Risk Management Using STPA

STAMP Workshop, MIT March 24-25, 2015

Gregory Pope
Is STPA a good tool for Risk Management?

- Typical Risk Management process says what to do, not how to do it.
- Defined in ISO 31000 as the effect of uncertainty on objectives
- There are risks that:
  - we know we have
  - we know we don’t know we have
  - we don’t know we have
  - we don’t know that we don’t have
Typical Risk Management Process

1. Identify the Risk
2. Assess the Risk
3. Develop Responses to the Risk
4. Develop Contingency Plan, Preventive Measures
Identifying Risk

1. Empirical/Experiential
2. Reviewing Lists of Possible Risks
3. Brainstorming
4. STPA (Systemic Theoretic Process Assessment)

This presentation will compare results of these risk identification processes on an actual project.
Assess the Risk

1. Magnitude of Impact
2. Priority
3. Probability of Occurrence

Highest
High
Medium
Low
Lowest
Develop Responses to the Risk

- **Status**
  - Identified
  - Active
  - Closed
  - Unassigned

- **Risk Response**
  - Leave It
  - Monitor
  - Avoid
  - Move
  - Mitigate
  - Unassigned
Develop Contingency Plan, Preventive Measures

- Software Quality Assurance Plan
- Software Configuration Management Plans
- Software Test Plans
- Disaster Recovery Plans
- On Going Risk Management Trackers
The Project: Advanced Simulation and Computing (ASC) at LLNL

- Large and complex project
- Replaces live nuclear testing with multi-physics computational simulations
- One aspect of stockpile stewardship
- Seems like there should be risks.
Threats to ASC Program

- Unpopularity of nuclear weapons
- Lack of funding (not urgent, important)
- Simulation results are not credible
  - Overly ad hoc process, untrusted results
  - Overly regulated process, retard research
  - New hardware disrupts software maturity
Threats to ASC Program

- Lack of qualified staff
  - Computational Physicists
  - Computer Scientists
  - Designers

Teller  Lawrence  Wrong Lawrences
Possible Consequences if ASC Program Eliminated:

- Resume live nuclear testing to maintain stockpile
- Stockpile may not work as expected
- Stockpile may become unsafe
Possible Consequences if ASC Program Eliminated:

Cease to have Nuclear Weapons expertise to:

- safely handle stockpile
- further reduce stockpile
- dispose of nuclear materials
- determine nuclear forensics
- disarm rogue nuclear devices
- prevent nuclear proliferation
- design future weapons if needed
Brainstorming Approach
(Team of Five Project SQE’s)

1. Scalability
2. Complex Make/Build/Test
3. Congressional budget reductions, Sequestration
4. Version availability
5. Documentation obsolescence
6. Oversight competency
7. Product realization
8. Loss of personnel
9. Disaster recovery
10. Part time assignments
11. Maintenance of code
12. Porting to various platforms

Also found with STPA
Also found with list
List Approach

(List of typical s/w developers risks according to Steve McConnell)

1. Creeping Requirements
2. Requirements Gold Plating
3. Released software has low quality
4. Unachievable schedule
5. Unstable tools delay schedule
6. High turnover
7. Friction between developers and customer
8. Unproductive office space

Also found with Brainstorming
Organizational Components As A System

Guide Phrases:
1-Constraints not given
2-Constraint is incorrect
3-Constraint is too late
4-Constraint is “noisy”

Constraints Consist of:
1-Planning
2-Organizing
3-Staffing
4-Directing
5-Controlling

Supervision

Behavioral
1-Experience
2-Communication
3-Education
4-Health
5-Attitude

Reports Consist of:
1-Written
2-Verbal
3-First Hand Observation
4-N Hand Observation

Guide Phrases:
1-Report not given
2-Report is incorrect
3-Report is too late
4-Report is “noisy”

