EVALUATING SAFETY CULTURE UNDER THE SOCIO-TECHNICAL COMPLEX SYSTEMS PERSPECTIVE

Francisco Luiz de Lemos

IPEN – Nuclear and Energy Research Institute
CNEN – National Nuclear Energy Commission_Brazil
Email: fllemos@ipen.br

OUTLINE

MOTIVATION

STAMP_ SYSTEMS THEORETIC ACCIDENT MODEL

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS

SAFETY_SAFETY CULTURE

THE THREE LENSES

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION

DISCUSSION AND CONCLUSIONS

MOTIVATION

- Despite all efforts, we continue to witness accidents that are, in great part, attributed to flaws in the safety culture of the organization.

- In this sense, blaming flaws in the safety culture for accidents, or incidents, would follow the same line of reasoning as blaming human errors, or an equipment failure, for an accident

- However, when it comes to more subtle interactions between components of the system, it becomes harder to detect potentially hazardous situations that are hidden, and can lead the system to hazardous states.

- Such a situation may not be easily detected by direct observation. These situations can occur in spite of the safety culture being regarded as positive.

MOTIVATION (cont.)

- With the objective of having a deeper understanding of the relation between the safety culture and the safety of the system we propose a combination of the STPA, Systems Theoretic Process Analysis methodology [1], and the Three Lenses approach [2].

STAMP_ SYSTEMS THEORETIC ACCIDENT MODEL AND PROCESSES

- STAMP, Systems Theoretic Accident Model and Processes is based on systems thinking and systems theory
- A system can be defined as a set of components and subsystems acting together towards a common goal or purpose.
- A system has boundaries, input and output. In STAMP a system is viewed as composed by hierarchical levels of control, where the upper levels have properties that emerge as a result of the interaction between components at the lower levels
- In STAMP, safety is considered an emergent property that arises from the interactions between the system components

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS

- STPA is an extension of the STAMP, Systems Theoretic Accident Model [3]. Both methodologies are explained in some more detail later on in this paper.
- In STPA it is assumed that accidents are the result of flaws in the control of the interactions between components and, therefore, even when all components of the system are working exactly the way they should, accidents can happen.
- A system can be defined as a set of components and subsystems acting together towards a common goal or purpose.
- A system has boundaries, input and output.
- In STAMP a system is viewed as composed by hierarchical levels of control, where the upper levels have properties that emerge as a result of the interaction between components at the lower levels

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS (CONT.)

- A nuclear power plant, has a structure that is comprised of the basic elements: human controllers, automated controllers and controlled process.

- The controlled process is the physical or sensed process that can potentially exhibit hazardous behaviour

- ***Accident = Hazardous condition + Worst Environmental condition***

- It should be noticed that the term “environmental conditions” refer to conditions that are “external” to the system. These are conditions over which the designers of the NPP do not have control.

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS (CONT.)

The Safety Control structure

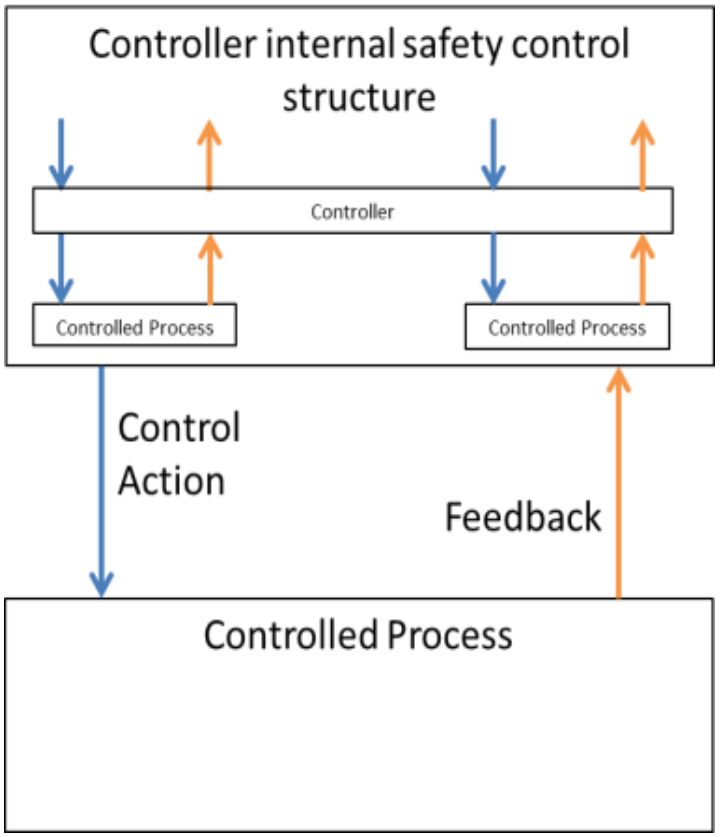

FIG. 1. A generic control structure, adapted from [3]

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS (CONT.)

