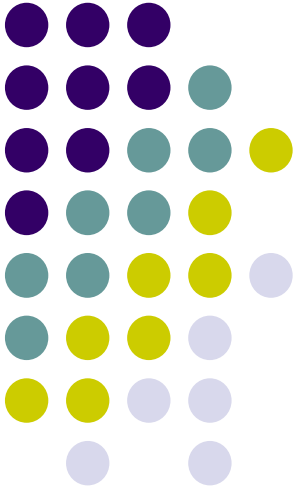
Introducing STAMP in Road Tunnel Safety

Kostis Kazaras

National Technical University of Athens, Mechanical Engineering School, Greece

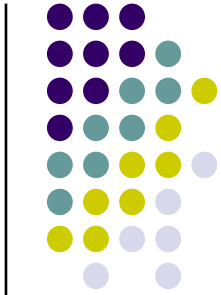
Contact details: kkazaras@gmail.com

kkaz@central.ntua.gr



Problem illustration

Approaches to Road Tunnel Safety



- **Prescriptive based approach**

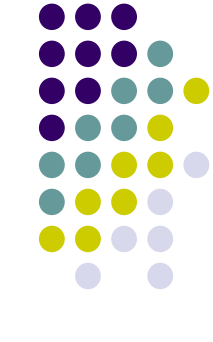
A tunnel is safe if it is in line with regulations
(e.g. European Directive 2004/54, US standard NFPA)

It does not consider either the individual characteristics of the tunnel or how the whole system 'fits' together

- **Risk-based approach**

A tunnel is safe if it meets predefined risk criteria

Risk-based approach



The conceptual link between safety and risk

Safety is the freedom from unacceptable risk

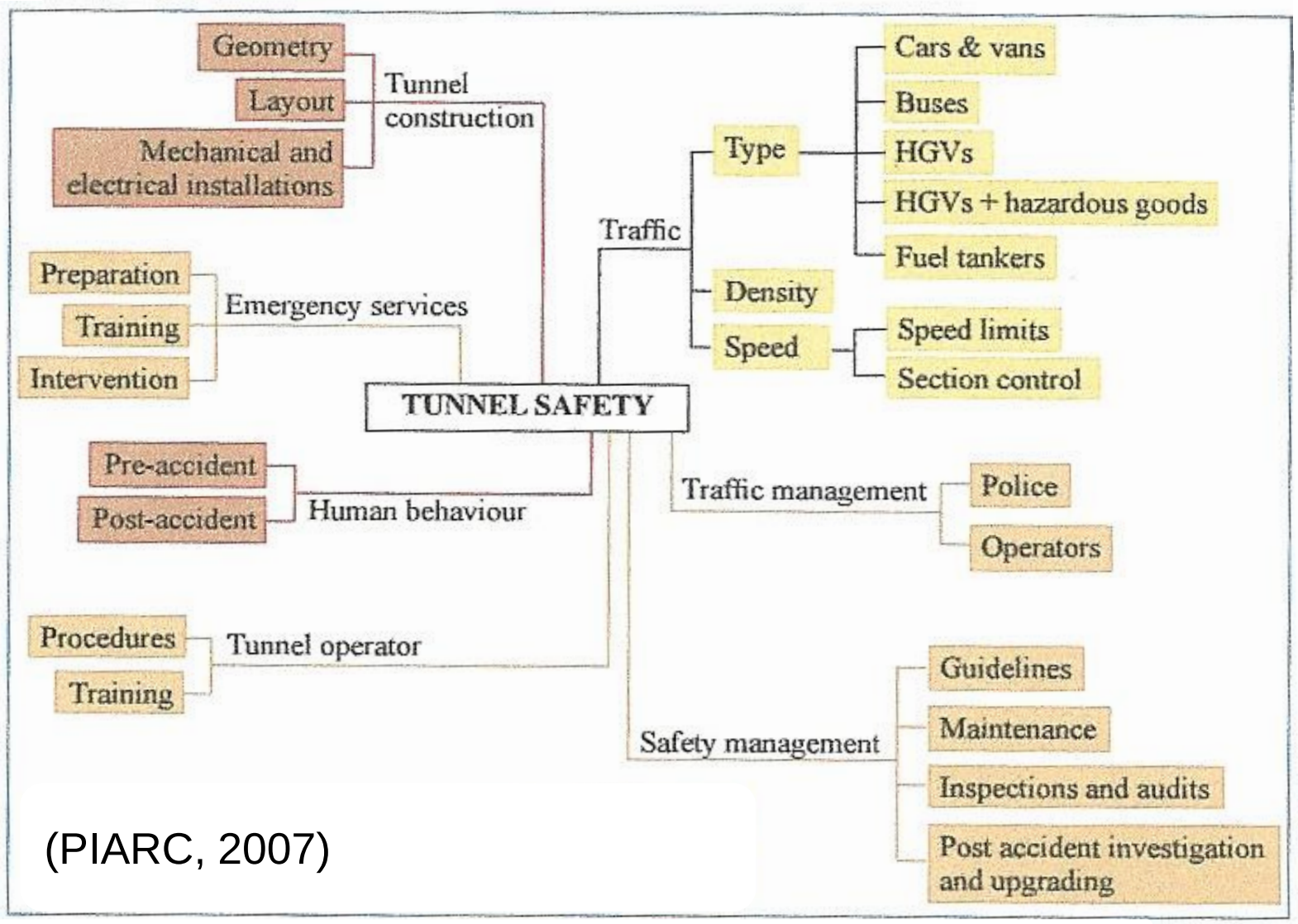
How?

Who defines, what are the acceptable criteria?

Meaning?