Supervised Activity

Behavioral
1-Experience
2-Communication
3-Education
4-Health
5-Attitude

Supervisor’s Person’s Model

Microsoft Visio Drawing
Box Duality:
Except for the top and bottom boxes, each box can be both a supervisor and supervised (assuming a functional organization)
GR1. Sequestration arbitrary funding cuts 1,1,5
Example Risk Identification OR1

OR1. Increased Functionality / Fidelity R2,1,2
Government Entity Risks

GR1. Sequestration arbitrary funding cuts
GR2. Congressional funds reallocation
GR3. Congress/Executive Delays
GR4. Congress Privatization of Labs
GR5. DOE Software Competency
GR6. DOE Turnover
GR7. NNSA Software Competency
GR8. NNSA Longevity Concerns
Government, Privatizing, Lab Risks

GPLR1. Funding from DOE, Oversight from NNSA
GPLR2. Taxes, Management Fee Increases
GPLR3. Work to Performance Incentives
GPLR4. LLNS Nuclear Weapons Competency
GPLR5. Nuclear Stockpile Managed by Private Firm
Lab Management Risks

LMR1. Top LLNL Management Bechtel Employees
LMR2. Acquisition Merger of LLNS Members
LMR3. Conflicting Priorities Hardware/Software
Development Risks

DR1. Overly Rigid S/W Compliance Standards
DR2. Requirements Unclear
DR3. Changing / Expanding Hardware Platforms
DR5. Lack of Standard Tools
DR6. Rare Skill Mix Required, Understaffing
DR7. Retiring Labor Pool
DR8. Competing with Commercial Market for Talent
DR9. Legacy Code Maintenance/Back Ups
DR10. Externally distributed codes
Operations Risks

OR1. Increased Functionality / Fidelity  
OR2. Input Correctness  
OR3. Quantifying Simulation Uncertainty  
OR4. Validating Results Against Experiments  
OR5. Over Reliance on Simulation S/W  
OR6. Group Think  
OR7. Future Power Resources (Less Memory/Core)  
OR8. S/W Must Change to Accommodate New H/W  
OR9. Retiring Experimenters and Designers  
OR10. Supporting External Users/Platforms
STPA Approach – Government Risks

GR1. Sequestration arbitrary funding cuts 1,1,5
GR2. Congressional fund reallocation 2,1,5
GR3. Congress/Executive Delays 3,1,5
GR4. Congress Privatization of Labs 2,5,5
GR5. DOE Software Competency 2,3,1/3
GR6. DOE Turnover 4,3,5
GR7. NNSA Software Competency 2,3,1/3
GR8. NNSA Longevity Concerns 1,5,5

Also Found with Brainstorm
STPA Approach – Government, Privatizing, Lab Risks, Lab Management Risks

GPLR1. Funding from DOE, Oversight from NNSA 4,5,1
GPLR2. Taxes, Management Fee Increase 2,3,5
GPLR3. Work to Performance Incentives 2,4,2
GPLR4. LLNS Nuclear Weapons Competency 2,4,3
GPLR5. Nuclear Stockpile Managed by Private Firm 2,2,1

LMR1. Top LLNL Management Bechtel Employees 2,2,1
LMR2. Acquisition Merger of LLNS Members 4,4,1
LMR3. Contending Priorities Hardware/Software 2,1,1
STPA Approach – Development Risks

DR1. Overly Rigid S/W Compliance Standards 2,4,1
DR2. Requirements Unclear 4,1,2
DR3. Changing / Expanding Hardware Platforms 2,1,5
DR4. Version Changes O/S, Libraries, Compilers R1,1,2
DR5. Lack of Standard Tools 1,1,5
DR6. Rare Skill Mix Required, Understaffing 1,3,3
DR7. Retiring Labor Pool 1,3,1
DR8. Competing with Commercial Market for Talent 1,3,1
DR9. Legacy Code Maintenance/Back Ups 1,3,1
DR10. Protecting one code distributed externally  R1,1,1

