Using STPA on the Assessment of Nuclear Security Culture

Francisco Luiz de Lemos[1]
Malvina Mitake

IPEN - Institute for Nuclear and Energy Research
[1]fllemos@ipen.br

INTRODUCTION

In this study we combine the IAEA security culture self-assessment methodology and the systemic approach STAMP/STPA

STAMP/STPA helped to find gaps in the organizational structure that could be further explored by the self-assessment methodology

MOTIVATION

The organization has a very complex dynamics where different cultures, and other mechanisms, needed to be understood before we proceed to the security culture assessment. These are noises that can obscure the mechanisms that can affect the focus of the self assessment.

Difficulties establishing the culture characteristics and indicators to be the focus of the assessment

Three lenses: culture, political and strategic design.

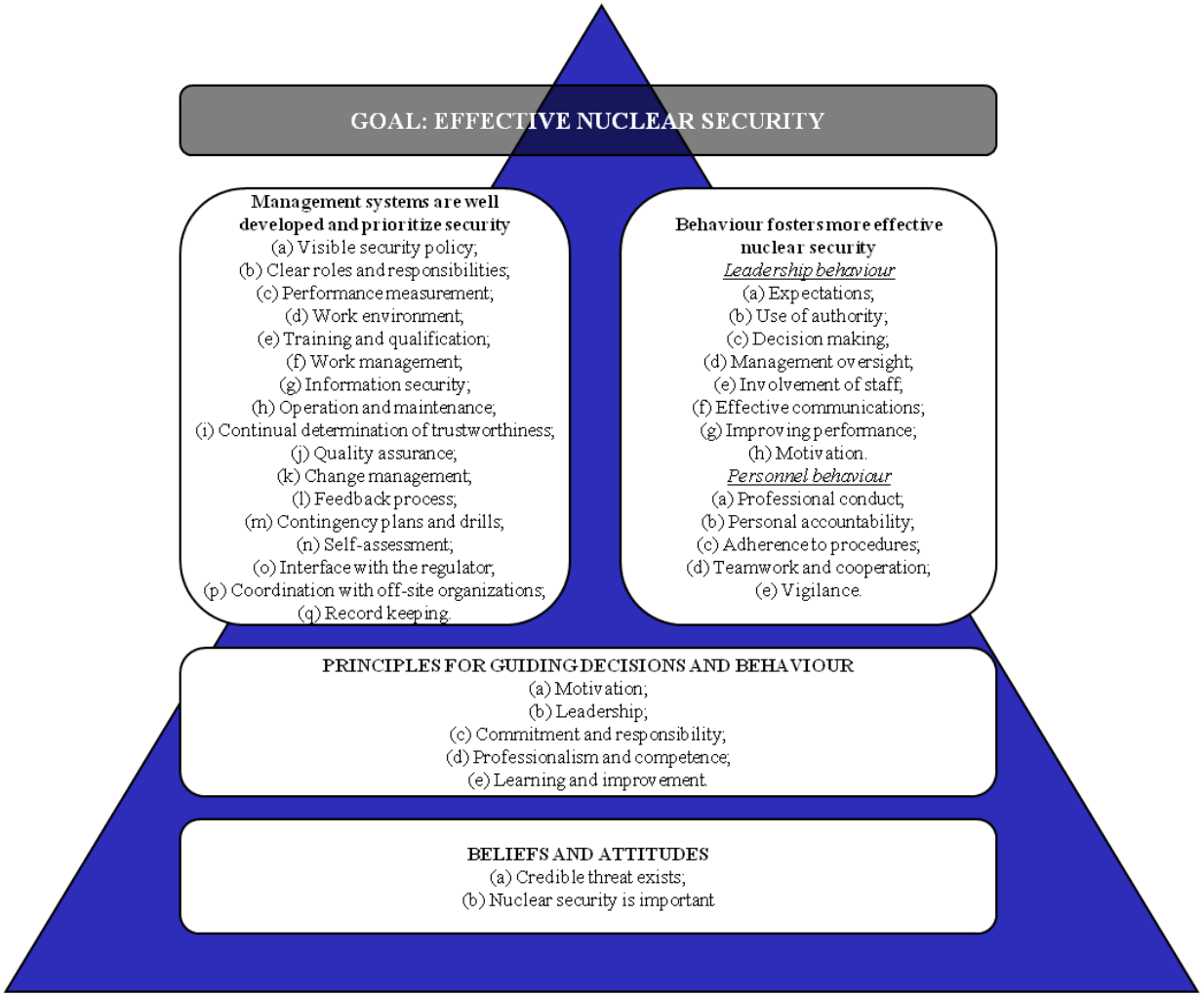
The security culture is one of the aspects of the organizational culture. These aspects culture are not compartmented, i.e. they exist together and interact.