Current road tunnel risk analysis are useful tools when building safety into design since they consider several technical aspects but they have limitations **to evaluate** the overall tunnel safety. The tunnel system cannot be **decomposed** in a meaningful way

Road Tunnel Safety



(PIARC, 2007)

Road Tunnel Safety

The tunnel safety chain

Prevention | Mitigation | Self-rescue | Emergency response

1. A steady flow of traffic
2. Ventilation system should control fire and smoke
3. An effective evacuation process
4. Effective emergency assistance

Safety requirements

Introducing STAMP/STPA in road tunnel safety

Looking at the past

Looking at the future

Accident analysis

- What went wrong?
- Why/how we weren't prepared for that?

Safety assessment

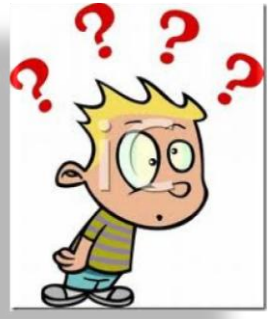
- What can go wrong?
- Are we prepared for that?

Considering organizational aspects, technical aspects, software behavior, human factors, interactions among system components

Case study

Safety constraint/requirement:

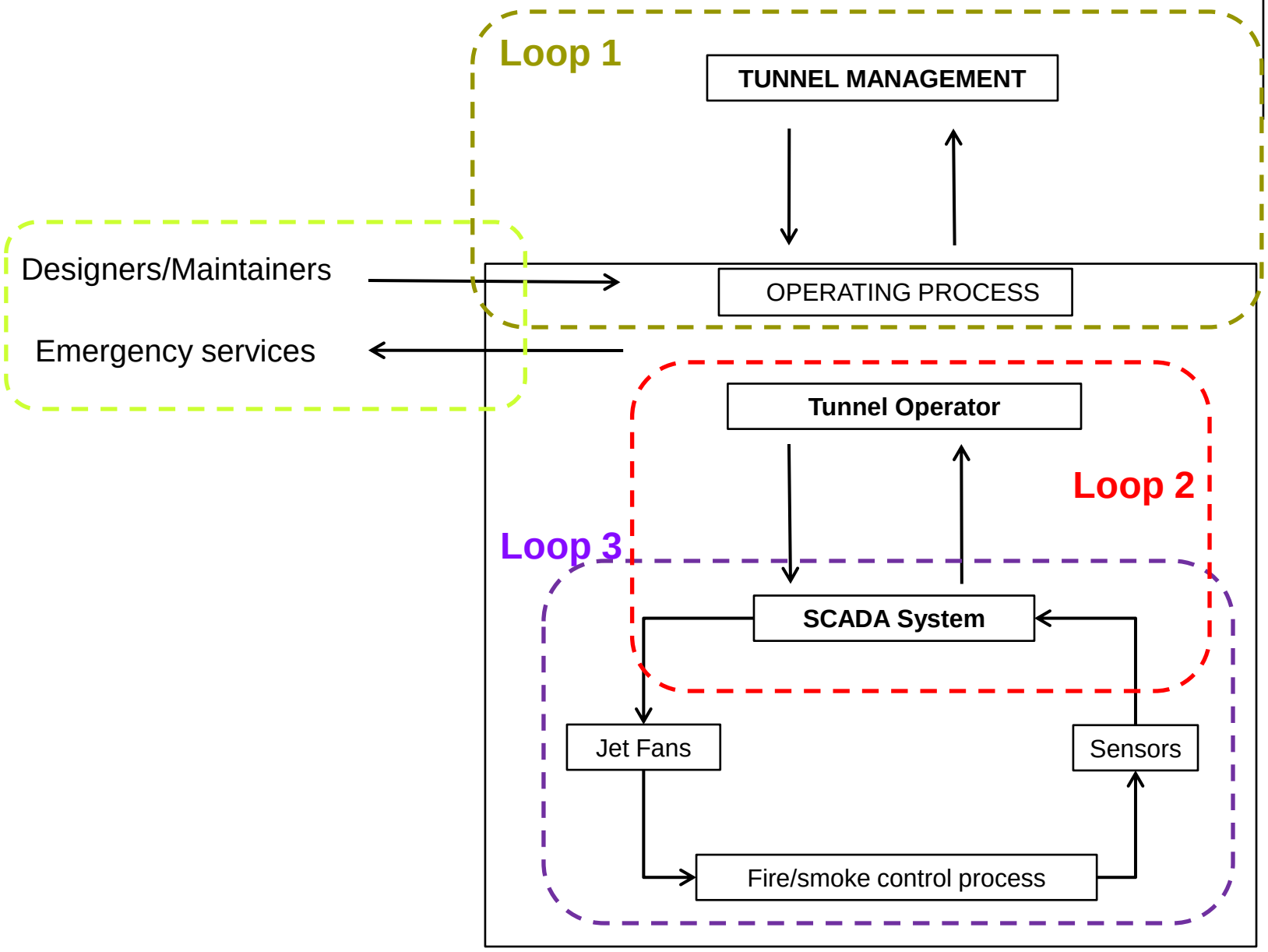
The ventilation system must provide routes with tenable levels of temperature and toxicity