Also Found with Brainstorm
STPA Approach – Operational Risks

OR1. Increased Functionality / Fidelity R2,1,2
OR2. Input Correctness R2,1,2
OR3. Quantifying Simulation Uncertainty R4,1,2
OR4. Validating Results Against Experiments R4,1,2
OR5. Over Reliance on Simulation S/W R2,1,5
OR6. Group Think 4,5,5
OR7. Future Power Resources (Less Memory/Core) R2,3,1
OR8. S/W Must Change to Accommodate New H/W R1,4,1
OR9. Retiring Experimenters and Designers R1,3,2
OR10. Supporting External Users/Platforms 2,5,2

Also Found with Brainstorm
Telephone Game, HCSC Simplified

Telephone Game
Risk = 10

Other Labs
Group Think, Same Board Members

Original Idea of Two Weapon Labs was to get independent opinions
## Mitigation Actions

**OR 7**
- **Scheduling OR7**
  - As the performance gap gets as measured by LIFEPACK increases the number of nodes, blade cards, processors per node, cores per node, threads per core increases.
  - **Active**
  - 2 - High
  - 3 - High
  - 4 - Low
  - Mitigate

**DR 5**
- **DOE and NNSA oversight capability**
  - Tornado in NNSA software SME is creating a SQA knowledge gap between LLNL and NNSA. Auditors interpreting guidance as requirements. Calling non-safety
  - **Active**
  - 2 - High
  - 3 - Medium
  - 4 - Low
  - Monitor

**DR 3**
- **Changing/Expanding Hardware Platforms**
  - Present trend is to reduce memory per processor and add requirement to thread software to take advantage of multi core processors. These transitions software projects have
  - **Active**
  - 2 - High
  - 3 - High
  - 4 - Low
  - Mitigate

**GR 1, GR 2**
- **Concurrent Budget Reductions, Reauthorization**
  - Moore's law in context of large scale exascale supercomputers needs to be included in the current size of the weapons complex and has begun revising funding for stockpile stewardship. Reducing the
  - **Active**
  - 2 - High
  - 3 - High
  - 4 - Low
  - Mitigate

**DR 5**
- **Lack of standard tools**
  - The "one size fits all" nature of the platforms and changing tool standards creates the need for toolset development for the software environment. The platforms and or multi-platform requirements need to be
  - **Active**
  - 2 - High
  - 3 - High
  - 4 - Low
  - Mitigate

**LMR 1, OR 8**
- **Facing Priorities HW/SW**
  - The HPC world tends to trade off in favor of what is best for hardware without as much regard for software impacts. New hardware requiring software changes relate to
  - **Active**
  - 2 - High
  - 3 - High
  - 4 - Low
  - Mitigate

**DR 4**
- **Version changes Q3, Libraries, Compilers, Version Availability**
  - As all the major versions of the latest version of compilers and third party software available from UC. UC tends to have old versions available for use but not the latest. Version
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Unassign

