The systematic integration of Human Factors into safety analyses: an integrated engineering approach

S. Colombo

Politecnico di Milano, Dipartimento di Chimica, Materiali e Ingegneria Chimica "G. Natta", Piazza Leonardo da Vinci, 32, 20133, Milan, Italy, simone.colombo@polimi.it

M. Demichela

Politecnico di Torino, Dipartimento di Scienza dei Materiali e Ingegneria Chimica, Corso Duca degli Abruzzi, 24, 10129, Turin, Italy

ABSTRACT: The performance of the Human Reliability Analysis (HRA) and integration of its outcomes into QRA schemes remains a quite difficult and complex task to perform. Even worse is the assessment of Organisational Reliability Assessment (ORA). The reasons of this difficulty mainly lay on the absence of a generically accepted paradigm that enables engineers to include systematically H&OF (Human & Organisational Factors) into the analysis. Broadly speaking, engineering approaches very often account for Error of Omission (EOO) forgetting the Errors of Commission (EOC), and, on top of that, they do not make any macro distinction between pre- and post-initiating human failures. This paper offers a paradigm on how to integrate H&OF into safety analysis by means of the Recursive Operability Analysis (ROA), which has been adapted to accommodate H&OF, and renamed Integrated Recursive Operability Analysis (IROA). By means of a practical example, the method will illustrate how to account for H&OF in a systematic and consistent manner using an engineering approach. The paper will even provide a paradigm for the construction of Integrated Fault Trees (IFT) consistent with the IROA framework.

1 INTRODUCTION

Incorporating Human Factors (HF) into safety analyses is a rather difficult and complex exercise. Indeed, engineers still find it difficult both to incorporating Human & Organisational (H&O) sources of risk into their daily analyses and to realistically quantify them. This is witnessed by the diffused practice of taking them into account only at a later stage of the analysis, when the human contribution, often reflecting only the contribution of sharp-end operators to the risk, is accounted for and analyzed vis-à-vis the dreamt accidental scenario. In practice, this means that a Human Reliability Assessment (HRA) is not performed and integrated into the safety analysis in a systematic and consistent manner but it is simply an added-on piece of information accommodated *ex-post* into the analysis.

Aim of this paper is to provide an improved methodological framework, with respect to that already proposed by S. Colombo et al. [1], that can ease the way in which safety analysts may account for H&OF since the early stages of their analyses. The present work builds on the conceptual scheme of the Recursive Operability Analysis (ROA) [2][3][4]; the step forward of the well known HAZOP [5][6][7][8].

The reason to grounding the work of the Human Failure Identification (HFI), within the broader HRA scheme, on the ROA framework, relates to the three positives aspects this technique holds compared to its predecessor. The first one is the easiness with which logic trees can be directly derived once the ROA is completed. It is a "virtually automatic transition to the quantification stage" [4]. The second advantage relates to the conceptual and numerical accuracy with which the analyses are performed [9, 10]. Actually, the ROA scheme, by rule, imposes the use of the inhibit logic gate (INH) which, despite its conceptual correctness [9], is not much used in the daily practice as often substituted by the "and" logic gate (AND). The third not negligible aspect, which makes the ROA a powerful technique, relates to the possibility of easily making conceptual cross checks throughout the analysis, thus allowing congruence verification between the ROA and the subsequent Fault Trees and Event Trees. This task is very hard to perform whether a classical operability analysis, applying the tedious and sometime misleading guide words, is used. These capabilities of the ROA and its versatility to modelling very complex situations are described in a number of papers [4][11][12][13].

In the present work, the ROA procedure is modified in order to allow for H&OF being directly and systematically taken into account during the Operability Analysis; this additional "virtue" enables to identifying explicitly the need for interfaces with the HRA.

2 RECURSIVE OPERABILITY ANALYSIS

The classical ROA is performed by means of a clearly structured framework which, if systematically filled in according to plant's streams and nodes, drives the analyst to unveil all potential hazards associated with the specific plant at hand.

The execution of an ROA may be heavily dependent on the proper division of a plant: boxes A, B, C and W in the flow diagram (Fig. 1) are dedicated to a check for this purpose. Another preliminary operation is the identification of the boundary nodes and those internal to each sub-system - |Box D|, i.e. the points where deviations of a process variable (temperature, pressure, etc.) may develop or propagate. These points must be suitably numbered. This operation must naturally go hand in hand with the identification of the process variables regarded as significant for the analysis-|Box E|.

The OA itself actually begins at box F. The details of the process from this box onwards will now be described.

|Box F|- A plant is usually analysed according to its flow lines. It is thus advisable to take a boundary node of the first sub-system as the starting point. |Box G|-The first process variable chosen to start the analysis is selected.

Its significant deviations from the stable operating conditions are examined|Box H|- and then the protection (or shutdown) systems able to intervene-|Box X|. |Box I|-Identification of a 'Deviation' (column 1) is followed by the search for all its 'Possible causes' (column 2).