STPA can be applied in two steps

Step 1: Identifying Potentially Hazardous Control Actions

- The control action, CA, can be potentially hazardous if it is inconsistent with the state of the system.

Step2: Identifying causal factors

- Once the safety constraints are defined, we can proceed to identifying the causal factors that can lead to violations of the constraints.

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS (CONT.)

The potentially unsafe control actions can be classified into four categories according to the state of the system:

- A required action is not provided or is provided and not followed
- A required action is provided and leads to a hazard
- A required control action is provided too early or too late, or in the wrong order
- A required control action is stopped too soon or applied too long

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS (CONT.)

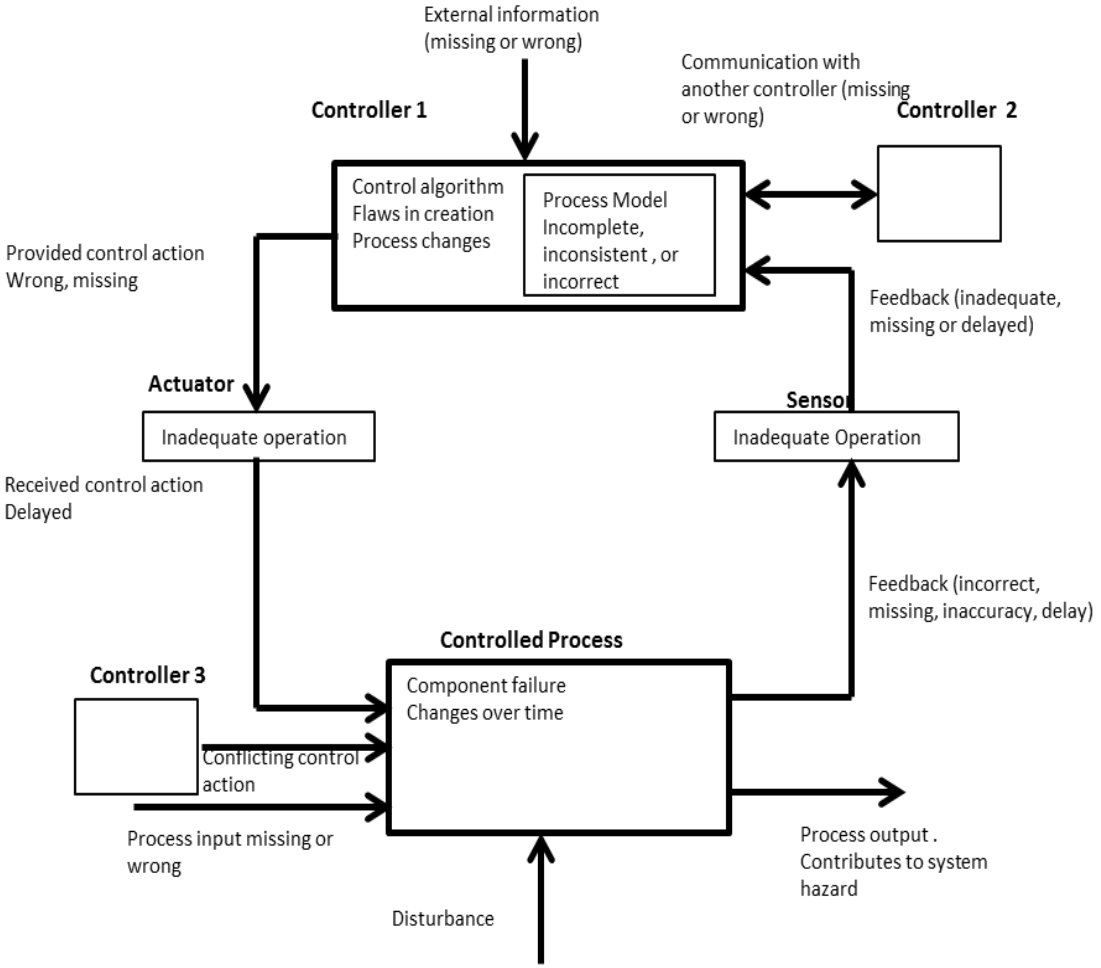

FIG. 2. A general control loop with causal factors, adapted from [5]

STPA – SYSTEMS THEORETIC PROCESS ANALYSIS (CONT.)