MOTIVATION

STAMP/STPA can help us to understand how different aspects of the organizational culture can affect the security culture of the organization.

In the hierarchic control structure the various components of the system must show coordination and consistency in their interactions .
The analysis can identify potential scenarios that could arise due to flaws in the structure.

SECURITY CULTURE



"Nuclear Security Culture: Implementing Guide," IAEA, September 2008

SECURITY CULTURE

It is also important to note what safety (security) culture is not. The term is often misinterpreted as compliance and rule following, but a strong safety culture entails members of the organization viewing safety as intrinsically important.

The Security Culture Self Assessment

1- Focus = Adherence to procedures

What do we know about the focus?
Indicator – III c
III. Personnel Behavior + c. Adherence to Procedures

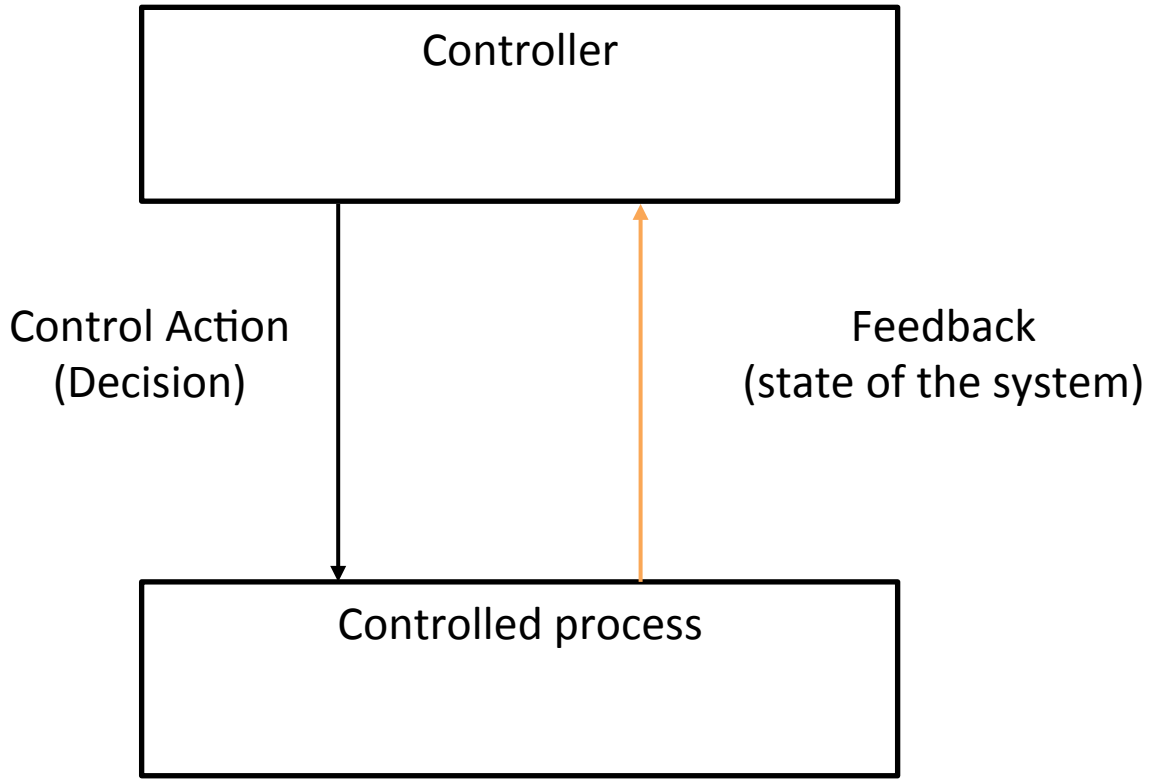
2- Select culture characteristics in Leadership Behavior and Management Systems which can contribute to better compliance .

