Risk Management Using STPA

STAMP Workshop, MIT March 24-25, 2015

Gregory Pope

Lawrence Livermore National Laboratory

LLNL-PRES-668705

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

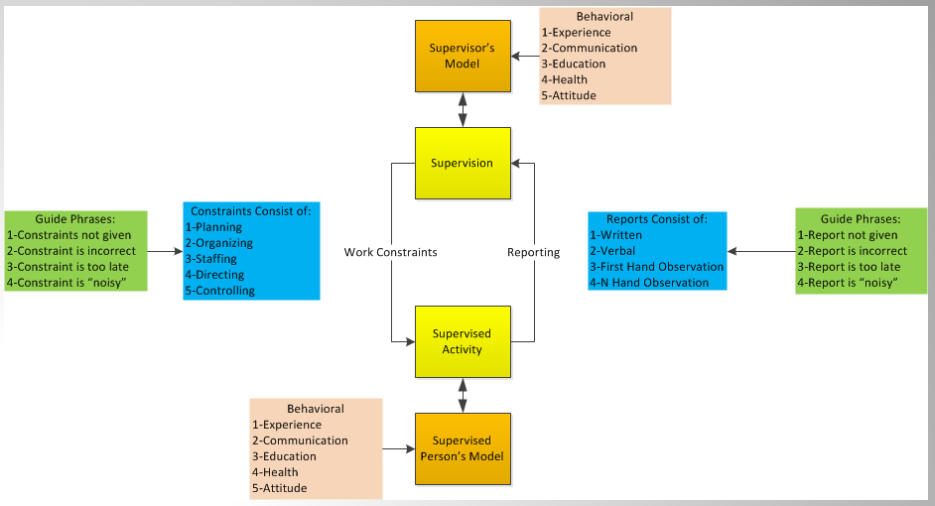
Is STPA a good tool for Risk Management ?

- 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 Reponses 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

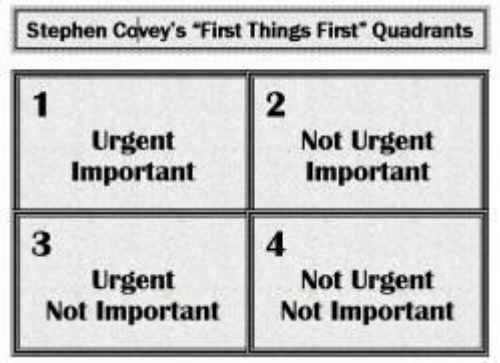
The Project: Advanced Simulation and Computing (ASC) at LLNL

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

Not These

Threats to ASC Program

- Unpopularity of nuclear weapons
- Lack of funding (not urgent, important)



Stephen Covey's "First Things First" Quadrants	
1 Urgent Important	2 Not Urgent Important
3 Urgent Not Important	4 Not Urgent Not 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