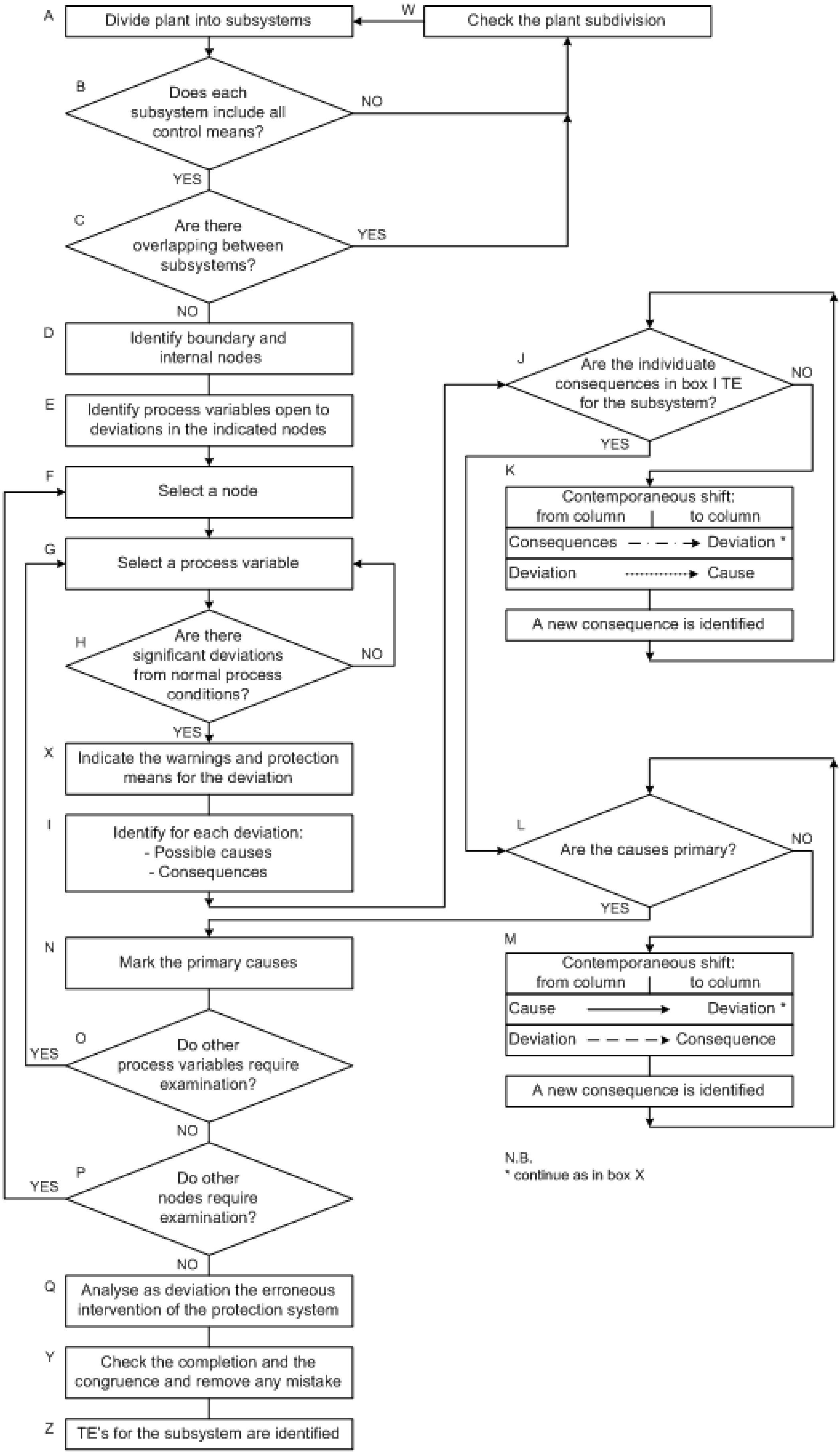

A
Divide plant into subsystems
W
Check the plant subdivision
B
Does each subsystem include all control means?
NO
YES
C
Are there overlapping between subsystems?
YES
NO
D
Identify boundary and internal nodes
E
Identify process variables open to deviations in the indicated nodes
F
Select a node
G
Select a process variable
H
Are there significant deviations from normal process conditions?
NO
YES
X
Indicate the warnings and protection means for the deviation
I
Identify for each deviation:
- Possible causes
- Consequences
J
Are the individuate consequences in box I TE for the subsystem?
NO
YES
K
Contemporaneous shift:
from column
to column
Consequences
Deviation *
Deviation
Cause
A new consequence is identified
L
Are the causes primary?
NO
YES
M
Contemporaneous shift:
from column
to column
Cause
Deviation *
Deviation
Consequence
A new consequence is identified
N.B.
* continue as in box X
N
Mark the primary causes
O
Do other process variables require examination?
YES
NO
P
Do other nodes require examination?
YES
NO
Q
Analyse as deviation the erroneous intervention of the protection system
Y
Check the completion and the congruence and remove any mistake
Z
TE's for the subsystem are identified

Fig. 1: Flow chart for the construction of a ROA.

These causes are separated from each other by a dashed line if they are linked by an OR gate, and joined by the ampersand (symbol &) if they are linked by an AND gate. The 'Consequences' expected from the 'Deviation' if the protection devices fail or are not present are placed in column (3).

|Box J|-At this point, having traced the origin of the causes, one investigates the gravity of the consequences. If one consequence is critical, i.e. appears as a Top Event (TE), it must be indicated in column (7) with a progressive number. In any event, to be identified as a TE a consequence must be the outcome of deviations for which protection systems have failed to come into action, or were not provided (Fig. 5).

|Loop K-J|-In the same way, if the first consequence is not a TE and hence conclusive for the analysis, it must be further analysed until either the consequence regarded as final is reached, or all the consequences regarded as possible and likely for the entire plant have been examined.

It will be seen, in fact, that each consequence is a deviation from the normal situation and, as such, can provoke other more serious consequences (domino effect) that are identified as follows.

|Box K|-The intermediate consequence is now converted into a deviation by shifting column (3) to column (1) (– · –➤) and its deviation is then automatically transformed into a cause by shifting column (1) to column (2) (········➤): one or more new consequences are identified.

The analysis is now continued by tracing back to the origin of the cause identified. This is done by moving from one node to the next along the flow lines of the process, using simple logic rules applied to columns (1), (2) and (3).

|Box L|-If the causes identified in box I are regarded as primary at the depth of analysis obtainable at this level, they are given an appropriate distinguishing mark, such as an asterisk -|Box N|, if not, they require further analysis. They are, in fact, other deviations from the normal operating conditions provoked by other causes that are identified as follows.

|Box M|- Non-primary causes are further examined by regarding them as deviations. The content of the item in column (2) is thus included in column (1) as well (⟶) and since this 'Deviation' must have a 'Consequence', column (1) must be shifted to column (3) (– – ➔). In this way, new causes are identified.

|Loop M-L|- Systematically one works up from a cause as a deviation to the causes regarded as primary with reference to the consequence identified in box I. It is worth noting that this development of the analysis automatically leads to the boundary nodes, which means that the adjoining sub-system must be analysed.

It should also be noted that combination of the two procedures Loop K-J and Loop M-L both ensures that the analysis is congruent and permits connection between branches in the subsequent logic tree development.

|Box 0|- Completes the inquiry for all the process variables identified in box E.

|Box P|-The analysis ends for all the nodes comprised in box D.

|Box Q|-If no unwanted consequences due to spurious intervention of the protective systems emerge after following the flow lines, it is essential for these deviations to be analysed separately. |Box X|- Each time a deviation is noted in box I or in the course of Loop K-J and M-L, columns (4) and (5) must show:

- the optical and acoustical devices installed to give warning of the deviation,

- the automatic protective or shutdown means provided for each deviation.

│Box Y│- Moreover, a completeness check to ensure that all the nodes identified and their process variables have been duly analysed should be made at this stage by scanning the head of each form. Following the column (1), (2) and (3) shifts for each deviation, cause and consequence must also carry out an OA congruence check.

│Box Z│-The analysis ends with the identification of all TE's.

In the example detailed in [2], a chef's assistant of a busy restaurant, is in charge to timely producing crispy and dry French fries while assisting the chef in preparing more complicated dishes (a classical batch process). The process plant used by the assistant for this goal is that of Fig. 2.