The Security Culture Self Assessment

What contributes to make better the focus? (how to evaluate the effects on security?

Leadership behavior	**Management systems**
1-Use of authority	1-Clear rules and responsibilities
2-Management oversight	2-Training and qualification
3-Involvement of staff	3-Work environment
4-Effective communication	4-Information security
5-Improving performance	5-Visible security policy
6-Motivation	6-Quality assurance
	7-Self Assessment

STPA – System Theoretic Process Analysis



A Generic Control Structure

Leveson, N. G. (2012). Engineering a Safer World. MIT Press

STPA – System Theoretic Process Analysis

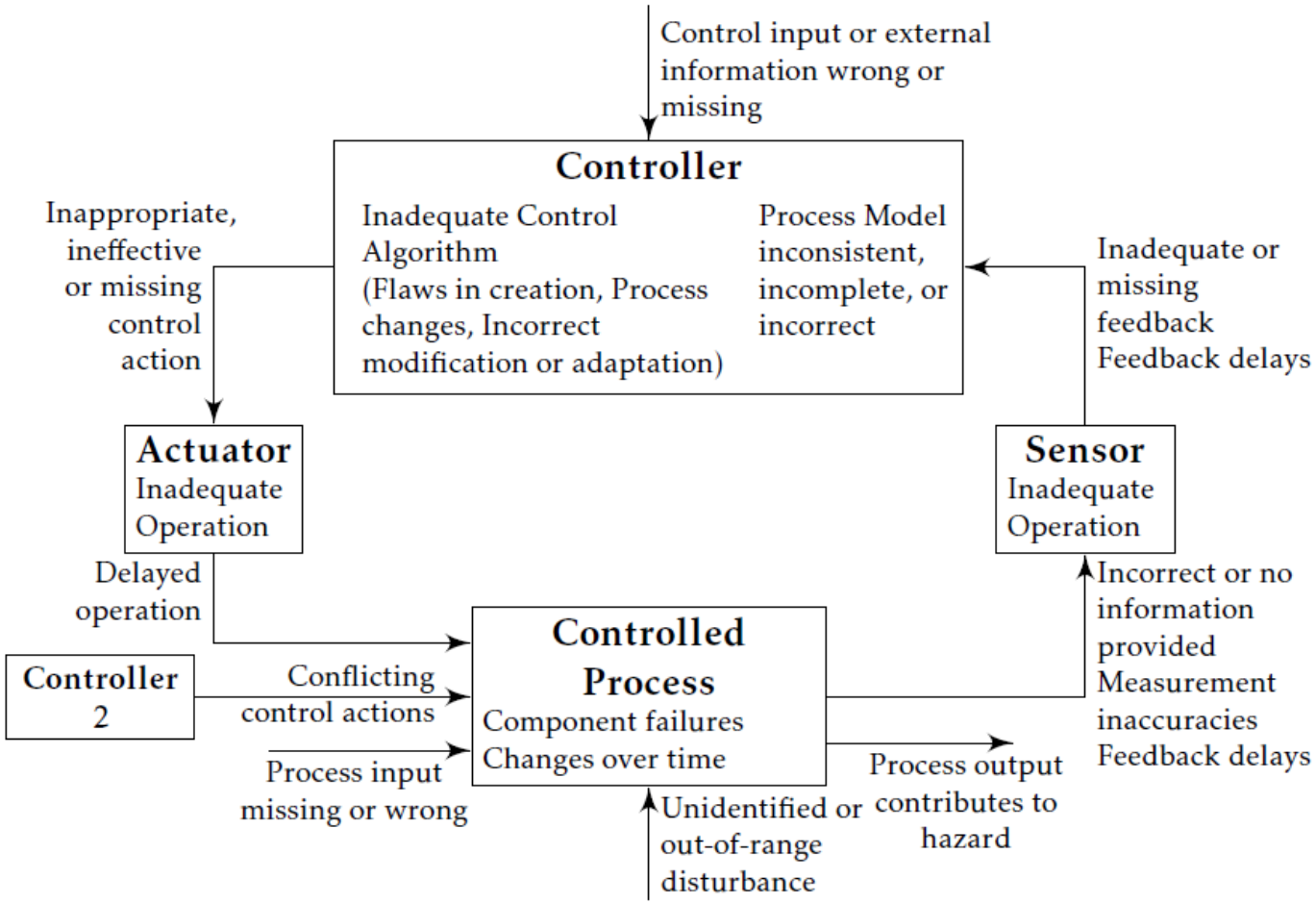
Instead of breaking system into components, analyzing each separately, and then trying to combine the individual analyses (a bottom up approach), STPA starts by looking at the system as a whole, identifying the constraints on the behavior of the components to ensure that working together they will maintain the safety, security, etc. properties of the system as whole (a top-down approach).

