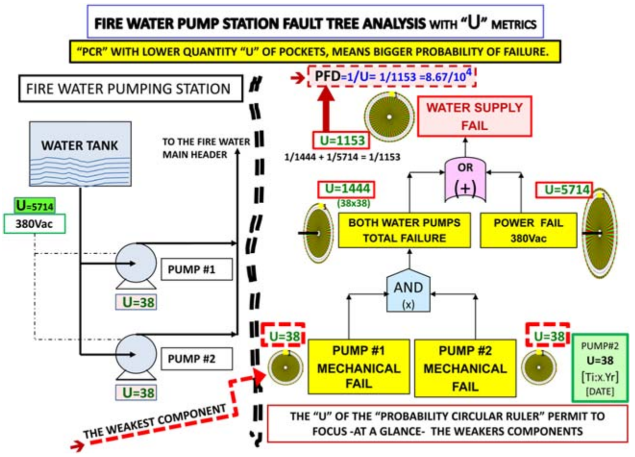

FIRE WATER PUMP STATION FAULT TREE ANALYSIS WITH "U" METRICS
"PCR" WITH LOWER QUANTITY "U" OF POCKETS, MEANS BIGGER PROBABILITY OF FAILURE.
FIRE WATER PUMPING STATION
WATER TANK
TO THE FIRE WATER MAIN HEADER
U=5714
380Vac
PUMP #1
U=38
PUMP #2
U=38
THE WEAKEST COMPONENT
PFD=1/U= 1/1153 =8.67/10^4
WATER SUPPLY FAIL
U=1153
1/1444 + 1/5714 = 1/1153
OR
(+)
U=1444
(38x38)
U=5714
BOTH WATER PUMPS TOTAL FAILURE
POWER FAIL 380Vac
AND
(x)
U=38
U=38
PUMP #1 MECHANICAL FAIL
PUMP #2 MECHANICAL FAIL
PUMP#2
U=38
[Ti:x.Yr]
[DATE]
THE "U" OF THE "PROBABILITY CIRCULAR RULER" PERMIT TO FOCUS -AT A GLANCE- THE WEAKERS COMPONENTS

Figure 20. Fire water pump station fault tree analysis. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

for a new one (or to make an integral overhaul) in order to prevent sudden unexpected dangerous failures with tragic consequences.

For this wear out time estimation, it is necessary to have from the manufacturer their declared or recommended "wear out time" (generally a laboratory number) which should be affected by the user with a factor considering the negative effects of the particular application to their process

(i.e., corrosion, erosion, high temperatures changes, vibrations, process pressure pulsations, etc.).

Then, in the Tagging Label, it could also be stated (Figure 21) the estimated wear out date "WO: date" as a reference to anticipate its probably ending of life.

Now, the tagging label will indicate the following data: [for example]

U = [RRF] = 2000
Ti = [full maintenance period] = 1 year
SD = [Startup Date]= 14/may/06
WO = [estimated Wear Out date] = 21/jun/11

APPLICATION EXAMPLES

In Figure 16a, we take (using fictitious values) an example of a boiler which has an unacceptable natural Flameout frequency of (1/6)/month (the Initiating Event Frequency, IEF), very far from the Organization Risk Probability Tolerable level of (1/1,440)/month.

This makes necessary including a LOP (Figure 16b).

In Figure 16c, we included a flameout SIF with a risk reduction factor of RRF = 250 (represented with a PCR of U = 250 pockets), which reduces the PFD to (1/1,500)/ month, lower than the required target.

Figure 17 depicts the Risk Reduction.

In Figure 18a, using PCR wheels, we can visualize the contribution of every component of the Flameout SIF and simultaneously realize that the PFD protective chain, probabilistically speaking, is weaker than it weakest link.

This weakest link (the shut-off valve in our example) becomes predominant in the SIF safety loop RRF.

Figures 18b and 18c demonstrate how the inclusion of a redundant Flame Detector strengthens the safety chain, but the weakest PFD device (the shut-off valve) always remains predominant.

As this safety valve must shut off the fuel gas flow with a plug/seat leakage seal class VI (high degree of gas-tight seal, hermetic) with a persistent high degree of integrity (low PFD), experience (as summarized in the NFPA 85 and 86) recommends the use of two of these shut-off valves in series and also a hermetic seal plug/seat vent valve in between (to reduce to zero the gas pressure in that section when the other two shut off the fuel gas supply) (Figure 18d).

