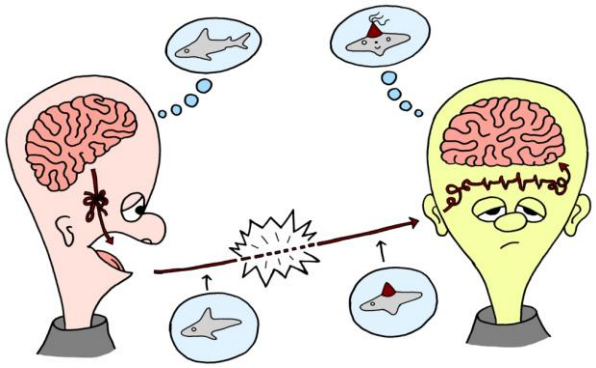
Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

DOCUMENTATION OF ASSUMPTIONS AND SYSTEM VULNERABILITY MONITORING: THE CASE OF SYSTEM THEORETIC PROCESS ANALYSIS (STPA)

Dr. Nektarios Karanikas, CEng, PMP, GradIOSH, MIET, MRAeS
Associate Professor of Safety & Human Factors

Aviation Academy

STAMP EU Workshop, 14-15 September 2017, Reykjavik, Iceland

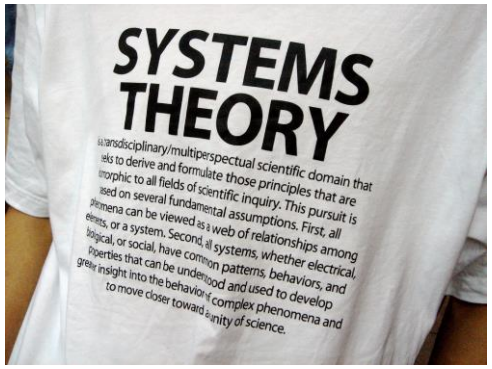


WHY ASSUMPTIONS?

- Assumptions are an inextricable part of problem-solving due to limited knowledge, capacity and resources to:
  - comprehend completely systems dynamics and complexity
  - exert full control over interactions and individual behaviours
  - ensure entirely that our solutions will sustain any external or internal disturbance
- Assumptions mainly refer to the:
  - conceptual and analytical models used
  - relationships and behaviours of system elements, considering also surrounding conditions
  - quality of available data

ASSUMPTIONS AND SYSTEM PERFORMANCE

- The more the assumptions made, the higher the dependency on agents and factors outside our direct control
- The validity of assumptions is of paramount importance to maintain viability of any solution
- Assumptions must be visibly documented to allow their check and revision
- The more the invalid assumptions, the more vulnerable the system
- The monitoring of validity of assumptions can function as a leading performance indicator



ASSUMPTIONS & STPA

- Ideally: a complete analysis with STPA includes all parameters affecting system performance and leads to development and testing of inclusive and exhaustive causal scenarios to evaluate system vulnerability
- Reality: we are not fully knowledgeable of and don't have full control over open systems – we might lack the resources required for analysis and testing
- Consequence: assumptions are unavoidably part of the STPA execution and deliverables

STUDY QUESTIONS

What assumptions might be made during the application of STPA?

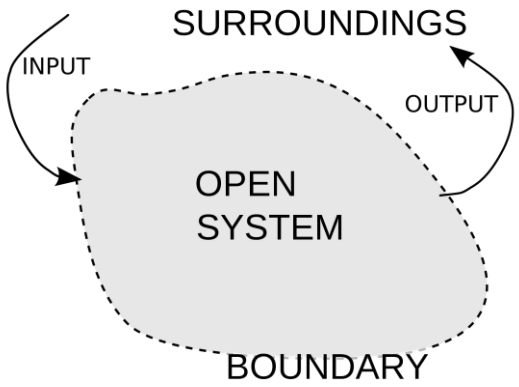
How can the acknowledgement of such assumptions assist the STPA analysts and system performance monitoring?

