Using STPA in the Design of a Nuclear Power Plant Control Room

A. Lucas STEPHANE
MS Business Intelligence
MS Experimental Psychology

Research Assistant
Florida Institute of Technology

April 19, 2012
MIT
Research Context (ongoing PhD) – digitalization of NPP MCR...

- **Sponsor**: AREVA R&D – Human Factors Department
- **Mission**: Force of Proposals
  - Early exploration of relevant emergent technologies

- **Vision**: sociotechnical Human Centric Convergence
  - Inter-domain (Aeronautics ➔ Nuclear, …)
  - Interdisciplinary (Psycho, Eco, Socio, Techno, Organizational)

- **Research Focus**: Design & Evaluation of **Instruments & Controls (I&C)**
  - 3 main layers of intertwined requirements
    - Presentation
    - Content
    - Joint Activity (co-activity, interaction)

- **Target System**: **Safety Instruments & Controls System (SICS)**
- **Target location**: Nuclear Power Plant Main Control Room (**NPP MCR**)
- **Target population**: **Knowledge Workers**
Research Phase I

- **Phase I - 2010: Exploration & Identification of**
  - Technology
    - Stereoscopic 3D (S3D): compact & natural presentation/visualization
    - 3D Gaming Engines: *full* interactivity (vs. animation)
    - Touch surfaces (fixed & mobile): joint activity/interaction
    - personal Drone *in operations*: accessing dangerous locations
  - Content
    - plant subsystems (i.e. *partial* approach, *single unit*)
    - *Incident* scenarios
  - Sociotechnical modeling
    - Belief Desire Intention Multi-Agent Systems
      - *External Viewpoint*: Roles, Responsibilities, Resources, Services
      - *Internal Viewpoint*: Beliefs, Desires, Intentions
    - Service Oriented Architecture *Reference Architecture*
      - techno mediation + management for Social Structures
  - **Usability** Design & Evaluation methods
    - Situation Awareness (*rational external* aspects)
    - *Self* Awareness (motivation, emotions, loss-aversion, cognitive dissonance)
    - Workload
    - Eye Tracking
Phase I: Lab Configuration...

- Auto-stereoscopic Display
- S3D Projector
- Data Glove
- S3D Laptop
- S3D Touch Display
Phase I: Lab Configuration... Touch surfaces: Tablet (*Remote Desktop*) & Touch Screen
Phase I: Lab Configuration...Personal Drone – Fly using tablet

Video Streamed on iPad from Drone frontal camera
Phase I: Lab Configuration...Eye Tracking
Research Phase II

• *Phase II - 2011: Fukushima and after…*
  ⇒ Reinforcing Safety in Design & Evaluation
    ▪ Requirements Management in terms of Safety Criteria for Design & Evaluation (beyond Usability)
      ▪ Integration of Safety & Usability methods & criteria…
    ▪ STAMP, STPA & SpecTRM proposed during Fall 2011

  ⇒ Content for uncertain/unpredicted/unpredictable situations
    ▪ Uncertainty approaches in design (KOMPASS)
    ▪ Adaptive Case Management: shift from process improvement (analytic stage) toward process execution (operations stage)

  ⇒ Accident scenarios & processes
    ▪ Fukushima accident understanding…
    ▪ Considering multiunit events & crisis management (Units 1 to 4)
      ▪ Complexity & uncertainty in understanding (i.e. NUREG-1935)
        ⇒ Complexity in design – intellectual unmanageability…
    ▪ Global approach
# Phase II: Integration toward Human Centric Convergence