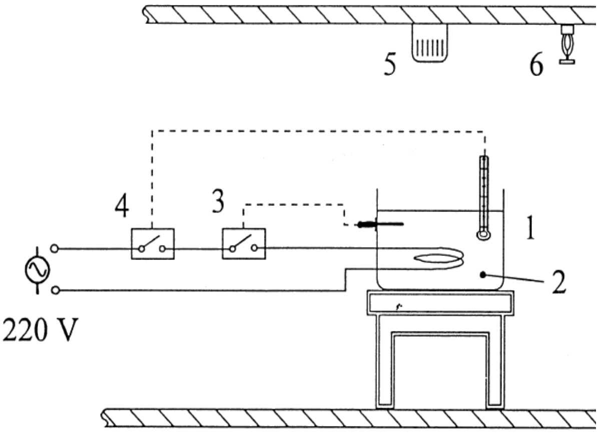
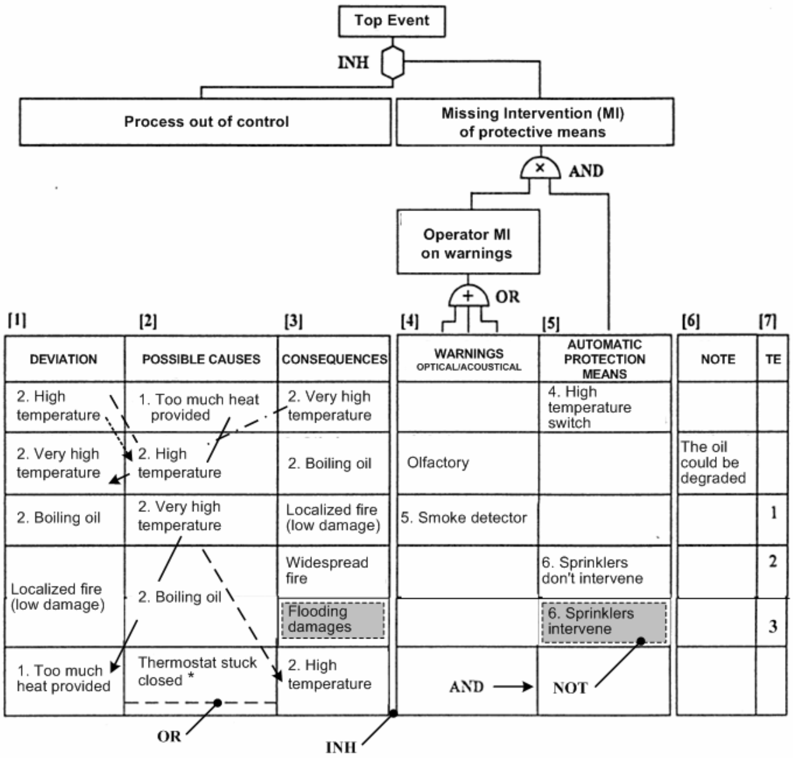


Fig. 2: Layout of the plant (1 Deep-Fryer, 2 Oil, 3 Thermostat, 4 High T cut off switch, 5 Smoke detector, 6 Sprinkler) as reported in [2]

The ROA application brings to the results in Figure 3.



[1]	[2]	[3]	[4]	[5]	[6]	[7]
DEVIATION	POSSIBLE CAUSES	CONSEQUENCES	WARNINGS OPTICAL/ACOUSTICAL	AUTOMATIC PROTECTION MEANS	NOTE	TE
2. High temperature	1. Too much heat provided	2. Very high temperature		4. High temperature switch		
2. Very high temperature	2. High temperature	2. Boiling oil	Olfactory		The oil could be degraded	
2. Boiling oil	2. Very high temperature	Localized fire (low damage)	5. Smoke detector			1
Localized fire (low damage)	2. Boiling oil	Widespread fire		6. Sprinklers don't intervene		2
		Flooding damages		6. Sprinklers intervene		3
1. Too much heat provided	Thermostat stuck closed *	2. High temperature	AND →	NOT		

Fig. 3: ROA framework as reported in [2]

3 INTEGRATED RECURSIVE OPERABILITY ANALYSIS (IROA)

To facilitate the understanding of the IROA it was decided to extend the example made in reference [2] and above described. In this revised version, the first level of protection, i.e., the apparatus 4 in the plant's layout, is made up of two components, namely (1) the high temperature LED and (2) the switch.

The assistant starts preheating the oil so to be ready when chips are to be timely produced to garnish chef's dishes. Not surprisingly, this protective mean turns off the appliance too often than desired during operations. Despite being quite inexperienced, the assistant has discovered the possibility to by-pass the switch. The assistant, after a while, decides to by-pass the high temperature switch so to avoid further blames of the chef for the delay in producing the desired chips. Actually, he/she is persuaded that, adopting this "escamotage", he/she can manage to produce chips in time without impinging on safety.

3.1 *Classical ROA vs. IROA*

From column 4 in Fig. 3 it appears quite clear that the human intervention is usually modelled as an operator Missing Intervention (MI) on warnings, while the identification of possible causes due to error of commission or other human related failures is left to the sensibility of the analyst.

From a HF perspective this approach is quite reductive and, thus, far from being realistic. Actually, in reality, due to the many stimuli received in the working environment, operators intervene on the system any time they are prompted to do it either by explicit warnings and alarms or by environmental hints. Even beyond this, they intervene both on the system and on the organisational set-up, unless there are suitable barriers, either software or hardware, preventing them to do it or helping them not to do it.

Typical example is that of by-passing the so-called Engineered Safety Features (ESF), in our case the apparatus 4, or ignoring procedures that, quite often, are perceived by operators more as disturb than a support to safer performing daily tasks.

In order for safety analyses to be realistic, credible, and effective, i.e., to be a support or a tool for decision-making, all these intangible aspects must be properly modelled. And this is what the IROA attempts to do.

3.2 *The IROA framework*

Basically, the IROA framework is similar to that of the classic ROA but with some added features that enable to accommodating systematically H&OF into the process. As reported in Figure 4, this is achieved with a minor modification of the flowchart of the classical ROA, and consequently of the frame for the analysis.

The main frame of the IROA is still made up of 2 blocks. According to the inhibit concept, the former block is devoted to the identification of those hazards that drive the system out of control, while the latter is conceived to modelling the effectiveness of protective systems.

Before analysing the chef's assistant work with the IROA conceptual scheme, it is worth briefly explaining where the IROA differs from its predecessor, with reference to the IROA tables in Figure 5.

