Managing Technical Project Risks using STPA

Shufeng Chen
System Safety Lead
WMG, University of Warwick, UK

MIT STAMP Workshop
6 June 2024
Background & Challenges

• Sustainable transportation research project.

• Multiple project partners.

• New teams with >70% new members.
From safety team: ‘Hey, I am looking for the new list of data dictionary for BMS, who should I speak to?’

From almost every team: ‘I need to book for an urgent travel, who should I reach out?’

From HW team: ‘Oh shit! When were the new requirements released? I didn’t even know that. I have to change the design again!’

From almost every team: ‘I can’t see the value of my work as I just follow the procedure to complete tasks.’
Motivations

To provide:
- Project stakeholders insights into the project structure

To identify:
- Existing or potential flaws in the project structure

To improve:
- Both efficiency and accuracy of project works and communications

To create:
- A blame-free working culture
Losses

\[ L_1: \text{Loss of human life.} \]
\[ L_2: \text{Loss of capabilities of meeting project scopes.} \]
\[ L_3: \text{Loss of organizational reputation.} \]
\[ L_4: \text{Loss of damage to the property.} \]
Project Team Level Hazards

L1: Loss of human life.
L2: Loss of capabilities of meeting project scopes.
L3: Loss of organizational reputation.
L4: Loss of damage to the property.

H1: Project stakeholder(s) resign(s). [L1, L2]
H2: Project stakeholders lose trackers on the project. [L1]
H3: Project operations does not meet H&S regulations. [L1, L2, L3, L4]
H4: Project budgets were overspent. [L2]
H5: Project data were lost. [L2, L3]
Control Structures

Government
- Grant Funding
- Technical Assistance
- Monitor Progress
- Audit

Funded Stakeholders
- Purchase
- Assure Quality
- Project Updates
- Progress Reports
- Special Needs

Vendor
- Supplied Parts
- Technical Supports
Control Structures
Some ‘Impressive’ UCAs

UCA1:
Safe Team issues outdated **SW Safety Requirements** to the SW Team when the SW team is in a critical phase of releasing the next version of the software.

Leading to:
H2: Project stakeholders lose trackers.
H3: Project operation does not meet H&S regulations.
H4: Project budgets are overspent.
Some ‘Impressive’ UCAs

UCA2: Finance Controller stops managing cost too soon when the project is still running and there are still purchase orders going on.

Leading to: H4: Project budgets are overspent.
Some ‘Impressive’ UCAs

UCA3: HV Workshop Manager provides WS Training too late when new team member has joined and started working in the workshop.

Leading to:
H3: Project operation does not meet H&S regulations.
Some ‘Impressive’ UCAs

UCA4:
General Management provides company visions too late (≥6 months) since new people joined.

Leading to:
H1: Project stakeholder(s) resign(s).
H2: Project stakeholder(s) lose trackers.
Some ‘Impressive’ Loss Scenarios

**UCA1:**
Safe Team issues outdated **SW Safety Requirements** to the SW Team when the SW team is in a critical phase of releasing the next version of the software.

What happened?
- Safety Team was believing that the latest requirements were uploaded (but actually NOT!).
- There was an error message, but it was unintentionally ignored as Safety Team was overloaded with other work.
Should the Safety Team be BLAMED???
What have we learned?

For General Management:
• To emphasize the importance of safety culture.

For Safety Team Leader:
• To have more precise task plans and prioritization.
• To ensure awareness of importance of requirements.

For HR and Safety Team Leader:
• To recruit dedicated requirement manager(s).
What have we learned?

An underperformance team member cannot simply be identified as the cause of a project risk.

Even a project team with fully skilled individuals does not prevent the project risks.

Instead, it could be a symptom of the flawed management.

The way team members interact with each other is the key to a successful project – i.e., teamwork.
What has STPA benefited us?

Improved project efficiency and collaborations:
• Graphical nature of STPA.
• System-thinking process.
• Change management.

Improved working & safety culture:
• Blame-free.
• STPA complements with project tasks.
• Pro-active identification of risks and communications.
Thank you...
Discussion...