<table>
<thead>
<tr>
<th>DESIGN STAGE</th>
<th>Safety Methods</th>
<th>BDI MAS</th>
<th>SOA RA</th>
<th>BPMN</th>
<th>Uncertainty</th>
</tr>
</thead>
</table>
| **Main Outputs & Span** | - Analysis  
- Drive Specifications  
- Drive Implementation | - Sociotechnical Cognitive Modeling  
- Implementation | - Reference Architecture  
- Drives Specifications  
- Drives Implementation | - Standard Notation  
- Modeling  
- Implementation | - Sociotechnical Criteria  
- Recommendations |
| **Artifact(s)** | - Interdependent  
- Intent Specifications  
- Human-Computer Interaction  
- Constraints | - Interaction Service Providers  
- Communication  
- External & Internal viewpoints | - Interaction Service Providers  
- Constraints  
- Quality of Service | - Interaction Service Providers | - Automation types  
- Limits of Control |
| **User(s)** | - Responsibilities  
- Requirements  
- Operator Task models  
- HCI models | - Roles, Responsibilities, Resources, Services  
- External & Internal viewpoints | - part of the Social Structure  
- Interaction driven by Intent  
- External viewpoint | - Information Providers & Consumers | - Expertise  
- Motivation |
| **Task(s)** | - Safety Margins/Constraints  
- Analysis  
- Allocation  
- Dysfunctional Interactions | - Agent plans (partial or complete)  
- Parallel execution | Achieve Awareness in:  
- Orchestration  
- Collaboration  
- Choreography | - Orchestration  
- Collaboration  
- Choreography  
- Parallel execution | - Process transparency  
- Dynamic Coupling in Process Control |
| **Organization(s)** | - External Interfaces  
- Environment Models  
- Audit  
- Resilience  
- Adaptability | - no specific support (i.e. any) | - Governance  
- Regulations  
- Contracts  
- Security Model  
- Flexibility  
- Agility  
- Adaptability | - Inherit SOA reference features | - Rigid vs. Flexible  
- Adaptability |
| **Situation(s)** | - Incidents & Accidents explicitly considered  
- Hazard Analysis | - no specific support (i.e. any) | - Case Analysis (functional & non-functional) | - Incidents & Accidents explicitly considered through Event Escalation | - no specific support (i.e. any) |

© Lucas STEPHANE, 04/19/2012   STAMP/STPA Workshop, MIT
Phase II: How: Non-Linear Safety methods - retrospective & prospective

- Fukushima Dai-Ichi **Multiunit** Accident Analysis using:
  - primary sources (TEPCO, NISA)
  - secondary sources: (IAEA, NUREG, AREVA and other reports)
  - STAMP: accident understanding...
  - STPA & SpecTRM: Design & Evaluation

- **STAMP output**: identifying main directions for the current design
  - holistic vertical (organizational layers) & horizontal (multiunit) analysis

- **STPA output**: providing **Safety Margins criteria for**
  - *Designing* the proposed I&C (visualization & controls; processes; decision-making under uncertainty)
  - *Evaluating* the proposed I&C

- **SpecTRM outputs**
  - Create Intent Specifications
  - Perform STPA
  - Verify & Validate Models through *Simulation & Experimentation*
Phase II: STPA - SpecTRM

DR record from the SpecTRM user guide. © SafeWare 2011
Phase II: WHAT

**WHAT is to be achieved:**

- Design and Evaluate **S3D representations** of I&C for the Safety Instruments & Controls System (*SICS*) that aim to **improve safety support for decision-making and consequent operations** (i.e. crisis management) in an accidental scenario

- Such S3D representations span both situated **Visual aspects** as well as **Collaborative aspects** (joint activity, interaction)

- **Direct Interaction** supported by **touch features** is accorded the main emphasis
  - Controls are embedded in the visual scene
Phase II: WHAT

**WHAT S3D content:**

- **Two main classes of I&C**
  1. **Internal I&C** related to the NPP: temperature, pressure, sociotechnical system states, **main plant organs** (i.e. reactor, Spent Fuel Pool, Diesel Generators) and their **trends**
  2. **External I&C** related to the **environment**: possible impacts on the environment

- **Two classes of processes** (including *analytic* aspects related to states and dynamics) in *normal & abnormal* conditions
  1. **Predefined processes** (if/when available)
  2. **Adaptive processes** in case no predefined processes are available (errors, exceptions, escalation)
Phase II: WHY

**WHY such S3D representations & content:**

- In current visual environments overloaded with information, **S3D representations** offer an efficient alternative for **tackling information density under time pressure**

- **Deep content** related to *Decision Making & Action*
  - Games against ‘Nature’
    - Influence Diagrams & *Dynamic* Bayesian Networks
  - Imperfect Information Games
    - plans of action (*BPMN* process representations)