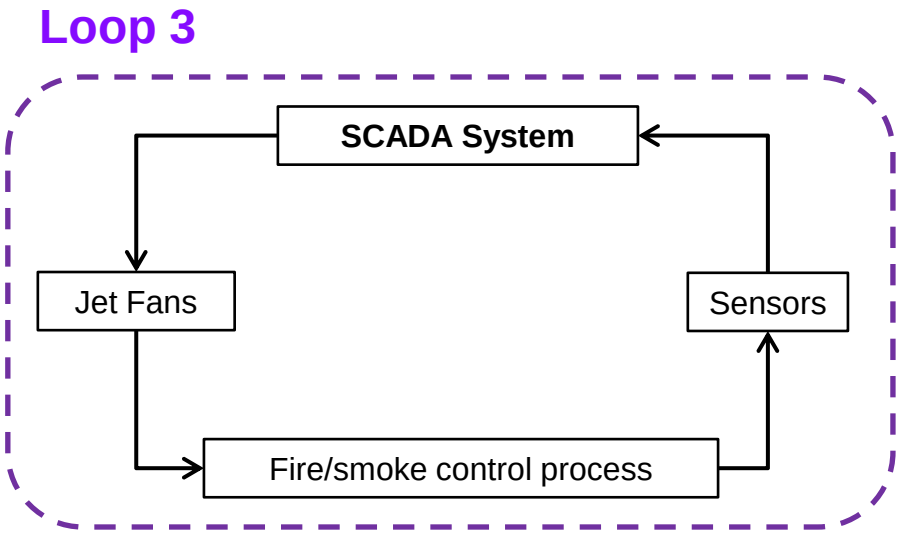
What can go wrong?

How could the safety constraint be violated?

The safety control structure



Identify hazardous control actions



At the sharp end of the system identify inadequate control actions that may violate the safety constraint

Inadequate control actions fall in the four general categories:

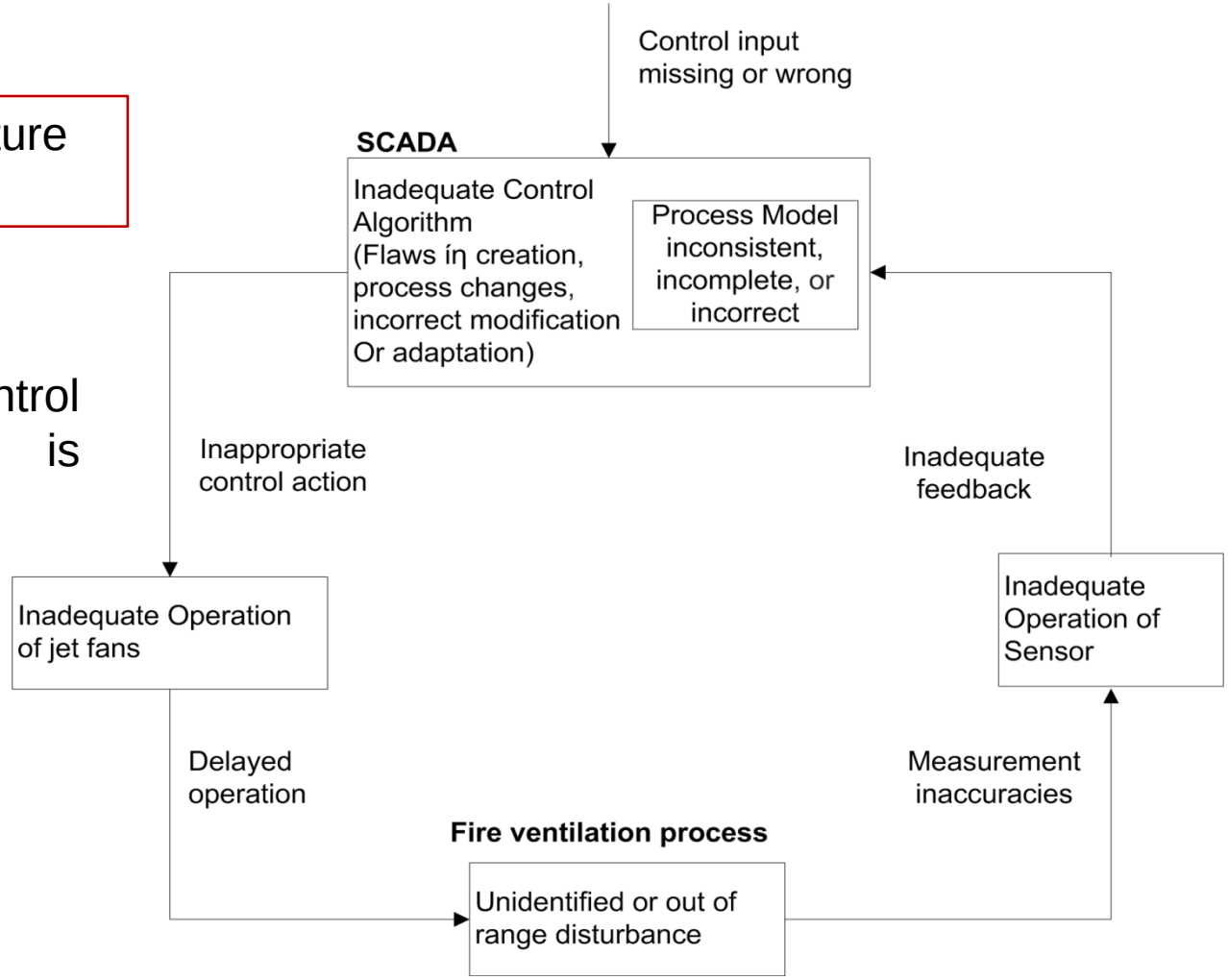
1. The smoke management ventilation mode does not control smoke effectively (a required control action to promote safety is **not provided**)
2. The smoke management mode contributes to other hazards i.e. affect the evacuation process, feeds the fire with oxygen, etc. (**unsafe control action provided**)
3. The smoke management mode is activated **too late**
4. The smoke management mode is stopped before the event has been declared closed (**stopped too soon**)

Determining how hazardous control actions could emerge

The whole control structure should be investigated

In Loop 3:

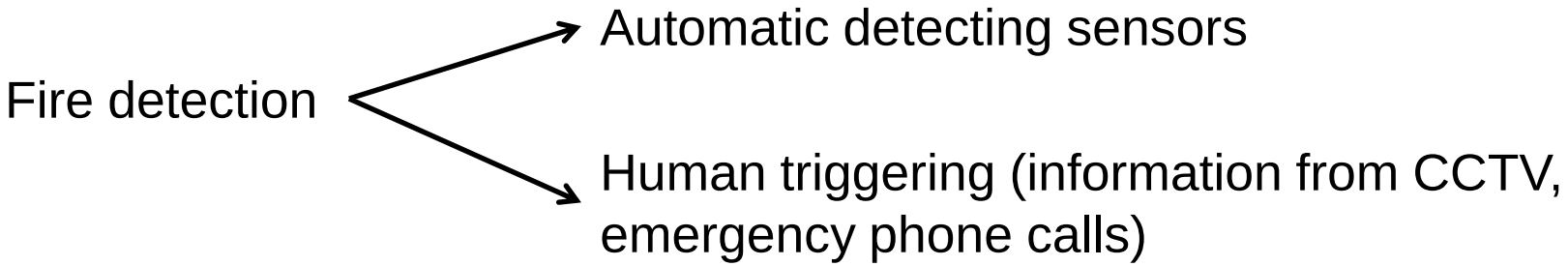
The classification of control flaws (Leveson, 2004) is used for the analysis



Determining how hazardous control actions could emerge (loop 3)

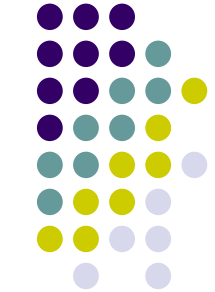
Control input or external information wrong or missing

Necessary control input:
- electrical supply during the emergency
- Fire detection



Electrical supply process and fire detection process should also be considered at this stage!

Determining how hazardous control actions could emerge (loop 3)



Inadequate control algorithm

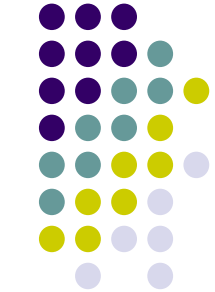
Flaws in creation

Examine response for scenarios including:

- Fire with high/low Heat Release Rate (HRR)
- Fire with Dangerous Goods Vehicles
- Traffic congestion downstream the fire
- Unusual environmental conditions at the tunnel portals
- Situations where particular actuators (jet fans) have failed or are not available

If the variety of the response of the system is much lesser than the requisite variety, there is potential to have inadequate control of the smoke/fire

Determining how hazardous control actions could emerge (loop 3)



Inadequate control algorithm

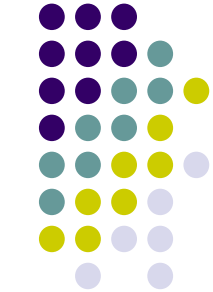
Flaws in adaptation

The smoke management mode overrides the normal ventilation mode in which several operational constraints exist, such as:

- The SCADA avoids starting particular jet fans which have reached a maximum number of starts per hour or they have reached a vibration threshold

Are such operational constraints deactivated when the ventilation is turned to smoke management mode?

Determining how hazardous control actions could emerge (loop 3)



Inadequate control algorithm

Process related changes

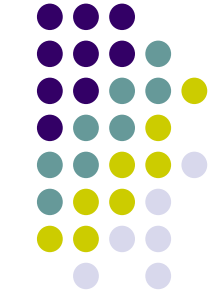
The control algorithm's design is based on parameters such as:

- Expected traffic flaw
- Type of materials transported inside the tunnel
- Meteorological conditions for the area

If these parameters change over time without adapting the control algorithm, there is potential for inadequate control

(such potential is examined at the management level, i.e. loop 1)

Determining how hazardous control actions could emerge (loop 3)



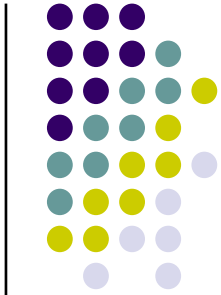
Inadequate process model

STAMP considers **inconsistency** between the process model and the actual system state as a common cause of accidents. Erroneous measurements (e.g. heat, CO detection, air flaw measurements) can lead to unsafe control actions.

Aspects that should be examined when evaluating such a potential are:

- Check for out of range values and system reaction to them
- Arrival rate check for sensors (e.g. a cyclic check every x seconds)
- How the tunnel length affects the speed of feedback (time lags)
- Update of the process model after electrical supply shut down (do variables from sensors initialize with the first coming values)?
- Has the influence of smoke stratification on sensors be considered?

Determining how hazardous control actions could emerge (loop 3)



Out of range disturbances, process output, coordination

- The limitations of the control system should be clear and they must have been passed to the operators (see loop 2)
- Thoroughly examine how the ventilation output affect fire fighting, communications systems (noise) and the evacuation process
- Since emergency services take over the command when they appear on site, thoroughly check for co-ordination issues