A strong security culture in each one of the subsystems does not necessarily means better security for the whole system.

STPA – System Theoretic Process Analysis

The enacted, multifaceted, and pervasive nature of organizational culture means it is something an organization *is* and is challenging to change deliberately, rather than something an organization *has* that can be changed directly and readily (Schein 2010).

STPA Control Loop with Causal Factors



Leveson, N. G. (2012). Engineering a Safer World. MIT Press

STPA Control Loop with Causal Factors

Four conditions are required for process control [Ashby, 1957; Leveson, 2012]:

1. *Goal*: the controller must have a goal or goals

2. *Action*: the controller must be able to affect the state of the system, typically by means of an actuator or actuators.

3. *Model*: the controller must contain a model of the system

4. *Observability*: the controller must be able to ascertain the state of the system, typically by feedback from a sensor

STPA Control Loop with Causal Factors

Analysis conducted as follows:

1- Build the hierarchical control structure of the system according to official information

2- Through observations and interviews, examine the basic functions of each entity in the control structure

3- Compare the requirements for each entity on the model control structure and the real life one.

How the requirements for each entity, for an effective control of the interactions, compare to the real life ones.

STPA Control Loop with Causal Factors

To do that we need to identify the responsibilities of the controller, actuator, controlled process, and sensors

How do these entities interact with each other, with the environment (outside of the system), and with other control loops

STPA Control Loop with Causal Factors

Often in practice components have different goals and perspectives

Organizational culture is not unitary, but differs systematically across subgroups (Schein 2010). For example, professions (e.g., engineering) and subunits (e.g., a specific organizational department) often evince distinctive cultures. Similarly, subcultures exist within hierarchical levels of an organization, meaning that senior executives, middle managers, engineers, and frontline workers may have distinctive cultures, including their views regarding security.

Difficult to identify all the noises and have a good understanding of the underlying basis for the potentially hazardous decisions, or control actions, that could lead the system to a hazardous, or vulnerability, state.