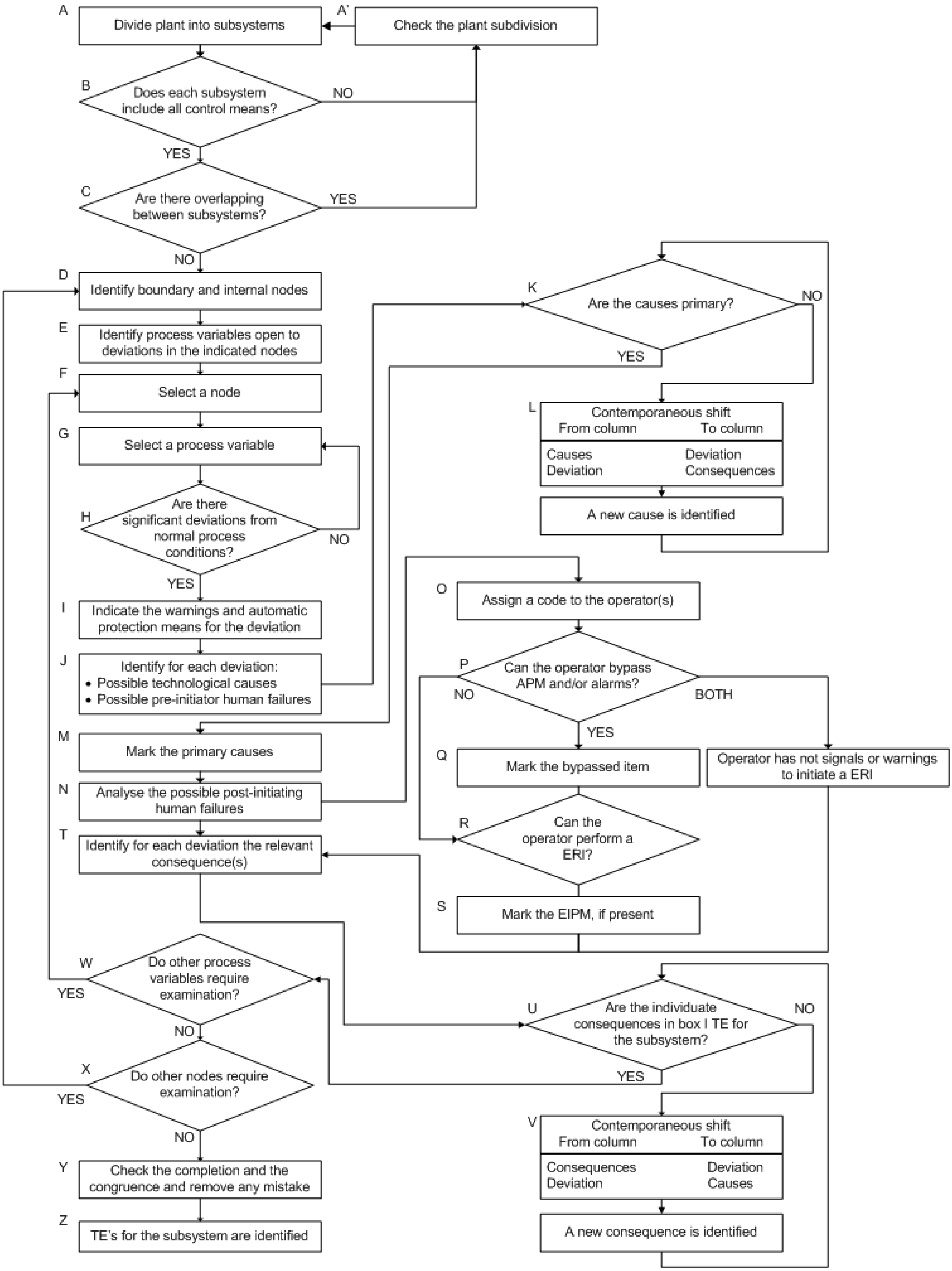

A
Divide plant into subsystems
A'
Check the plant subdivision
B
Does each subsystem include all control means?
NO
YES
C
Are there overlapping between subsystems?
YES
NO
D
Identify boundary and internal nodes
E
Identify process variables open to deviations in the indicated nodes
F
Select a node
G
Select a process variable
H
Are there significant deviations from normal process conditions?
NO
YES
I
Indicate the warnings and automatic protection means for the deviation
J
Identify for each deviation:
• Possible technological causes
• Possible pre-initiator human failures
K
Are the causes primary?
NO
YES
L
Contemporaneous shift
From column
To column
Causes
Deviation
Deviation
Consequences
A new cause is identified
M
Mark the primary causes
N
Analyse the possible post-initiating human failures
O
Assign a code to the operator(s)
P
Can the operator bypass APM and/or alarms?
NO
BOTH
YES
Q
Mark the bypassed item
Operator has not signals or warnings to initiate a ERI
R
Can the operator perform a ERI?
S
Mark the EIPM, if present
T
Identify for each deviation the relevant consequence(s)
W
Do other process variables require examination?
YES
NO
U
Are the individuate consequences in box I TE for the subsystem?
NO
YES
X
Do other nodes require examination?
YES
NO
V
Contemporaneous shift
From column
To column
Consequences
Deviation
Deviation
Causes
A new consequence is identified
Y
Check the completion and the congruence and remove any mistake
Z
TE's for the subsystem are identified

Fig. 4: IROA flow chart

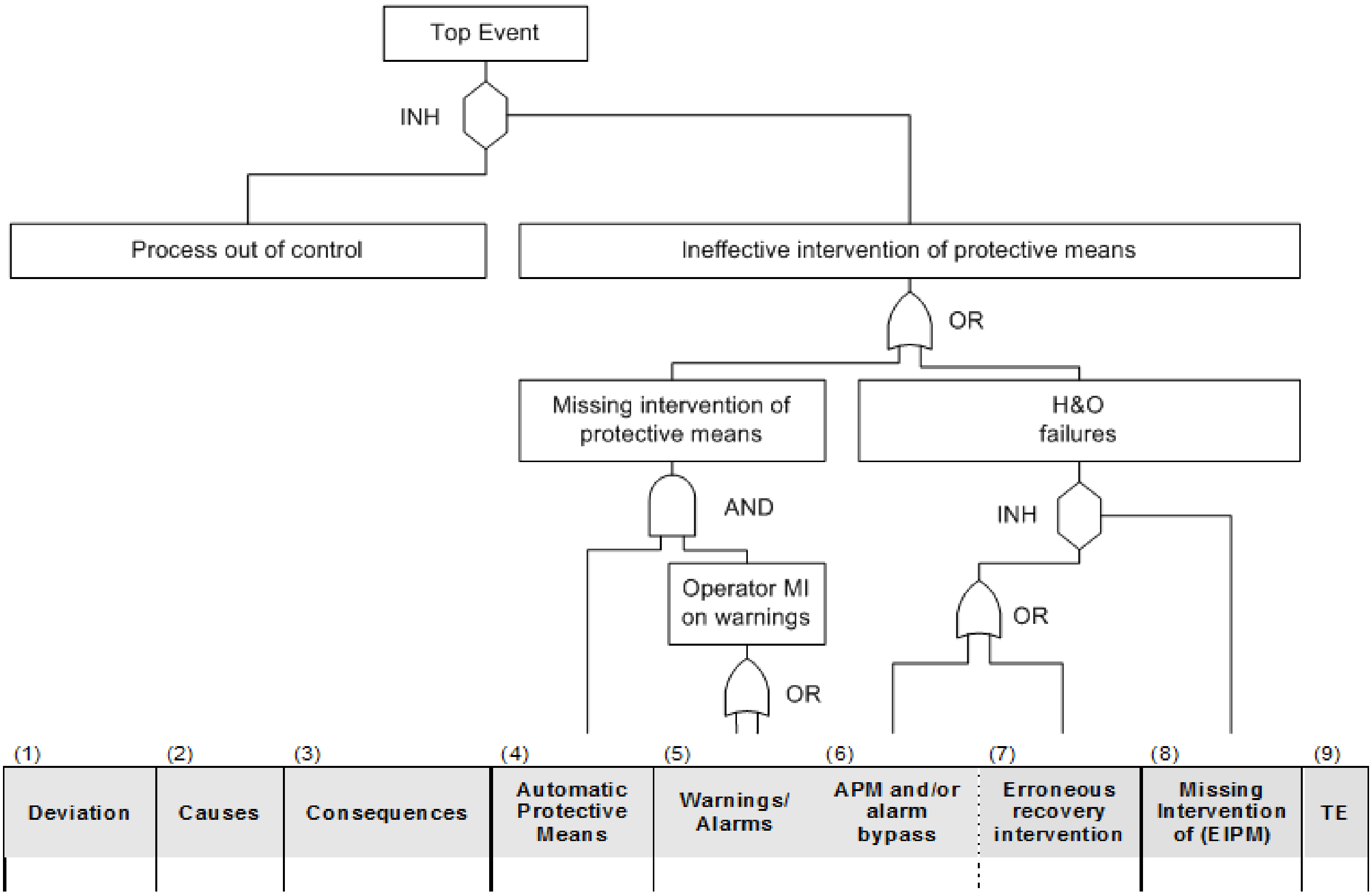

Top Event
INH
Process out of control
Ineffective intervention of protective means
OR
Missing intervention of protective means
H&O failures
AND
INH
Operator MI on warnings
OR
OR
(1) Deviation
(2) Causes
(3) Consequences
(4) Automatic Protective Means
(5) Warnings/ Alarms
(6) APM and/or alarm bypass
(7) Erroneous recovery intervention
(8) Missing Intervention of (EIPM)
(9) TE