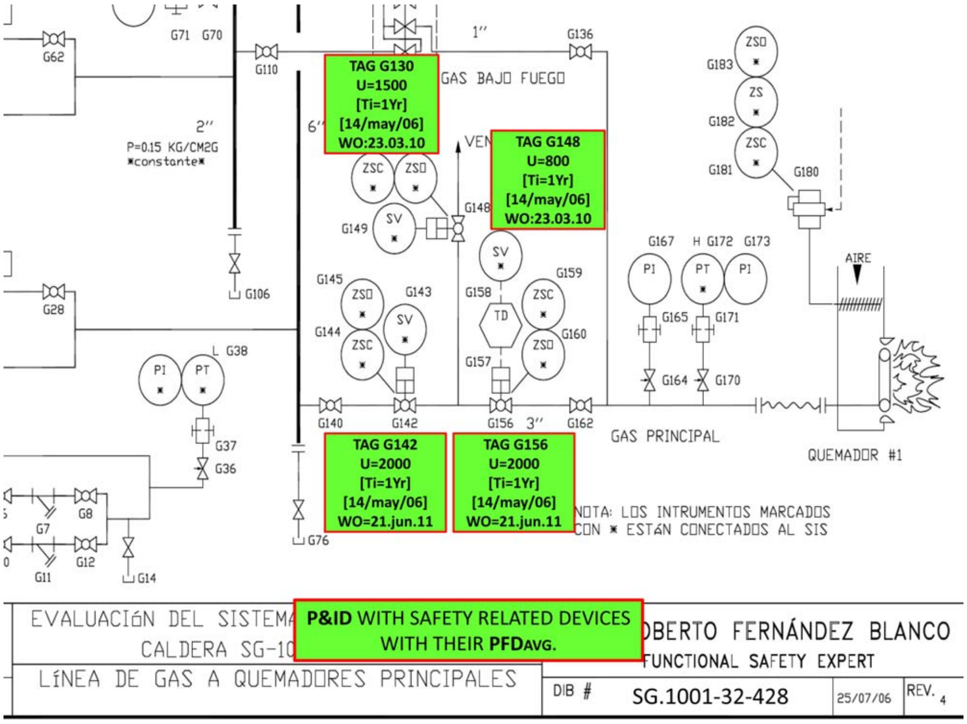


Figure 21. Partial view of a P&ID with proposed tag labeling of safety-related devices. [Color figure can be viewed in the online issue, which is available at **wileyonlinelibrary.com**.]

This three valves manifold substantially reduces the PFD avg. for the fuel gas shut off, but it is also mandatory to establish a rigorous timely test interval to verify and confirm the proper operation, the proper sequence, and the proper conditions of the valves seal leakage class VI.

Figures 19 and 20 exhibit the application of the PCR "U" values to the diagrams of an ETA and a FTA.

An indicating tag "[U = ?][Ti = ? year][Ti = date][WO = date]" can easily be included in any P&ID nearby to the respective safety related device, potential source of a dangerous initiating event, as shown in Figure 21 linked to the Fuel Gas Shut-Off and Vent valves.

TO SUM UP

Once a PCR has been visualized as a safety metric tool, it will be not necessary to draw the wheel.

It will be enough to simply state the "U" or RRF value, the Ti period, the starting date and (optionally) the estimated wear out date WO, as shown in Figure 21.

ACKNOWLEDGMENT

I express my gratitude to Ronald J. Wiley, Ph,D., PE and Mr. Arthur H. Baulch, Journal Specialist, Technical Publications (AIChE) for their assistance in the preparation of this article.

LITERATURE CITED

1. R. Fernández Blanco, Understanding hazards, consequences, LOPA, SILS, PFD and RRF as related to risk and hazard assessment, Process Saf Prog 33 (2014), 208–216, Available at (in Spanish): **http://www.dasiscorp.com/pdf/SN-516-11-Articulo-SIL-or-RRF-para-CCPS.pdf** and (in English): **http://www.dasiscorp.com/pdf/SN-516-11-English-SIL-or-RRF-for-CCPS.pdf**.
2. CCPS, Inherently Safer Chemical Processes: A Life Cycle Approach, 2nd Edition, Wiley-AIChE, Hoboken, NJ, 2008.