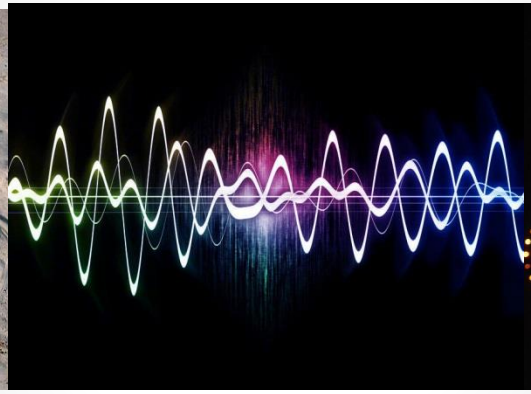
Teller

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

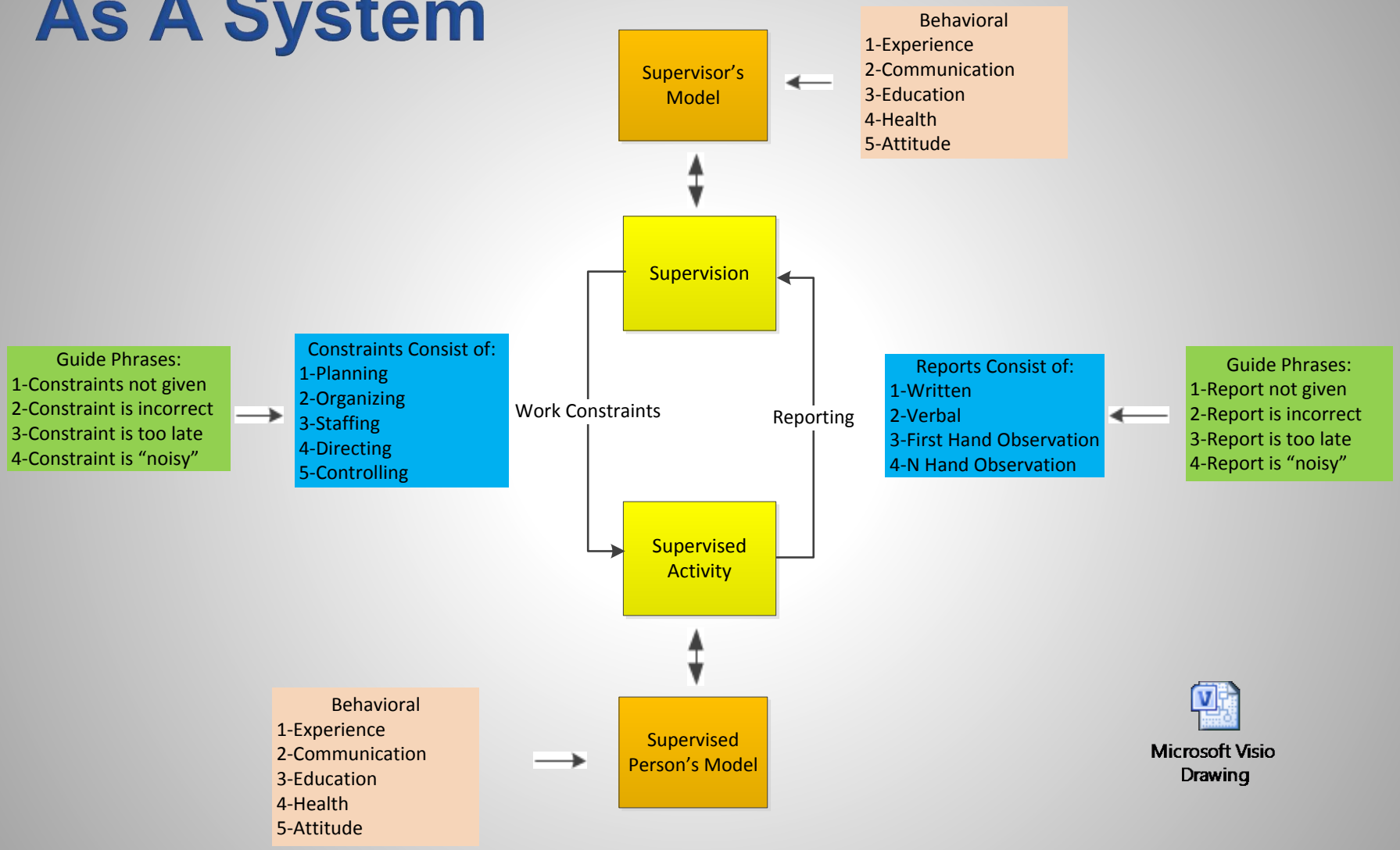
List Approach

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

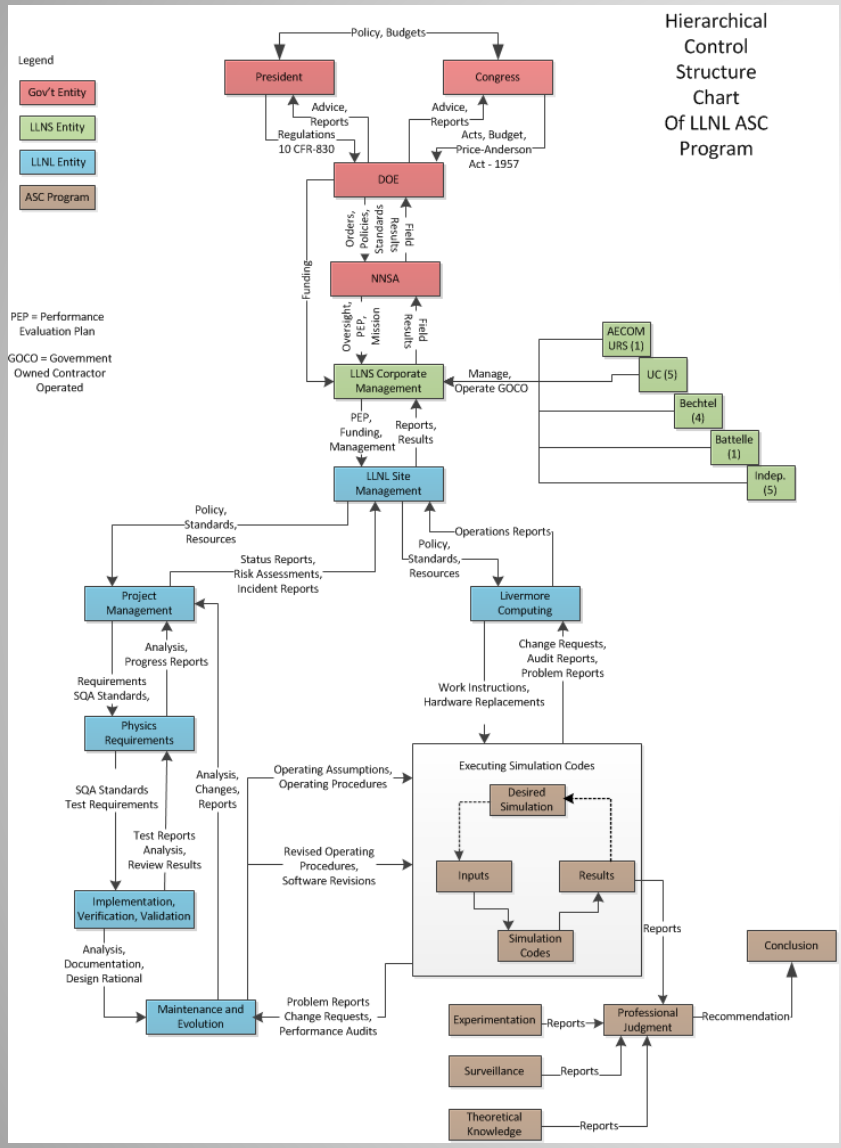
1. ~~Creeping Requirements~~
2. ~~Requirements Gold Plating~~
3. ~~Released software has low quality~~
4. ~~Unachievable schedule~~
5. ~~Unstable tools delay schedule~~
6. High turnover
7. Friction between developers and customer
8. ~~Unproductive office space~~