Fig. 5: IROA framework

Block 1

In order to allow for the human contribution permeating the analysis any time there is, or there should and/or could be, an interaction between the technology and/or the organisation and the human, and not only when the system fails to control itself, the block 1 was modified. This modification enables to explicitly identifying the root causes deriving from a human failure and originating a process deviation (see boxes J & N, Figure 4).

As anticipated above, the first block, i.e., that grouping column 1 to 3 in Fig. 5, is devoted to the identification of those primary events that leads the system out of control. In this part of the analysis even human failures are now accounted for in an integrated fashion together with technological ones. In particular, human interventions in this block have to be modelled as pre-initiators of events, meaning those acts which contribute to let system's components to fail or be in an undetected failing state. In the IROA scheme pre-initiating human failures are modelled, together with the technological ones, in column 2 with the aim to unveil primary human-related root causes.

Essentially, in the classical ROA scheme the technological causes are investigated through the recursive mechanism until primary causes are identified. Actually, primary causes correspond to events which are possible to associate a frequency of occurrence to.

To keeping consistency throughout the analysis, the same approach must apply even for the identification human failures, no matter whether they represent pre-initiating or post-initiating human failures. And this is what has been done while moulding the IROA process. The interface with the HRA has then been made explicit and systematically incorporated into the assessment, thus allowing the analyst to identifying the type of human failures involved and the associated frequency of occurrence.

The types of human failures to identify are dependent on the taxonomy adopted, which can follow either an "informal" heuristic approach or a more formal and structured cognitive model. The same applies for the quantification step, which is strongly dependent on the method used to quantifying the Human Error Probabilities (HEP). Amongst the most advanced second-generation methods, one can find ATHEANA [14], CREAM [15], MERMOS [16], and the like.

The most famous heuristic taxonomy is the one proposed by Swain and Guttmann [17]. According to this taxonomy human failures can be subdivided into three main categories, namely, (1) Error of Omission (EOO) – acts omitted (not performed), (3) Error of Commission (EOC) – acts performed inadequately; or in the wrong sequence; or too early or too late, (3) Extraneous acts – wrong or not required actions performed.

The second category also includes errors of quality, i.e., those errors characterising a human failure in the sense of non-exact achievement of the aimed goal, such as too great or too small an extent or degree. To put it differently, they represent an ineffective action. This is why we named the second block of the IROA, the one supposed to stop the process out of control (right harm of the INH gate), ineffective intervention of protective means. Certainly, human beings, i.e., operators, can be conceived, despite in a dry definition, protective means.

This simple approach encompasses virtually all kinds of human failures that are likely to occur. It is clearly pretty coarse and it does not allow to sharply discriminating amongst many types of failures.

To make it sharper it can be conveniently coupled with another heuristic taxonomy by Spurgin et al [18], which is "context oriented" and involves the following categories:

- Maintenance-testing failures by which operators fail to restore system's components and affecting the system availability, i.e., latent failures (what we called pre-initiating human failures);
- Triggering failures by which operators can initiate an event/accident sequence;
- Recovery failures by which operators fail to recover from a system upset/deviation;
- Misdiagnosis failures by which operators can prolong, intensify or aggravate the scenario dynamics;
- Restoring failures by which operators fail to restore apparatus initially unavailable to the system.

Typically, for sake of simplicity, in this sample use case pre-initiator human interventions will be of the kind of missing or erroneous intervention during maintenance, inspection, repair or modification, i.e., those creating latencies in the system.

Block 2

Block 2, instead, is devised to identifying and accommodating post-initiator human interventions, i.e., those human actions which contribute either to prevent the dangerous transient to further proceed to Top Event (TE) or to worsen it by accelerating its occurrence (co-causes).

Considering the innate flexibility humans hold, they should be involved, i.e., modelled in the analyses, in a way that depicts more convincingly the natural interaction between them and the system. In reality, operators go hand in hand with the process scrutinizing its behaviour often applying, more or less consciously, a symptoms-based approach.

This approach, even if quick and effective for most of the cases, lacks of far-seeing and can be responsible of rash judgments which, in turn, can lead to human failures. This latency of humans to promptly, for not saying impulsively, react on weak signals should, too, find its place in the analysis.

In line with the ROA paradigm, the top event occurs if, and only if, there is a missing intervention of protective means.

Quite similarly, in the IROA scheme the top event occurs if, and only if, there is an ineffective intervention of protective means. This slightly different definition allows for the accounting of the dynamic process of recovery in which the human intervention plays a key role. Actually, moving from the concept of missing to that of ineffective intervention lets the imagination of the analyst picturing more realistically the evolution of the dangerous transient taking place; a dynamism in which many human corrective actions are performed before the top event occurs. Even further on this, the IROA framework models the actual interactions between the human beings and the technological system in place.

Again, the ROA procedure has been modified in order of explicitly modelling the human behaviour (see P, Q and R boxes in Figure 4). The ROA framework has been modified accordingly by expanding the "*missing* intervention of protective means" from two columns to six, in order to make it possible to correctly describe the "*ineffective* intervention of protective means" (Figure 5).

What will be called the left hand of block 2, i.e., that grouping column 4 to 5 and reflecting what is called human-technology system failure, is devised to bridle the behaviour of the human-technology system, meant as an optimally integrated one. This means that the two controllers, namely the automatic controlling system in place and the human one, do not "disturb" each other when performing their respective duties; there is a symbiosis between the two.

In this optimal system, where design features perfectly reflects usability concepts, operators do not have to struggle for taking the automatic control system under control so to avoid its excessive or modest intervention. Instead, there is a real interpenetration and collaboration between the technology and humans that makes the system much safer. The failure occurs actually only when the intervention of both the Automatic Protective Means (APM) and the Humans fail.

Unfortunately, optimal systems are more dreamy than real. In reality, it is easier to find a control system that come too often/seldom into action forcing operators to be particularly attentive and awake so as to prevent either too many shut downs, with a consequent loss of production, or too many ineffective automatic adjustments that lead to products out of specification.

Very often, because of this sometime profound incompatibility, i.e., low technology usability, between the system and the operators controlling and using it, operators intervene on the control system by-passing the so-called Engineered Safety Features (EFS). Indeed, once this step is done the reliability of the system can dramatically drops down as it goes on "manual mode", and the entire control activity is up to operators' capability to cope with system behaviour.