STPA Control Loop with Causal Factors

According to Leveson [2012], there are several fundamental vulnerabilities in a hierarchical system. “At each level of the hierarchical control structure, inadequate control may result from missing constraints (unassigned responsibility for safety), inadequate safety control commands, commands that were not executed correctly at a lower level, or inadequately communicated or processed feedback about constraint enforcement”

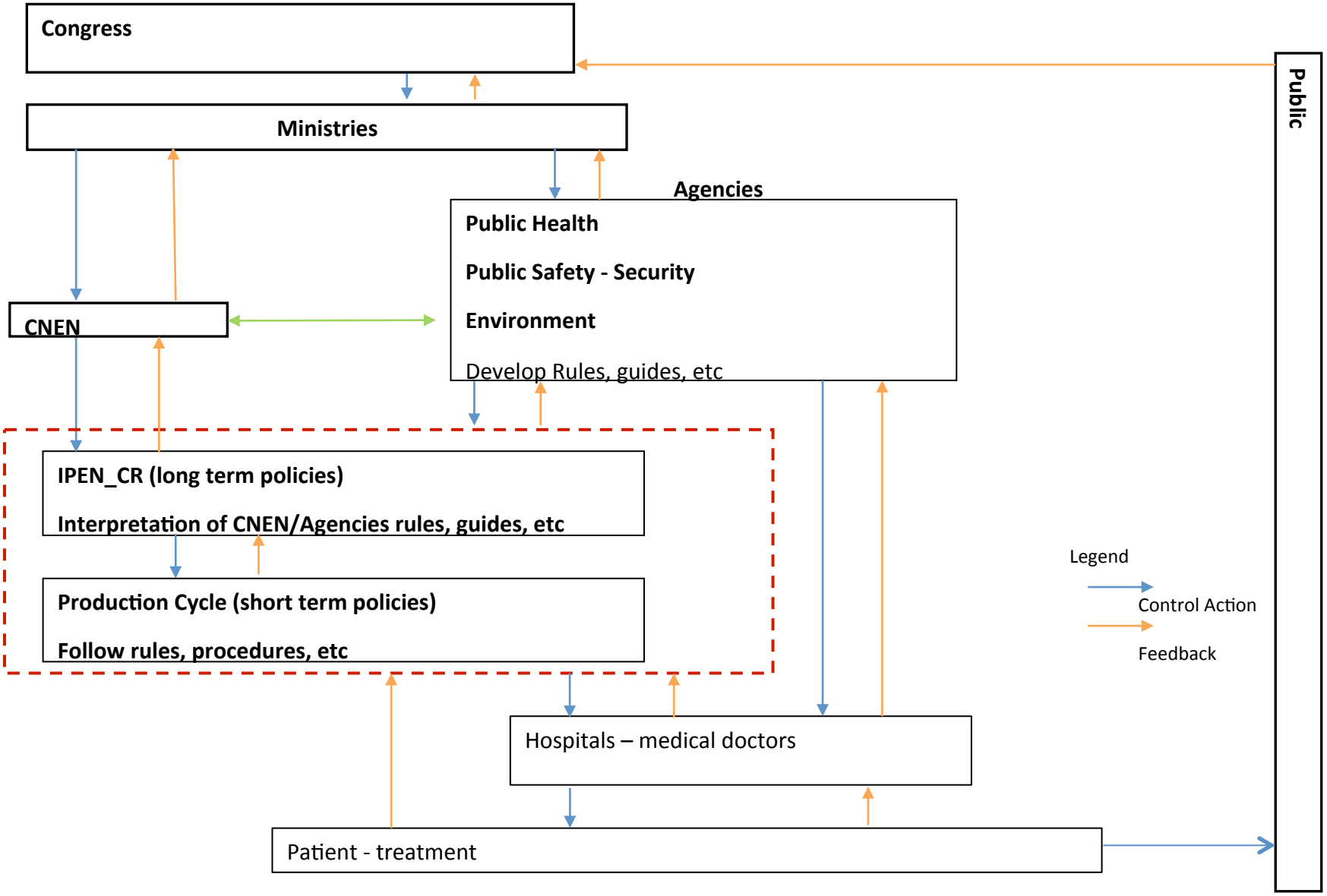
“the required relationship among the system variables (the control laws), the current state (the current values of the system variables), and the ways the process can change state” [Leveson, 2012, p.87], or the dynamics of the process.