**GR 6, GFR 2**
- **Reliability of LLNL**
  - Major impact was 7 years ago with RIF. Now the impact is high overheads of management and administration fees, cutting into discretionary funds for research projects. High
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**DR 10**
- **Protecting externally distributed code**
  - The new external distributed external to LLNL need to be protected. The code that contains only Version is encrypted, a key is sent separately. Agreements must be
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GR 8**
- **NNSA Longevity Concerns**
  - NNSA independent study suggests eliminating NNSA as autonomous agency and either eliminating it or putting under DOE. NNSA stakeholders meeting under Stephen platforms and or multi-platform requirements need to be
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GR 6**
- **DOE Turner**
  - DOE tends to staff positions with little regard for software quality experience. This lack of experience can cause miscommunication and focus on non-important issues
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GFR 3**
- **Work to Performance Incentives (PEP)**
  - Annual goals set for high-level management would favor efficiency at expense of safety and security.
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GR 5, GR 7**
- **DOE and NNSA oversight capability**
  - Tornado in NNSA software SME is creating a SQA knowledge gap between LLNL and NNSA. Auditors interpreting guidance as requirements. Calling non-safety
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 5**
- **Over reliance on simulation codes**
  - PFM and SCMP suites continually run again simulation codes to determine validation to experimental data. DOE facility is used to back up ASC codes after six months of on-site back up. Off site back up is for two years. Back ups are sent twice a year. Back up confirming test is done once yearly and coordinated with LC. Details in DBF's for each code team. LL
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 10**
- **Support external users, platforms**
  - One of the challenges with scientific research codes is that they may not be used by persons not collocated with developers or with less training in code operation.
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 2**
- **Input correctness**
  - The simulation codes are very dependent on correct input for correct results. Input parameter set is large.
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GR 8**
- **NNSA Independent study suggests eliminating NNSA as autonomous agency and either eliminating it or putting under DOE**
  - DOE has been more reasonable in this interpretation of contractual requirements. This may have a positive impact. Distribute White Paper on Safeness of Safety Software
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 3**
- **Uncertainty Quantification**
  - Code use for answering questions which do not have corresponding experimental data require simulation to provide a measure of uncertainty.
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GR 1**
- **Compliance with commercial marketplace talent**
  - Commercial firms are recruiting lab computer scientists away, such as Nifx, Google, Intel, Cray.
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 1**
- **Overly rigid SW Compliance Standards**
  - had a growing external customer base which increases platforms to be supported. New required physics features added, due to inputs from simulation
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 8**
- **Proactive Safety Software Development**
  - Find the key can be date bound. Expose the use of nifty LM tool the codebase on-demand. Use the MAC address. This assures the code stays on one platform.
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 9**
- **Legacy code maintenance, Back up documentation maintenance**
  - How to maintain older codes which may have had author retire. If a natural disaster strikes will the codes and documentation be destroyed? Documentation for ASC codes consists of over 45 documents that require periodic
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**GR 5**
- **Requirements Unclear**
  - Requirements for developing simulators informed by different scales requires more resources than currently available. Requirements contain unanswerable front and
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate

**OR 7**
- **Simulation Uncertainty**
  - As the performance gap gets as measured by LIFEPACK increases the number of nodes, blade cards, processors per node, cores per node, threads per core increases.
  - **Active**
  - 2 - High
  - 3 - High
  - 4 - Low
  - Mitigate

**DR 7**
- **Mitigate**
  - The new machines actually seem to slow the codes down or require wasting resources. Next gen HPC moving to heterogeneous platforms and stacked memory which should help with this issue. However it will create new challenges in converting codes to take
  - **Active**
  - 3 - Medium
  - 4 - Low
  - Mitigate
Comparison of Approaches: Venn Diagram

- List
- Brainstorming
- STPA

- List 2 Risks
- Brainstorm 12 Risks
- STPA 36 Risks
Identifying risks:

- that we know we have - Brainstorming
- that we know we don’t have - Lists
- that we don’t know we have – STPA & Brainstorm
- that we don’t know that we don’t have - STPA
STPA Summary

- Found more than 3x risks than simple list or brainstorming techniques
- Found a wider range of risks (both Vertical and Horizontal)
- Finds risks “outside the box”
- Finds risks outside of my sphere of influence
- STPA can easily be combined with list, brainstorming, and empirical/experiential techniques.
Next Steps

- Automate STPA risk management process to exhaust all combinations to see if it yields useful risks.

Work Constraints Types 5
  Guide 4
  Traits 6

Reporting Types 4
  Guide 4
  Traits 6

Combinations = 11,520

Times # of Boxes-2  18

Total Risk Comb. = 207,360

How to tell a risk from a non-risk w/o human in the loop
STPA Final Thought

STPA provides an excellent tool to call attention to shortcomings in a rational and less judgmental way.

Download copy of presentation at: www.silverbuckshot.net/STPA