This last step is the one not very much modelled by any safety analysis practice since thought to be either something to relegate to malicious actions and, as such, not to model, or, even worse, something avoidable by putting in place more barriers or pushing further the automation.

As the old Latin adage says "*in media stat virtus*". In practice, what happens is that the two systems can alternate each other according to the task to perform. In fact, operators, once they got used to a new system, know very well its limitations and act accordingly by limiting its intervention (by-pass), i.e., substituting it with their corrective actions, or, where allowed, complementing its limited activity with their flexibility and experience, thus making the system effective. The same concept applies for the use of the organisational set-up. Very often operators find more useful to go for short-cuts by-passing organisational procedures.

It has to be noted that a recent work from Fadier *et al.* [19] has shown that in case of poor technology, these inappropriate actions of the operators, instead of reducing the plant reliability and safety, can improve it.

This discrepancy between design intentions and actual use of productive system by human beings, create a grey zone that needs to be modelled if realistic pictures on safety levels are searched for.

In the IROA methodological frame the trade-off between an optimal human-technology system and a bad one is modelled by attributing the ineffective intervention of protective means to the following two main causes:

- Missing intervention of protective means, and;
- Human Failure.

The right hand of block 2, i.e., that grouping column 6 to 9, has been conceived exactly for modelling the by-pass of ESF.

As said above, when an operator by-passes the ESF the system switches from automated to fully manual becoming extremely vulnerable since dependent only on human capabilities to recover from the unstable transient.

In the IROA frame, this is modelled in column 6. Essentially, despite the potential physical behaviour of a system is the same regardless to the APM in place, the effects of corrective actions can have an impact on the course of the event. Thus, the effects of human interventions on system behaviour must be modelled to check whether their impact change the transient sequence. Actually, if the consequences are different from those of column 3, after an erroneous intervention of the operator, the new sequence generated by the human intervention has to be addressed in column 7 as a normal consequence of the system. In practice, this is to say that if the APM are not in place bounding the system's behaviour, the human interventions can change the system behaviour in a way difficult to predict. And this is especially true in high-technology, high-complex and tight-coupled systems where the effects of human interventions can be differed in time and space.

Conventionally, the human intervention at this stage will provoke either the same consequence identified in column 3 – no divergence and then the analysis goes on "normally", or a worsening effect, thus forcing the analyst to take this newly generated consequence as the one to further analyse in column 1, i.e., a new deviation to bring down. This can clearly be the immediate subsequent more severe consequence of the previous deviation or a brand new one.

In the IROA concept, the human failure to recover has to be taken into account in two different cases:

- if the alarm system fails or the operator fails to "detect" it or another form of indication (misreading, misjudging, etc.), as in the traditional ROA;
- if the plant is left without ESF, due to their by-passing;

In both cases, a missing or ineffective intervention of Erroneous Intervention of Protective Means (EIPM) can be considered, and if its missing or ineffective intervention occurs, it will bring up directly to the ineffective intervention of protective means, i.e., fail to stop the wrong action.

Conceptually, there are two types of protective means. The former are those that intervene automatically to prevent technological or human failures to occur, while the latter are those coming into action to stop the effects of a human intervention already performed. The distinction between the two types can be made clearer with a simple example.

When using a word processor it often happen to loose the work due to an erroneous switch off of the program without saving. To avoid totally or partially this situation, the program can save automatically every while according to customer settings, or stop the effect of the action of the user, when he has already send the "quit" command, advising him and waiting for his decision about saving or not.

The automatic save of the work by the program is clearly the APM. On the contrary, the function stopping the effect of the wrong operator action, which has already been performed, falls into the EIPM concept. Thus the two are conceptually different as from a human failure standpoint the APM is a preventive means while the EIPM is a protective one.

3.3 *The chef's assistant*

The IROA for the chef's example is that of Fig. 6, built following the flow chart in Fig. 4.

Row 1

When high temperature is reached in the deep-fryer, a traditional ROA would assume the operator not to intervene on the system at this stage as considering it perfectly working.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Deviation	**Causes**	**Consequences**	**Automatic Protective Means**	**Warnings/ Alarms**	**APM and/or alarm bypass**	**Erroneous or Ineffective recovery intervention**	**Missing Intervention of EIPM**	**TE**
2. hT	1. Too much heat provided	2. hhT	4A. hT switch	4B. hT LED	4A. hT switch	O1.ERI on LED		
1. Too much heat provided	3. Thermostat stuck closed	2. hT						
3. Thermostat stuck closed	3. Thermostat fails to open*	1. Too much heat provided						
	O1. erroneous intervention (EI) during maintenance							
	O1. EI during inspection							
O1. EI during maintenance	O1. misdiagnosis*	3. Thermostat stuck closed						
O1. EI during inspection	O1. Misdetection of flaws*	3. Thermostat stuck closed						
2. hhT	2. hT	2. Boiling oil		olfactory		O1.ERI on olfactory warning		
2. Boiling oil	2. hhT	Localised fire		5. Smoke detector				1
		Widespread fire				O1.ERI on smoke detector signal		2
Localised fire	2. Boiling oil	Widespread fire	6. Sprinkler		6. Sprinkler			2
		Flooding	6. sprinkler correct intervention					3

Fig. 6: IROA for the frying operation

This means the system, whether left alone controlling itself, would perfectly works producing the desired products within the minimum time; in this case crispy and dry chips. In Fig. 6 this would be modelled simply by reporting in column 4 only the Missing Intervention of High Temperature Switch protective means. The failure of the switch would permit the system to go on towards the TE by further increasing the oil temperature. Despite being within the optimality as the human contribution perfectly integrates the technological one, this way of modelling does not depict the reality.

It is quite unrealistic to think that, in a situation where the switch does not open and the LED still keeps flashing, the operator, whether detecting the flashing LED, does not intervene manually either by putting off the power or by making the necessary control actions.

Or, at least, he/she does not check what is going on especially whether there is a symbiosis, i.e., a good interaction, between the technological and the human controllers. Thus, from a reliability standpoint, this integrated system can keep going on its degrading way even if the human protective means fails. And this can happens, column 5, either if the high temperature LED is faulty or the operator does not detect it when working. These two added “features” make the system more realistic and much safer since, despite it is true that humans can intervene erroneously on the system it is even true that they can even save a critical circumstance thanks to their experience, flexibility and quickness in adapting to it.

Up to this point, this new way of proceeding should not overturn the current way of modelling scenarios. What sensibly change the situation are columns 6 to 8 as they unveil the potential incompatibility between the human and the technological controllers. The high temperature protective mean does not work optimally as it switches the deep-fryer too often forcing the assistant to slowing down chef’s work. The assistant is then, say, under two fires, namely (1) the blames of the chef and (2) the multiple “quenching” of the APM. To overcome the uncomfortable situation the assistant is “pushed” to by-pass the ESF, here the high temperature switch, to get the production done in time, i.e., the one imposed by the manager, which in turn is imposed by customers.