STPA Control Loop with Causal Factors

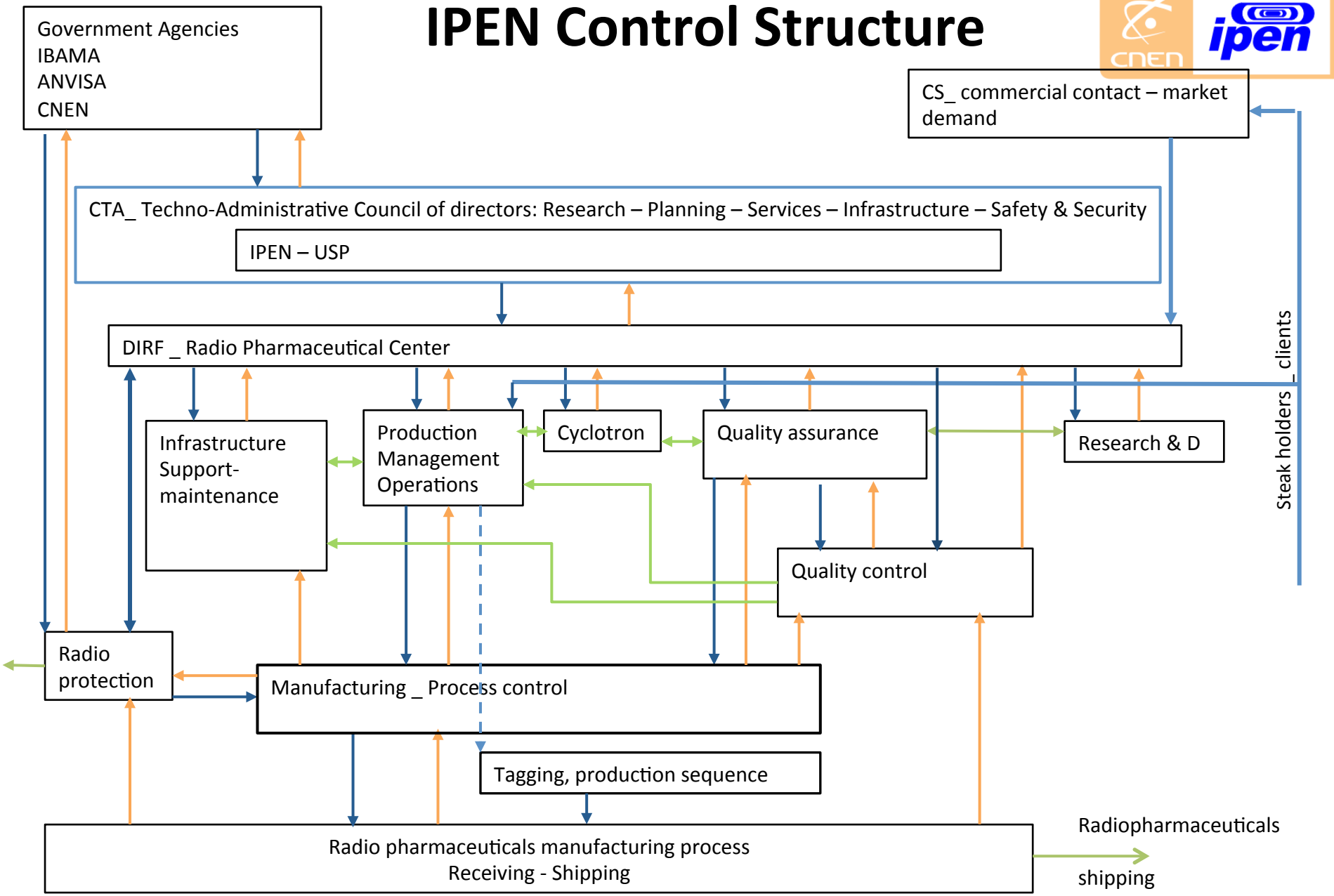
1- Coordination of multiple controllers. There must be some priority of action, or "leader", when processes (or control agents) can be manipulated by more than one source.