The decision making process to issue a control action can be a result of a very complex process. In a large and very complex socio-technical system all the flow of information, mental maps, algorithm, etc. are subject to constant influences from many components, such as multiple controllers and multiple stakeholders.

Models are abstractions of the actual system. Therefore, it is important to note that these elements are figurative and do not always represent physical equipment.

SAFETY _ SAFETY CULTURE

Safety

Safety has similar meanings for STPA and the IAEA.

However, in STPA safety has a broader meaning. In STPA an accident is an unacceptable loss.

For the IAEA
Any harmful effects of ionizing radiation to people and the environment would be considered as an unacceptable loss, or an accident.

For the utility owner perspective, an economic loss can also be considered as an unacceptable loss, or an accident.

In STPA, both, “economical loss” and “harm to people and environment”, are considered within the same safety assessment, which makes it relatively easier to deal with conflicting goals in the same framework.

SAFETY _ SAFETY CULTURE

Safety Culture

The International Nuclear Safety Group (INSAG) defines safety culture as:
"The assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receives the attention warranted by their significance."

One important observation about this definition of safety culture is:

What do the expressions "emphasize safety over competing goals" or "make nuclear safety the overriding priority" mean?

The definition do not make it clear how to make it a priority, i.e. how to deal with different goals, during design and operations of the system.

THE THREE LENSES

We begin this section with an excerpt from the book Design for a Brain.

“The system state, at any point in time, is the set of relevant properties describing the system at that time. These properties are represented by state variables. As the system can have an infinite number of state variables that can describe its state, only a subset of those variables are chosen to describe the relevant behaviour of the system according to stakeholder and the purpose being analysed. In other words, the analyst chooses his system.”

THE THREE LENSES (CONT.…)

The “Three Lenses” is an approach for organizational analysis. It is about using different perspectives to view an organization.

Depending on the perspective different variables and relationships in the system are considered

- Strategic Design Lens
- Political Lens
- Cultural Lens

It is important to keep in mind that all the variables, and relationships, highlighted by each one of the lenses co-exist in the system, and that the lenses approach helps us to make sense of these variables and their relationships, which reveals a much more complex socio-technical system.

THE THREE LENSES (CONT....)

The Strategic Design Lens

The basic idea of strategic design is "get people with the right knowledge and give them appropriate tasks to do and sufficient information to accomplish the organizational goals"

Political Lens

The organization is viewed as a contest for power among stakeholders with different goals and underlying interests. Goals and strategy are either imposed by a ruling coalition or negotiated among interest groups. As circumstances change, power shifts and flows, coalitions evolve, and agreements are renegotiated

Cultural Lens

The cultural perspective assumes that people take action as a function of the meanings they assign to situations. The cultural lens focuses on norms, meaning, artefacts, and values. Managers become the creators of meaning, using symbols and stories.