Column 6 tries to shape exactly this situation. After by-passing the high temperature the safety of the productive system is exclusively under operator’s control. As such, it has no sense to speculate about the reliability and availability of APMs as they are off, i.e., practically inexistent. This is reflected in the reliability of the protective system that for this last part of the second block is simply given by the possibility that either the operator misdiagnose the situation, e.g., he/she does not correctly intervene because he/she does not know what the flashing LED means, or he/she does not detect it (to be detailed in the logic tree).

As taken it for granted in the above description, it is worth noticing that while there is a missing intervention of APM, such as the high temperature switch for the case of row 1 here analysed, it has to be investigated whether this occurrence can be traceable back to human pre-initiator causes, i.e., those analysed in block 1. Put it differently, once a protective means is identified in column 5, its potential latencies built-in by erroneous or missing (human) interventions have to be addressed.

Furthermore, at this time of the accidental sequence what it is interesting to model is, once more, the by-pass of ESF. For this case, the maintenance operator needs to by-pass the high temperature switch and, what is more important, forget to put it back into service once completed the work.

Even worse, the system was deliberately put off because of previous false alarms. Unfortunately this approach impinges on the safety level, leaving a substantial hole in the protective system as during emergency not everything goes smoothly and as expected and restoring further barriers can be problematic. This is especially true in high-technology, high-complex and tight-coupled systems.

Column 7 represents the possibility for the operator, once the APM is by-passed, to making an erroneous intervention on an on-site warning or indication.

The need for, and consequently the lack of, protective means devoted to contain the effects of a possible erroneous intervention of an operator, is now highlighted in column 8.

Rows 2 to 5

These rows contain the substantial novelty in accounting for HF as pre-initiators. Essentially, in the classical ROA approach, it is simply stated that there is a Missing Intervention of the thermostat (stuck closed). From an HF perspective this position is satisfactory only whether the component has just been installed and put into service. In other words, it is acceptable if, and only if, the causes of failure are not traceable back to erroneous human intervention performed either during maintenance, repair, and modifications or during the decision making process. This reflects the reality that humans intervene on the system, through maintenance, repair and modifications, to keep it safe throughout its life. And it even reflects the fact that humans do even make decisions on how often and if intervening on the system. It is quite well know how often maintenance is not regularly performed because of a prior decision on its costs. Thus, in row 3, the thermostat can stuck closed even whether upstream there has been an erroneous intervention either during maintenance or inspection or a decision on maintenance and/or inspection frequency and appropriateness was made.

Row 6

Scrutinizing block 2, the operator can not intervene on smell for instance because either he/she does not know that specific smell is a sign of dangerousness or because he/she does not detect it due to an annoying flu. Alternatively he/she does not detect the smell simply because the extracting unit is particularly efficient and strips quickly out smells from the room not allowing reaching the human threshold for perception.

Row 7

Same as previously, the assistant can even not intervene on smoke either because the smoke detector is faulty, and thus simply not audible, or because, symmetrically to what described in row 5, the smoke of the deep-fryer quickly mixes up with that produced in the preparation of other dishes making the two indistinguishable, especially under the pressure of the rushing hour of a busy restaurant. Or, as above, “thanks” to the efficient extracting unit.

Here, it is possible to see what the effects of an erroneous intervention of the operator could be. Once the fire is on, the assistant may even erroneously intervene on it amplifying its effect, for example, by flinging a tea towel on top of it in the attempt to chock it off, this leading to a spreading of the fire. The same TE reached if the APM sprinkler does not intervene in case of fire.

Once all the types of human erroneous or missing intervention has been identified, the merit of their root causes is to be discovered applying a Human Reliability Analysis (HRA) method. Misdetection, for instance, can be caused either by lack of training, meaning that the operator does not detect a situation because he/she does not have the knowledge to do it, or because of internal and/or environmental disturbances, the so-called Performance Shaping Factors (PSFs) present in the context where the accidental scenario is developing, and that do not allow to properly do it.

Similarly to the HRA process, once the human primary events have been identified, the search for their route causes and the associated probability of occurrence entails the inclusion of the organisational aspects associated with them. Probably redundant to say, but this is obvious and consistent with the concept that Human

& Organisational Factors are not only those factors which characterize the interaction between humans and the technology they handle but, more broadly, are those which enable to reveal the many interrelations amongst humans and the socio-technical context in which humans daily perform their duties.

In the most advanced HRA methods [14][15][16] this is fully reflected in the framework of the methodology, which does not allow to disregard organisational aspects when performing the analysis as they are integrated in the structure and permeate its practical implementation.

4 THE LINK BETWEEN IROA AND LOGIC TREES

As anticipated in the introduction, one of the main advantages of the recursive approach it that of easing the extraction of logic trees once the operability analysis is completed. In this respect, the IROA does not make any exception. The most comfortable way to transform the identified safety issues from the IROA structure to that of Fault Tree is to extract from the IROA table the Incidental Sequence Diagram (ISD) procedure [4]. It is the logic diagram, reporting in a graphical way the information collected in the IROA, linked through the logic gates inherent in the analysis (as shown in Fig. 3). It differs from a Fault Tree only for the undeveloped causes, both technological and human, of the ineffective interventions of protective means, that will be included just before its quantification.

The new paradigm proposed for the IROA, conceptually framed by the two blocks illustrated above, has, too, to be reflected in the construction of the logic trees.

Fig. 7 represents the ISD of IROA here described. Grey boxes represent the interfaces with the HRA.

This paradigm differs substantially from that one can derive from the ROA depicted in Fig. 1, for two main aspects, namely, (1) the simplistic representation of the human being as a machine-like acting entity, and (2) the exclusion of erroneous interventions as a complement of those of omission.

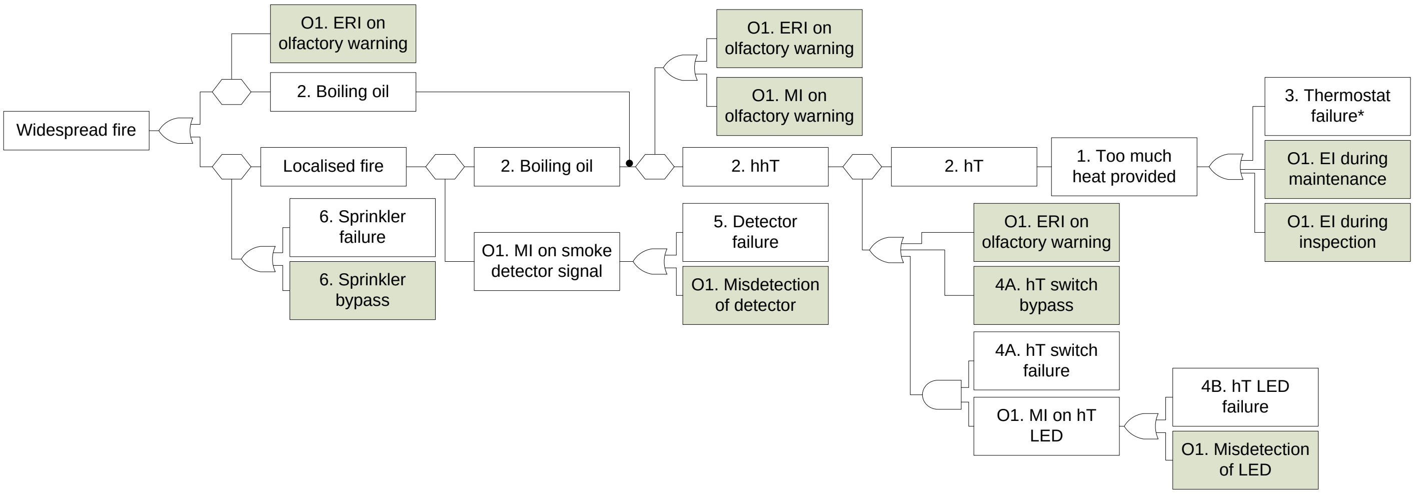


Fig. 7: IROA Incidental Sequence Diagram

The process branches of the INH gates are directly extracted from block 1 of Fig. 6 simply by following the classical ROA procedure. From a HF perspective pre-initiating human failures are represented there.