PRINCIPAL RESULTS

- Ten assumption groups were identified
- Assumptions might be generated along the various stages of STPA preparation and execution as well as the exploitation of the analysis deliverables
- Assumptions falling in six of the groups are deemed as inevitable
- The assumptions linked to the rest of the groups depend on the scope and resources linked with the analysis and utilization of its products

PRINCIPAL RESULTS

- The analysis stage and system level of assumptions were connected with their expected impact:
  - the higher the hierarchical level the assumptions are invalid, the higher the vulnerability of the system
  - the assumptions generated earlier in the analysis will have larger effects on system performance than the assumptions made at lower analysis levels
- The monitoring of assumptions validity is suggested to be performed under a top-down system level priority



ASSUMPTIONS: SYSTEM DEFINITION

The elements and interactions excluded from the analysis, where applicable:

- have predictable effects on the system under study

(Assumption group No 1 - Inevitable)

- change at a pace that allows a successful adaptation of the system under study to maintain achievement of its objectives

(Assumption group No 2 - Inevitable)

ASSUMPTIONS: SYSTEM OBJECTIVES & CONSTRAINTS

Assumptions group No 3 (System Objectives)

The system objectives included in the analysis do not conflict with the system objectives excluded from the analysis

Assumptions group No 4 (System Constraints)

The agents outside the system under study maintain the system constraints assigned to them

ASSUMPTIONS: CONTROL STRUCTURE & SYSTEM REQUIREMENTS

Assumptions group No 5 – Inevitable (Control Structure)

The behaviour of elements and/or subsystems belonging to system levels lower than the ones analysed can be confidently predicted

Assumptions group No 6 – Inevitable (System Requirements)

External agents will fulfil the requirements assigned to them

Assumptions group No 7 – Inevitable (System Requirements)

The system controllers will fulfil the requirements assigned to them given that external agents will have fulfilled their relevant requirements

ASSUMPTIONS: CAUSAL SCENARIOS TESTING

Assumptions group No 8

The occurrence of causal scenarios not to be tested is practically improbable

Assumptions group No 9

The requirements excluded from scenario testing are always fulfilled

Assumptions group No 10 - Inevitable

The results from causal scenario tests are reliable and valid

REMARKS (1/2)

- The list of assumption groups was based on a specific line of reasoning grounded in literature and practice
- The total number of analysis assumptions per case will be finalised after all STPA application iterations
- It was out of the scope to consider assumptions relevant to the skills of the analysts in terms of analysis depth and quality
- The current study aims to:
  - raise awareness of analysts about possible and inevitable “imperfections” of any analysis
  - demonstrate that even system-focused and systematic analysis techniques such as STPA can be still subject to assumptions

REMARKS (2/2)

- The assumption groups proposed can be amended based on further experience and perspectives of other analysts as well as future research
- But most importantly:

The systematic nature of STPA allowed a systematic way of indicating areas of possible assumptions. This confirms the analytical power the technique offers.

ACTION ITEMS

- Documentation and traceability of assumptions consistently and transparently to increase the credibility of STPA analyses
- Inclusion of a dedicated section about assumptions in the next versions of the STPA Primer or future relevant handbook/guidebook
- Incorporation of fields about assumptions in the software packages supporting STPA application (e.g., XSTAMPP, SAHRA, ERMF)

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

DOCUMENTATION OF ASSUMPTIONS AND SYSTEM VULNERABILITY MONITORING: THE CASE OF SYSTEM THEORETIC PROCESS ANALYSIS (STPA)

Dr. Nektarios Karanikas, CEng, PMP, GradIOSH, MIET, MRAeS
Associate Professor of Safety & Human Factors

Aviation Academy

Questions please?

STAMP EU Workshop, 14-15 September 2017, Reykjavik, Iceland

CREATING TOMORROW

Contact: n.karanikas@hva.nl