Inadequate operation of jet fans and sensors

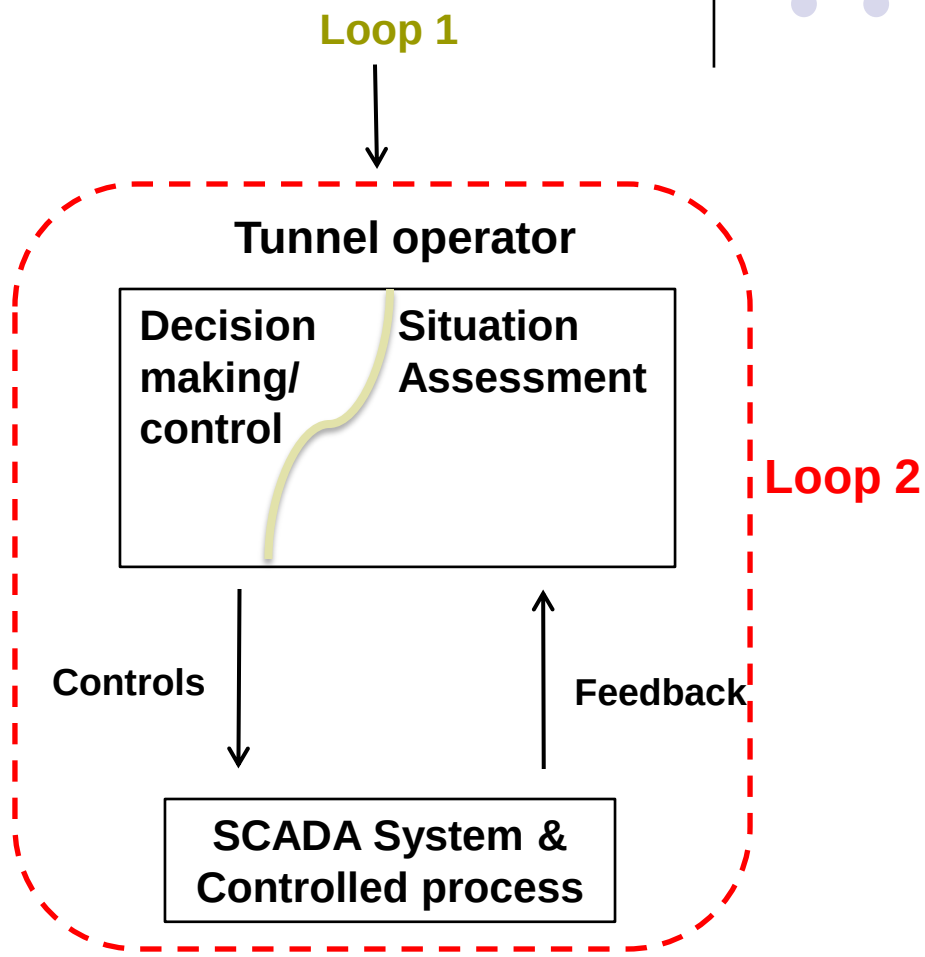
- Examine if there is an adequate maintenance program, whether the operational assumptions and limitations have passed from designers to maintainers
- Examine whether tests on the reliability of the equipment have been performed/scheduled

Determining how hazardous control actions could emerge (loop 2)

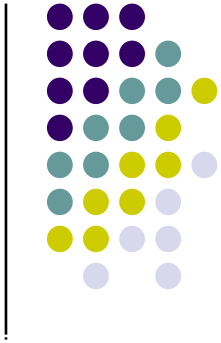
- The tunnel operator's error modes (phenotypes) result in the four identified hazardous control actions
- These actions could occur due to:
  (1) inadequate control
  (2) inadequate feedback

Feedback concerning

1. The state of the controlled process
2. The effects of the operator's actions



Determining how hazardous control actions could emerge (loop 2)

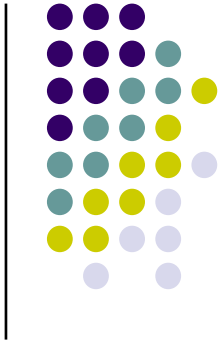


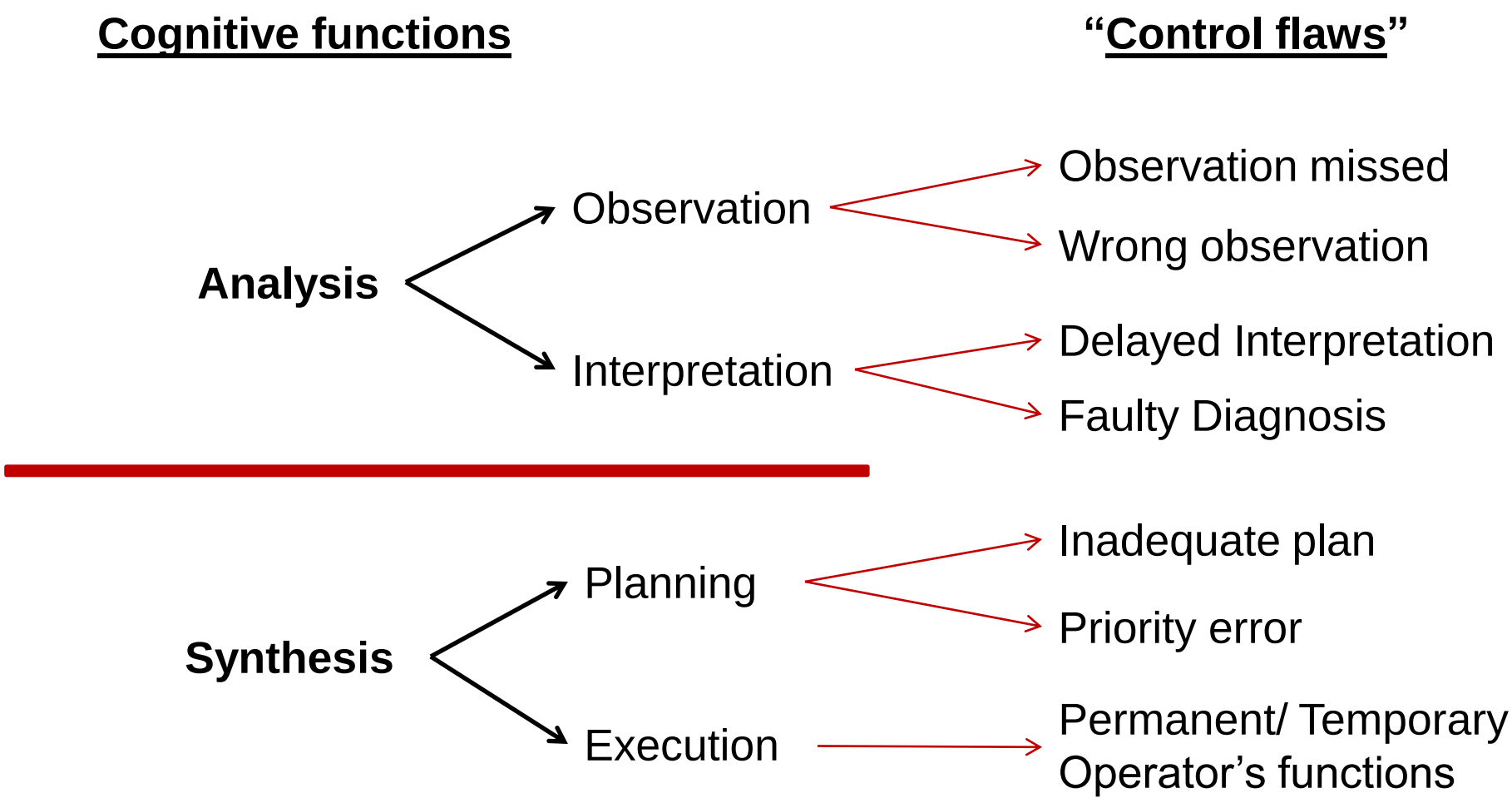
- To examine the potential for the hazardous control actions at this level, concepts from the classification scheme provided in CREAM (Hollnagel,1998) are also used in the analysis.