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION

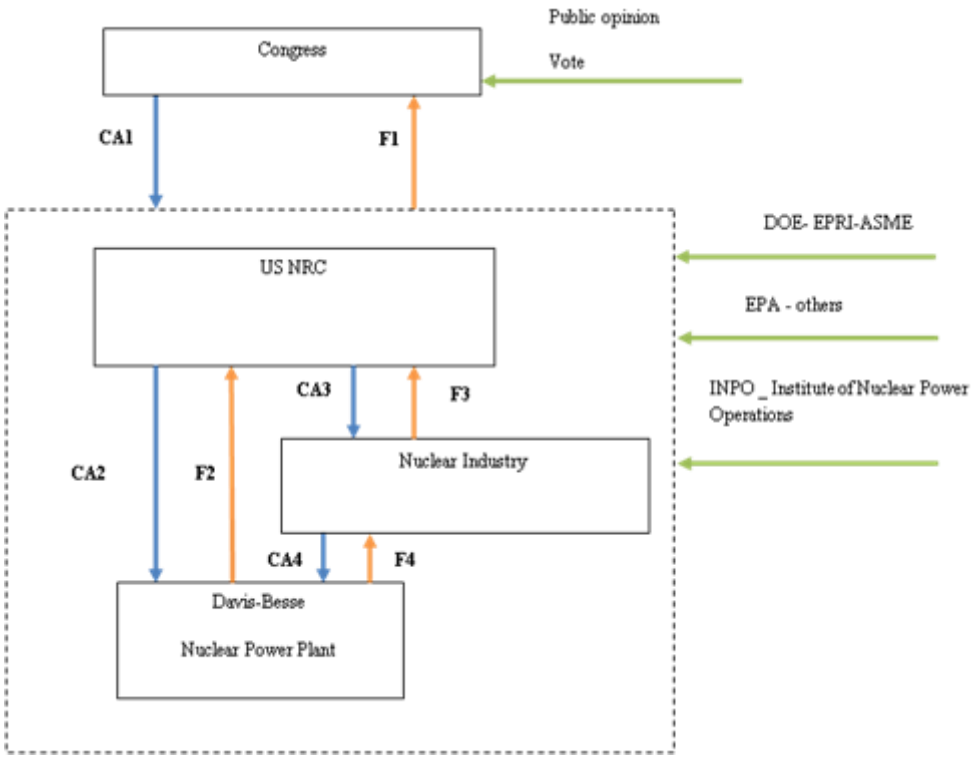

FIG.3. National nuclear energy generation partial safety control structure

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

For this system we consider the following accidents:

A1: People or the environment are exposed to radiation
A2: Loss of reputation for the USNRC
A3: Loss of reputation for the Nuclear Industry

Next, we identify the hazardous states that could lead to the already identified accidents:

H1: Radioactive material released from a NPP: A1; A2; A3
H2: Generation of Electrical Power Stopped: A2; A3
H3: Serious Equipment Damage: A1; A2; A3

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

Control action, CA3, issued by the US NRC, requiring the shutdown of reactors in 2001. This CA was issued after receiving a feedback from the industry, F3. This feedback was the result of inspections in similar plants as mentioned bellow:

F3: "*Inspection of Oconee Nuclear Station 1 (Nov. 2000), Arkansas Unit 1 (Feb. 2001), Oconee Unit 3 (Feb. 2001) and Oconee Unit 3 (April 2001) showed both axial and circumferential cracks in Control Rod Drive Mechanisms*" [10].

CA3: "*October 15, 2001: The NRC staff distributed a draft order requiring the shutdown of reactors by December 31, 2001, for CRDM nozzle inspections*" [10].

TABLE 1. CONTROL ACTION 3 – CA3: INSPECTION REQUIRED

Control Action	Potentially Hazardous				
	1- Not Providing causes hazard	2- Provided causes hazard	3- Provided Too early or too late causes hazard	4- Stopped too soon or applied too long causes hazard	5- Provided but not followed
Inspection Required	- There is a corrosion process that continues until the vessel is perforated by corrosion - LOCA H1-H2-H3	- There was no need for the inspection H2	1- Too early - Provided when there is no corrosion visible. Makes the Plant to shut down unnecessarily. H2 - Causes unnecessary delays in the generation of energy. H2 2- Too late - Provided after the corrosion is in a very advanced stage or had already perforated the RV H1-H2-H3	1- Stopped too soon - Inspection initiated but stopped before any sign of corrosion is found H1-H3 2- Applied too long - Inspection lasts for a long time causing unnecessary delays in the generation of energy. H2	- The corrosion continues until the vessel is perforated by corrosion H1-H2-H3

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

In the example, there are basically two contexts, or conditions, for the control action to be hazardous:

- The Plant continuing operation when there is a corrosion process in the RPV, leading to damage to the equipment and consequent release of radioactive material.

- The Plant is unnecessarily shutdown when there is no corrosion at all.

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

There should be no limitations by judgements of weather the causes are highly improbable. If the cause is not impossible, then it should be considered

(a) ***Provided causes hazard***

Regulator decides for the inspection requirement in spite of the low probabilities of the occurrence of the process.

DB Plant decides to conduct the inspection without pursuing further information about the differences in the Plants.

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

(b) ***Not providing causes hazard***

Regulator thinks that there is no need for inspections; therefore, the regulator does not issue an inspection requirement.

This could be a result of a flawed feedback from the industry, F3 and F2, which convinces the NRC that there is no safety concern and there is no need for inspections.

The Plant askes to cancel the inspection

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

(c) Provided too early or provided too late causes hazard

Provided too early

Regulator decides for an early inspection for precaution

Plant decides for an early inspection for precaution

Provided too late

Regulator takes a long time to identify indicators of the urgency of the problem.

The Plant asks for a delay in the inspection

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

(d) ***Stopped too soon or applied too long causes hazard***

Applied too long

The NPP workers unsecure whether they should stop or continue with inspection, carrying out extra tests to assure that there is no corrosion, causing unnecessary delays in energy generation.

Regulator asks for more explanations and requires extra inspections

Stopped too soon

The NPP think it is unnecessary to continue inspection as they feel pressed by the industry to be productive

The NPP stop inspection because they would have to go through very difficult procedures to continue and they think it is not worth it

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

(e) *Provided but not followed*

Industry receives requirement but does not follow it because they think it is not necessary or they do not want to stop generation of energy. Industry asks for a delay.