Also found with Brainstorming

Organizational Components As A System



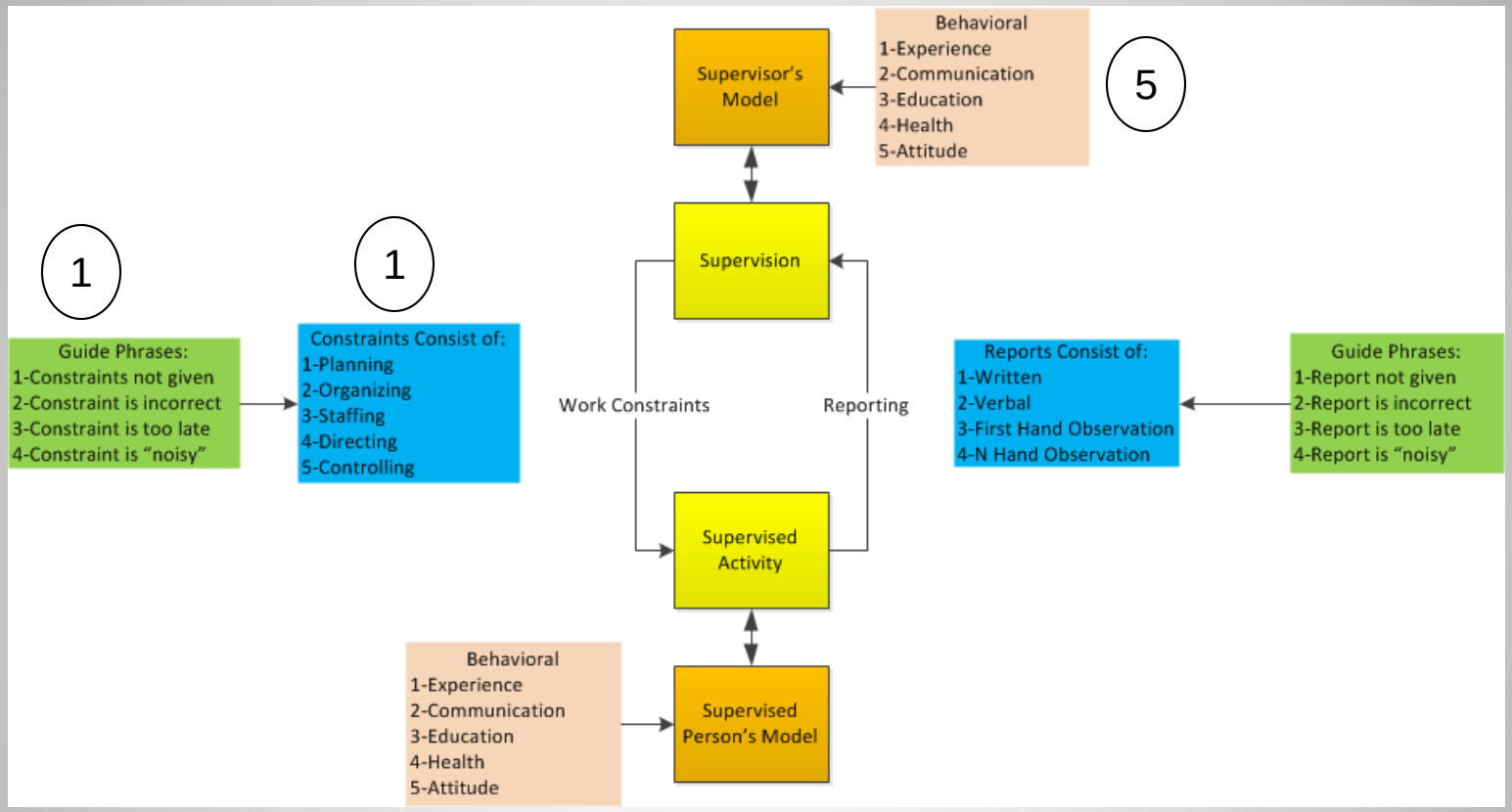
Hierarchical Control Structure Chart



Box Duality:
Except for the top and bottom boxes, each box can be both a supervisor and supervised (assuming a functional organization)