2- Consistency of action. Any two controllers with safety-responsibilities related to the same process variables must ensure certain consistency characteristics. These controllers must have a consistent understanding or model of the current state, other actions that can affect that state, and how the state will evolve from those actions.

National Control Structure



IPEN Control Structure



IPEN Control Structure

Different categories of personnel: Transportation, newcomers, maintenance, etc..

Challenges for a common security culture, managing personnel effectively, and carrying out the responsibility for maintaining a safe and secure working conditions.

Across hierarchical levels there are very distinct cultures, including their views on security.

IPEN Control Structure

There is no established policy for assessing the organizational or security culture.

STPA can help to tailor indicators to the specific needs and concerns for a specific sub-system.

Necessary to gather data from multiple levels (executives, managers, employees) and functional areas.

IPEN Control Structure

Control Structure Components

1. *Goal* condition: the controller must have a goal or goals
2. Control *Action* condition: the controller must be able to affect the state of the system, typically by means of an actuator or actuators.
3. *Model* condition: the controller must contain a model of the system
4. *Observability* condition: the controller must be able to ascertain the state of the system, typically by feedback from a sensor

- Basic functions of each entity in the control loop. The requirements for effective, safe and secure system behavior
- Responsibilities
- Observe how these entities interact with each other, with the environment, and with other control loops?

IPEN Control Structure

System's goals

1- To provide the public with a health system that promotes the well being of the population and the patient's and public safety [the national system]

2- To produce radionuclide and radiopharmaceuticals, for treatment and diagnosis, according to the state of the art in science, technology, and best practices

3- To foster the advancement of scientific knowledge; the development of new products; and the enhancement of the existing production techniques

IPEN Control Structure

System's Accidents

Patients are harmed (by the product or lack of it)
Public or workers are contaminated by radioactive material
Environment is contaminated by radioactive material
Radioactive material is stolen
Critical information is stolen
Financial losses
Government/CNEN/IPEN reputation is harmed

OBS. : All the accidents are related to safety and security

IPEN Control Structure

System hazards

1- Products are not shipped or wrong product is shipped
2- Radioactive material released to the environment
3- Radioactive material /radiopharmaceutical is available to unauthorized access
4- Critical information is available to unauthorized access

System's safety and security requirements

The supply chain of radionuclide and radio pharmaceuticals must be reliable
The high quality of radionuclide and radio pharmaceuticals must be assured
The production cycle is protected against any unauthorized access to information and/or to material
No radioactive material is released to the environment or to the public
Any consequences from unauthorized access to materials and/ or information must be minimized

Analysis

Assumptions:

1- People assume that the security system in place (cameras, biometrics, etc) is enough to assure security

2- People assume that the organizational structure in place does not need to be changed. They take it for granted.

3- There is no need for special regulations regarding security of the sources and/or the radiopharmaceuticals

4- Onsite the company campus is safe and secure

5- Following rules is enough to assure safety and security

Analysis

Starting with one of the hazards:

1- The wrong radiopharmaceutical is shipped

This could happen because:

1- Customer places wrong order
2- Commercial department makes wrong notes
3- Products are changed in the shipping area
4- Tags are placed on the wrong package

Some accidents linked to the above hazards

Patients are harmed by a wrong product or lack of it
Financial losses
Government/CNEN/IPEN reputation is harmed

Conclusions

No common understanding about security policy, regulation, etc

All the regulations are focused on manufacturing procedures, quality assurance, etc (Best practices)

Safety mostly considered as a radioprotection problem

Security mostly viewed as a physical protection problem

Difference in cultures at the various levels of hierarchy

Thank You for your Attention