- **S3D mapping of Context Space & Resources Space** for enhancing *understanding & awareness*
Phase II: WHY

**WHY such a context:**

- The accidental context enables to demonstrate the usefulness of S3D representations & content, supported by relevant devices

⇒ **Design a minimal autonomous I&C for Vertical & Horizontal communication and collaboration**

  - networked handheld devices (i.e. tablets): loss of electrical power (i.e. Station Black Out)
  - personal drones in operations: surveillance & monitoring of equipment in inaccessible locations (i.e. due to high radioactivity levels)

- It is assumed that at least in one location, one S3D display can function...
Phase II: How: **Core of the study**

*Hard* Decision-Making in uncertain / unpredicted / unpredictable situations:

- Based on the *prescriptive decision analysis approach* (*Goal-driven*)
  - Influence Diagrams & *Dynamic* Bayesian Networks: prior (subjective) probabilities (human collaboration)
  - Preferences
  - Risk analysis
    - *Conflicting Objectives*
  - Trade-offs / Satisficing / Sacrificing
  - ... Adaptive Case Management

- Completed with *consequent adaptive plans of action* (*Event-driven*)
  - Adaptive BPMN
  - Coopetition

- Similar approaches: Integrated Risk Picture (SESAR); AgenaRisk
  - Difference: in these approaches, probabilities are proposed ex-ante...
Phase II: How much: Specifications & Implementation
Phase II: How much: **Specifications & Implementation**

…Multiunit in a near future…
Phase II: How much: *Experiment Design*

**Scenarios**

- Based on *Life-Critical Role-Playing Game*
- Implementing *decisions & consequent actions in terms of multiple choices of explicitly valuated spatiotemporal losses / gains (payoffs)* - human, technical systems, environmental, financial - under pressure & incentives
- Timeline
- User profiles (personae)
  - Scientific (mathematics; physics,…)
  - Engineering
  - Business, political…
Ongoing Tests & Refinements...
Ongoing Tests - Eye Tracking...
Ongoing Tests - Eye Tracking...
Perspectives: STPA for sociotechnical spatiotemporal patterns

Influence Diagram
State: Uncertainty -/= 

Bayesian Net
State: Uncertainty -/= 

Process(es)
State: Uncertainty -/= Execution: OK; KO 

User(s)
State: Uncertainty -/= 

Type
Location

Build/Understand/Share Influence Diagram
Build/Understand/Share Bayesian Net
Select Decision Option on ID or BN
Select Process(es)
Understand Consequences
Reiterate or Validate Decision
Monitor Process(es) Execution
Reiterate…

Environment
State: OK; KO 

System(s)
State: Uncertainty -/= Execution: OK; KO 

Personal Drone
Execution: OK; KO 

Time \([t_X..t_Y]\)
Perspectives: STPA for sociotechnical spatiotemporal patterns

System Dynamic Pattern (ex ante – i.e. Design)
User Behavior Pattern (ex post)

S.M. Magnusson: T-patterns
Perspectives: STPA for sociotechnical spatiotemporal patterns

Sociotechnical Pattern (*ex post*)
Conclusion

• Focus on dynamic uncertainty
• Tackle accidental contexts (past and possible) and integrate *user feedback* in design

• Safety on top of Usability
• Integration of Safety and Usability methods for Design & Evaluation

• Multidirectional training: users – designers – evaluators…
Acknowledgments

• Dr. Nancy Leveson, MIT
• Dr. Margaret Stringfellow, MIT

• Dr. Guy Boy, FIT
• Dr. Semen Köksal, FIT
• Dr. Jeffrey Bradshaw, IHMC
• Dr. Andrew Duchowski, Clemson University
• Dr. Marco Carvalho, FIT

• HF Expert Ludovic Loine, AREVA

• Dr. Sherry Borener, FAA
• Dr. Thierry Bellet, IFSTTAR
• Dr. Gudela Grote, ETH
Discussion...

Questions & Feedback are welcome

Thanks 😊

Lucas STEPHANE
astephane2010@my.fit.edu
(+1)321-549-0207