Person genotypes	**Technology genotypes**	**Organizational genotypes**
- Specific cognitive functions - Person related functions	-Equipment function (has been analyzed in loop 3) -Interface	-Ambient conditions -Communications -Training (analyzed in loop 1)

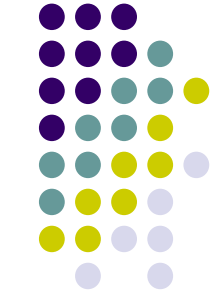
Since technology and organizational genotypes are examining thoroughly at other loops, at this level the analysis concentrates mainly on cognitive related functions

Determining how hazardous control actions could emerge (loop 2)





Determining how hazardous control actions could emerge (loop 2)

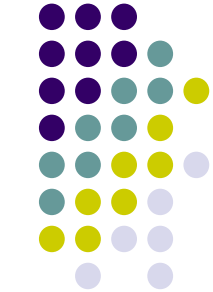


Examining the potential of control flaws

Inadequate Observation

- During long period of normal operating, vigilance may be threatened. This is especially critical during the night (3-6 am). How does the system cope with this? (e.g. switching between monitoring and other control activities)
- Feedback channels may fail during an emergency. Have redundant paths (e.g. cameras, sensors) been designed?
- Provide not only visual signs but also sound signals for detecting critical situations

Determining how hazardous control actions could emerge (loop 2)



Examining the potential of control flaws

Inadequate Interpretation

- Examine whether there are incoming signals during an emergency, some of which are not relevant. Is it possible for the operator to switch off some alarms during an incident?
- How is feedback displayed to the tunnel operator?
  -Avoid displaying absolute values if not necessary, indicate whether a value is over or under a limit
  -Design the control panel to mimic the physical layout of the tunnel
  -Minimize the need for extra mental processing to get the information

Determining how hazardous control actions could emerge (loop 2)