The entire lateral branchs of the INH gate represent, instead, the protective system. The sub-branches of this protective system respectively result from block 2 of the IROA framework. These branches are clearly linked by an OR gate since it is enough that one of the two fails to let the entire protective system failing.

To obtain from the ISD the Integrated Fault Tree, as in the classical ROA it is necessary to deepen the causes of the ineffective intervention of protective means (lateral branches of the INH gates), including the possible pre-initiator human failures.

5 CONCLUSIONS

This paper, providing a framework that enables to integrating H&OF into Operability Analyses in a systematic manner, contributes making safety analyses more realistic.

In particular, the IROA concept here described allows for safety analysts to discern between the human primary causes which contribute to put latencies into the system's components, i.e., the so-called pre-initiating human failures, and those which can either trigger an accidental sequence or contribute to change the course of an ongoing one, i.e., the so-called post-initiating human failures. Furthermore within the two varieties the IROA concept should allow analysts to fairly well distinguish between erroneous interventions and missing ones.

Another relevant contribution the IROA offers is given by the possibility both to modelling the by-pass of the ESFs and the consequences that an erroneous human intervention can have on the accidental sequence once the ESFs in place have been by-passed. This dynamism of the procedure can positively compel the analyst to improve his/her ability to look beyond the accidental scenarios created by pure technological failures. In addition, thanks to the use of the INH gates and its sequentially structured frame, it even allows for better modelling of the timings of the potential accidental sequence.

The IROA structure as presented in the present paper, thanks to its systematic nature, can ease the translation of its procedure into a fully computerized code.

Finally, last but not least, thanks to the easiness with which logic trees can be extracted from a completed IROA, the present framework provides a feasible way forward to systematically account for H&OF both in a qualitative and, potentially, even a quantitative fashion. The paper does not clearly cover the open issue of H&OF data elicitation.

NOTATION

APM Automatic Protective Means

EIPM Erroneous Intervention of Protective Means

EOC Errors of Commission

EOO Error of Omission

ESF Engineered Safety Features

HF Human Factors

HFI Human Failure Identification

HRA Human Reliability Analysis

H&OF Human & Operational Failures

IFT Integrated Fault Trees

IROA Integrated Recursive Operability Analysis

ITE Integrated Top Event

MI Missing Intervention

ORA Organisational Reliability Assessment

QRA Quantitative Risk Assessment

ROA Recursive Operability Analysis

TE Top Event

AKNOWLEDGEMENTS

The authors wishes to acknowledge both Prof G. Biardi and N. Piccinini for their many suggestions and hints that allowed to keep lucidity and rigorousness, as well as staying on the right track.

This work owes its results to the EC funded research project VIRTHUALIS (www.virthualis.org) thanks to which this work has been made easier, even because of the many stimulating discussions had with project's partners, and without which gaining the same results would have been much harder and longer.

REFERENCES

[1] Colombo, S., Biardi, G., Cacciabue, P. C., Piccinini, N., 2004, "Recursive Human Operability Analysis: Integrating Human Factors into Safety Analyses", Proceedings, 7th International Conference on Working With Computing Systems Conference, 29 June – 2 July 2004, Kuala Lumpur, Malaysia, ISBN 983-41742-0-9

[2] Piccinini N., 1995. "Operability Analysis as a tool for fire risk evaluation", EuroFire 95, Nimes, 25-27 March 1995.

[3] N. Piccinini, 1996. "L'analisi di Operabilità", Automazione e Strumentazione, 44 (6), 75-83.

[4] Piccinini N., Ciarambino I., 1997. "Operability analysis to the development of logic trees", Reliability Engineering & System Safety, 55, 227-241

[5] Lawley, H. G., 1974, "Operability studies and hazard analysis", Chemical Engineering Progress, 70, 45-46

[6] Chemical Industrial Safety and Health Council of the Chemical Industrial Association, 1977, A Guide to Hazard and Operability Studies, Alembic House, London

[7] AICHE, 1985, Guidelines for Hazard Evaluation Procedure, New York

[8] Lees, E. P., 1996, Loss Prevention in the Process Industries, Butterworths, London

[9] Demichela, M., Piccinini, N., Ciarambino, I., Contini, S., 2003, “On the numerical solution of fault trees”, Reliability Engineering & System Safety, 82, 141-147

[10] M. Demichela, N. Piccinini, I. Ciarambino and S. Contini, 2004, "How to avoid the generation of logic loops in the construction of fault trees", Rel. Engng Syst. Safety, 84 199-209.

[11] M. Demichela, N. Piccinini, 2002, "Dot Chart Analysis as a Means to Develop a Fault Tree: Application to a Catalytic Hydrogenation Unit", Rel. Eng. Syst. Safety, 76, 63-73.

[12] Demichela M., Marmo L. and Piccinini N., 2002, "Recursive Operability Analysis of Systems with Multiple Protection Devices", Rel. Engng Syst. Safety, 77 301-308.

[13] M. Demichela, N. Piccinini, R. Pellegrin, 2003, "Productivity improvement of a BDK process plant via QRA tecniques", J. of Loss Prevention in the Process Industry, 16, 381-387.

[14] Barriere, M. T., Bley, D. C., Cooper, S. E., Forester, J., Kolaczkowski, A., Luckas, W. J., Parry, G. W., Ramey-Smith, A., Thompson, C., Whitehead, D. W., and Wreathall, J., 2000, “Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)”, Technical Report NUREG – 1624, US-NRC, Washington DC.

[15] Hollnagel, E., 1998, Cognitive Reliability and Error Analysis Method (CREAM), Elsevier, London

[16] Le Bot P, Desmares E, Bieder C, Cara F, Bonnet J-L., 1998, “MERMOS: un projet d’EDF pour la mise a jour de la méthodologie EPFH”, Revue Générale Nucléaire

[17] Swain, A. D., Guttmann, H. E., 1983, “A Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, USNRC, Washington DC-20555

[18] Spurgin, A. J., Lydell, B. D., Hunnaman, G. W., Lukic, Y., 1987, “Human Reliability Assessment, a systematic approach, in Reliability 87, NEC Birmingham

[19] Elie Fadier, Cecilia De La Garza, Armelle Didelot, 2003, “Safe design and human activity: construction of a theoretical framework from an analysis of a printing sector”, Safety Science 41 759–789