The DB does not understand the requirement and, therefore, does not follow it.

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

Causal analysis for the hazardous control actions

TABLE 2. Approximate classification of causal factors according to the Three Lenses

Lens / Control Action	Cultural	Strategic Design	Political
Provided		DB decides to proceed with inspection	Regulator takes isolated decision
Not provided	They thought the plant was safe – Leaks were not a safety concern	Technical Specifications were followed	DB prevailed over NRC arguments
Provided Too early		DB decides to proceed with inspection	
Too late	DB thought plant was safe – Leaks were not a safety concern The process was long and people got used to it making it difficult to notice changes	DB was well evaluated by NRC and INPO	
Provided For Too long			
Stop too soon	DB thinks it is not necessary further inspections	DB thinks inspections is waste of time	
Provided but not followed	DB was well evaluated They thought plant was safe – Leaks were not a safety concern		DB wants to obtain economic benefits and the industry prestige associated with very short maintenance outages.

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

Rationale for the classification

The decisions of issuing, or not, a control action, as well as the decision to follow, or not, the CA's, can be a result of complex interactions and relationships throughout the system.

These relationships and interactions do not necessarily have to be related to culture.

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

The Cultural Lens

Decisions based on perceptions and beliefs

In all but a few cases, cracking in nozzle applications has been attributed to primary water stress corrosion cracking (PWSCC). The mechanism of PWSCC is not completely understood, and prediction of crack initiation time has proven to be difficult, if not impossible [12].

“This resulted in less vigorous inspections and dismissal of some indicators because they believed the plant was safe” [13].

This produced "a whole new phenomenon," says John Grobe, head of an NRC task force investigating the incident. "This kind of corrosion has never been seen before on a reactor pressure vessel head." [11].

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

Strategic Design

1- This situation that could be classified as a cultural as well. However, the access had not been fixed because they had plans for future modernization, for example, as part of a strategy to achieve more efficiency*:*

The inspections were made more difficult by the design of the reactor service structure, which provided only "mouse holes" for inspection [8].

2- Decision can be part of a strategy to achieve goals:

Another factor that motivated against inspection was that the neighbourhood of the reactor vessel head is an intense radioactive field and hence radiation exposure of individual workers would be involved. Low radiation exposure is one of the measures of success among nuclear power plants [8].

EXAMPLE: DAVIS-BESSE VESSEL HEAD DEGRADATION (CONT.)

Political Lens

1- The Plant can be considered as a stakeholder in a broader system. This situation could be associated with strategic Lens as well:

Notice that this whole scenario unfolded during the world-wide phenomenon of electric power industry restructuring. Did the competitive pressures of restructuring exacerbate conditions at Davis-Besse? Only by digging into the details of the behaviours and conditions will we ever find out [8].

2- This situation was also cited as having strategic design characteristics. It is repeated here because this situation can also mean political power in the broader system where the Plant is one stakeholder*:*

Davis-Besse had been rated 'INPO 1', which meant that an independent review process undertaken by industry peers had judged it to be a high-performing organisation [14].

DISCUSSION AND CONCLUSIONS

The proposal of this paper was to analyse the role of the safety culture in the safety analysis of a complex socio-technical system.

Most of the literature treats safety culture under the perspective of an organization alone, giving little consideration to the broader system in which this organization is inserted.

By blaming flaws in the safety culture for accidents, or incidents, we fail to grasp important underlying mechanisms that shape the decision making process throughout the system.

The Nuclear Power Plants are part of a broader system and, therefore, they affect, and are affected by, other components of that system.

The Three Lenses approach offers yet an additional, or complementary, perspective, by introducing the cultural, political, and strategic design lenses, to interpret the mechanisms that underlie the decision making process throughout the system.

DISCUSSION AND CONCLUSIONS

We think that STPA and the Three Lenses approach could help answer, or at least help to answer, to the following questions:

a) How strong should the safety culture have to be to prevent the incident from happening?

b) If the degraded head had been discovered during earlier inspections, would it mean that Davis-Besse deserved a better safety culture classification?

c) How would have the event unfolded in case the workers had a better access to that spot in the RPV? (The “mouse hole” access [8])
This is a good example of interactions between components of the system, i.e., the designers and the operation workers.

d) How much more training, on safety culture, the workers would need to help avoid the next big accident?

DISCUSSION AND CONCLUSIONS

We conclude that, while a strong safety culture is necessary to keep the systems safety, it is not enough.

The combination of STPA and The Three Lenses approaches could help us to go deeper in the understanding of the system variables and components interactions.

Hopefully, it could help find the gaps in the safety control structure for a lasting solution.

Thank you for your attention