Examining the potential of control flaws

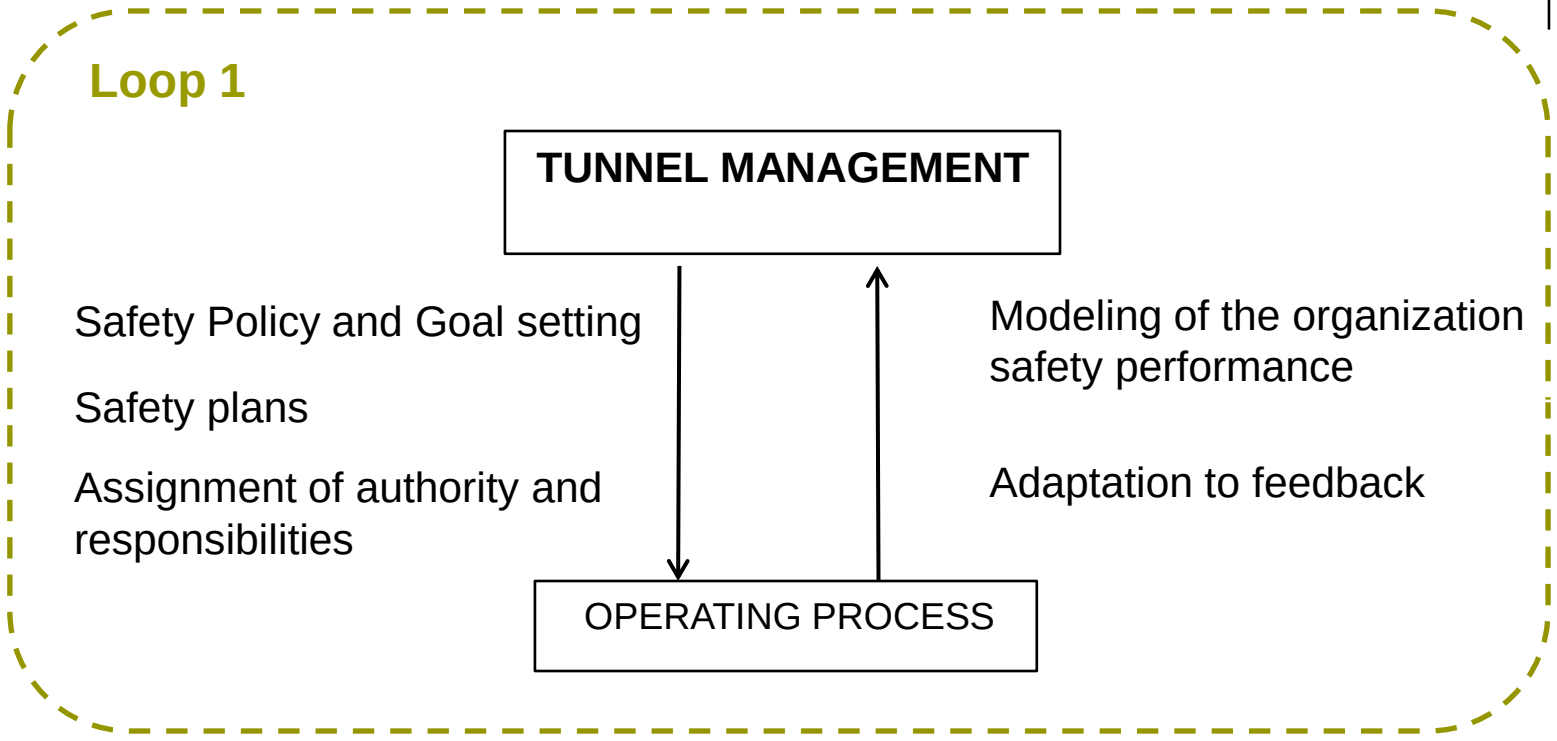
- **Inadequate planning**

  Many different decision actions may be required, therefore rule-based and skill-based activities should be preferred to knowledge-based activities (see loop 1).

- **Temporary/Permanent person related functions**

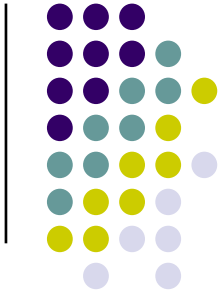
  Fear, fatigue, panic, bad eyesight, color blindness. The working hours of shifts and the selection criteria for recruitment should be examined. The ambient conditions in the control room (temperature, sound, illumination) should also be examined.

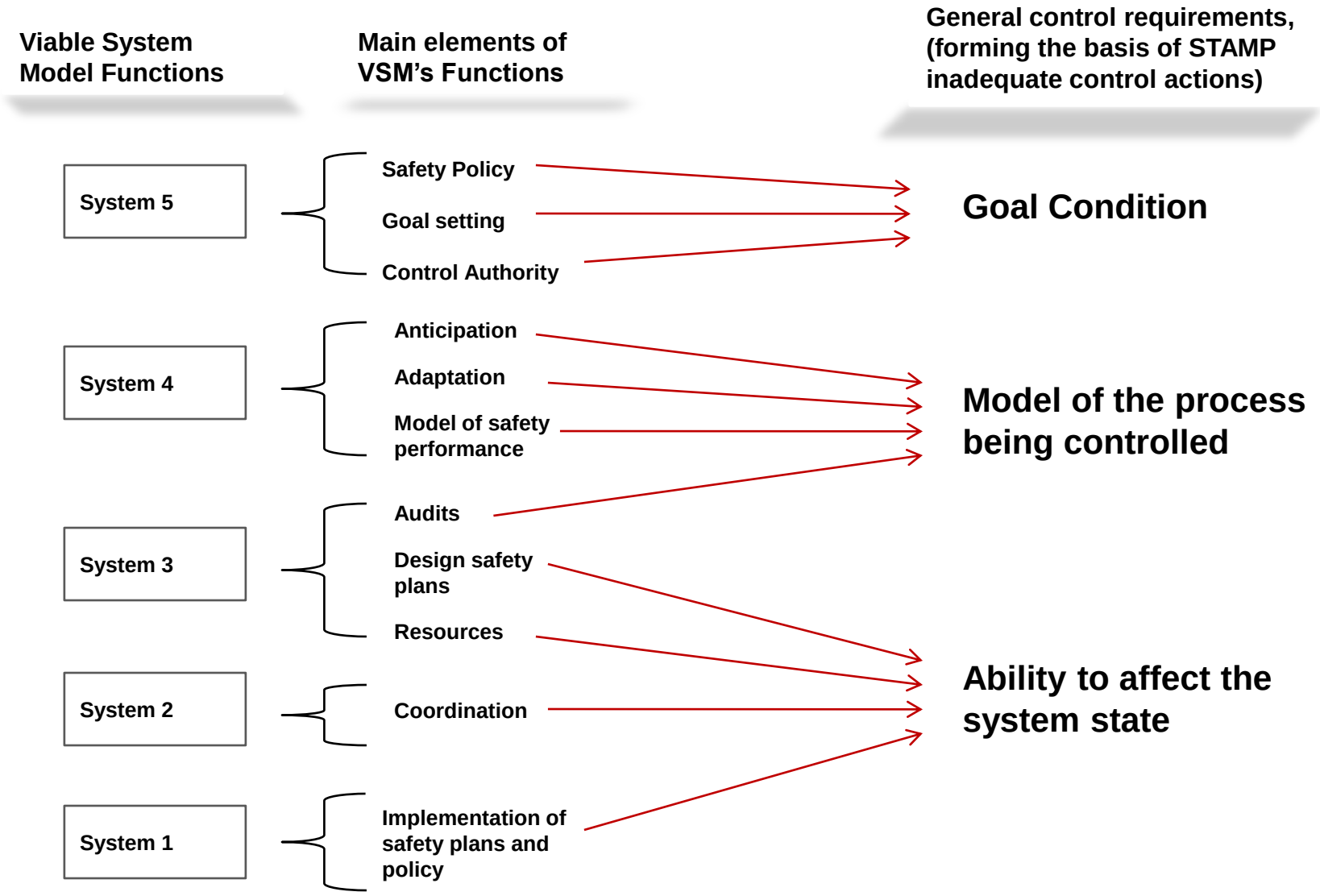
Determining how hazardous control actions could emerge (loop 1)



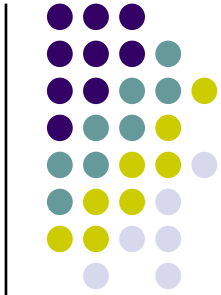
At this level some concepts from organizational models (i.e. the Viable System Model; Beer) can be used in order to enhance the analysis

Determining how hazardous control actions could emerge (loop 1)





Determining how hazardous control actions could emerge (loop 1)



Inadequate assignment of authority and responsibilities

Examine for:

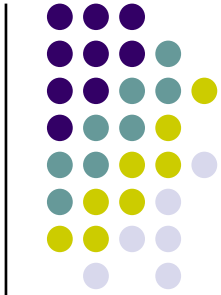
- Gaps and overlaps of responsibilities among the tunnel operator, the SCADA system and the emergency services
- Examine the selection criteria for the tunnel operators during recruitment

Inadequate design/implementation of safety plans

Examine whether:

- Specific incident handling procedures have been designed for the smoke control in coordination with emergency services
- Specific safety plans have been designed for scenarios that can't be controlled by the SCADA control algorithm
- A particular training program for the tunnel operator is followed

Determining how hazardous control actions could emerge (loop 1)



Inadequate modeling of safety performance

Examine whether there are adequate feedback/feed-forward mechanisms for modeling the tunnel safety performance, such as:

- Safety inspections audits, debriefing of emergency exercises
- A structured method for accident/incident analysis so as to learn from events
- Updates concerning: the traffic forecast study, restrictions based on the transportation of DGs through the tunnel, changes in tunnel personnel and tunnel facilities

Inadequate adaptation to changes

Examine whether the feedback and feed-forward loops have been closed. For example: if changes occur in the tunnel personnel and/or in the tunnel equipment, has the tunnel organization the appropriate procedures to update the safety plans?

Introducing STAMP/STPA in road tunnel safety

For accident analysis:

Identify the safety requirements/constraints associated with the accident and investigate how/why they have been violated. Generate recommendations

For safety evaluation:

Identify the safety requirements/constraints associated with the possible accidents and evaluate if the system has the necessary safeguards to avoid the losses

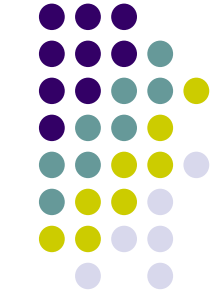
What tools and criteria can be used during the evaluation process? To evaluate trade offs in the system design?

A thought for quantifying results

How can we enhance a STAMP based assessment with a quantitative support tool?

- ✓ A methodology based on the **Analytic Hierarchy Process** (AHP) for a quantitative safety assessment
- ✓ A decision support tool to evaluate and compare alternative system components and operational strategies

A thought for quantifying results



The steps of the methodology

1. Define the goal of the hierarchy and put it at the top level

2. Build downward the hierarchy. Each level has to gather the factors that influence the elements of the above level and that are directly influenced by the elements of the level below

3. At the bottom of the hierarchy place the indexes which represent the factors that will be considered to judge the system

A thought for quantifying results

Level 1

The ventilation system must control smoke/fire

..other safety requirements/constraints

Since the goal of the hierarchy is the overall tunnel safety, at this first level the high-level safety requirements and constraints are defined

Level 1: The ventilation system must control smoke/fire

Level 2	**Level 3**
SCADA System	Control inputs
	Control algorithm
	Process Model
	Jet fans/sensors operation
	Out of range disturbances/ process outputs
Tunnel Operator	Analysis (observation, interpretation)
	Synthesis (planning, execution)
Tunnel Management	Assignment of control authority and responsibility
	Design/implementation of safety plans
	Modeling of safety performance
	Adaptation to changes

Level 2 & Level 3 increase the detail by analyzing aspects related to the main topic of the parent levels

A thought for quantifying results

Level 2	Level 3	Indexes (Level 4)	Possible answers
Tunnel Operator	Analysis	Redundancy of feedback channels Does the control panel mimic the physical layout of the tunnel	(SENSORS, CCTV, etc) Yes/No

The questions that form the level 4 and evaluate the safety of the tunnel are the issues highlighted by the STAMP based assessment

For each possible answer the alternative options takes a qualitative ranking score by the analyst, which is afterwards translated into a quantitative score by a software tool which is based on AHP method. Criteria for the qualitative ranking can be based on the effectiveness, stability, observability, response time and level of confidence for the design option to enforce the safety constraint

A thought for quantifying results

Safety evaluation indexes	Scores (0-100)
Overall safety assessment index	80/100
Safety assessment score for the safety constraint x	65/100

- The overall safety assessment index expresses that the system gains a score of 80, on a scale from zero to one hundred.
- Relative scores measure the safety performance of the system according to specific safety requirements. Therefore, areas for improvements are easily highlighted.
- When modifications are introduced in the system, such an assessment tracks the dynamic evolution of the whole system.

Final thoughts about the STAMP/STPA

- ✓ A very supportive method in the attempt to examine the whole system
- ✓Systems thinking in safety is easier to be said than to be done. STAMP provides a structured way to evaluate the system and identify weak points
- ✓Leading safety performance indicators can be introduced based on the STAMP method

final thoughts..

New tools can be proposed to enhance the analysis when examining organizational/human factors and when presenting the analysis to decision makers

Additional information in:

Kazaras K., Kirytopoulos, K. (2011). **Applying STAMP in road tunnels.** IET Conference Publications.

Kirytopoulos K., Kazaras, K. (2012). **The need for a new approach to road tunnel risk analysis**. Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, ESREL 2011

Thank you!