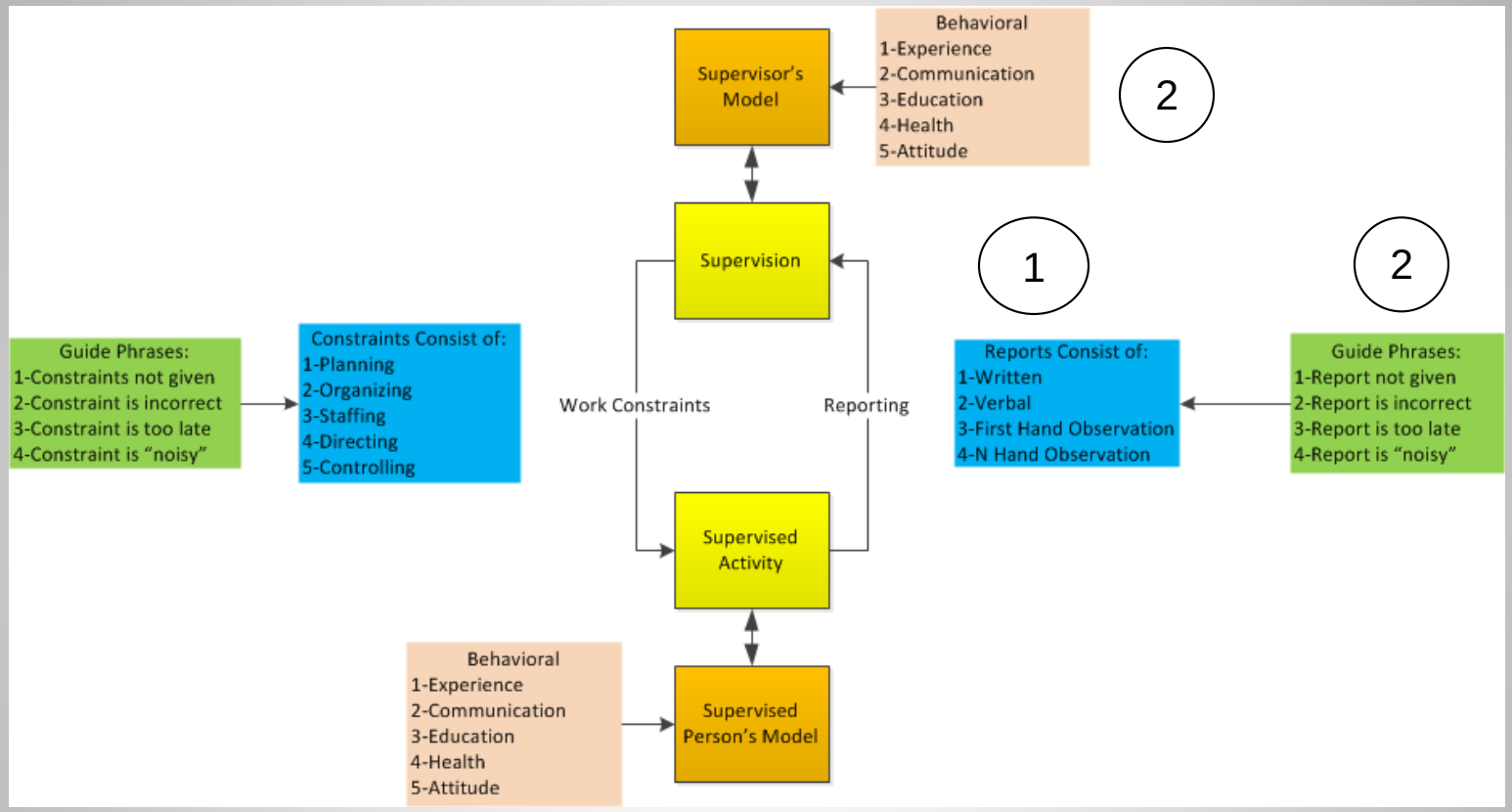
Microsoft Visio Drawing

Example Risk Identification GR1



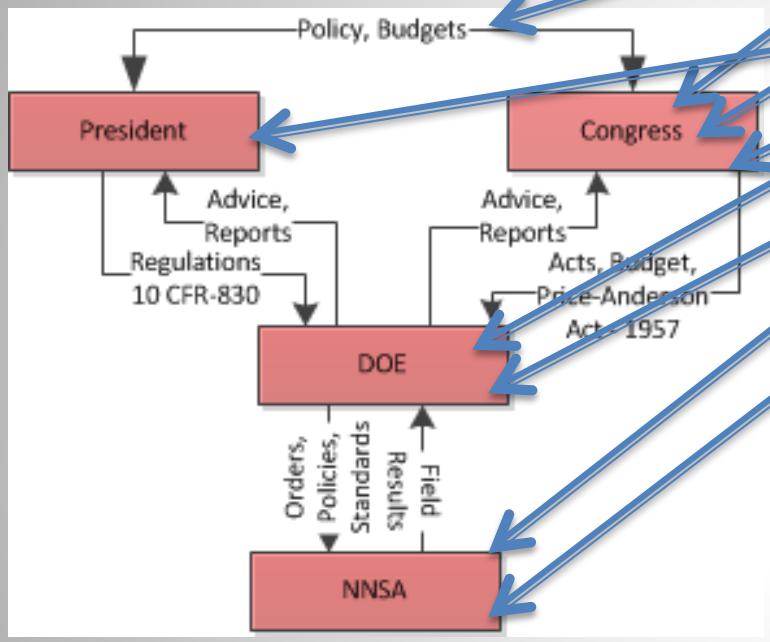
GR1. Sequestration arbitrary funding cuts 1,1,5

Example Risk Identification OR1



OR1. Increased Functionality / Fidelity R2,1,2

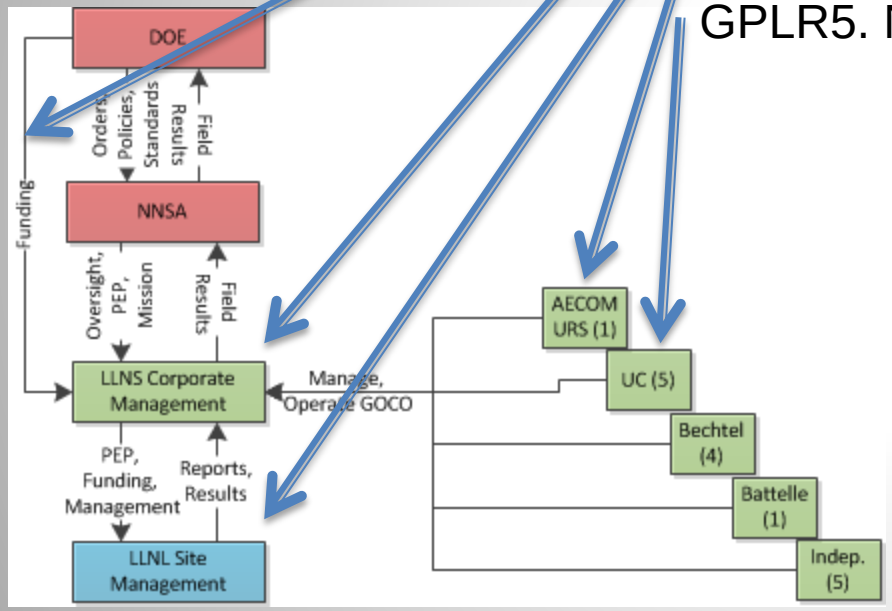
Government Entity Risks



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

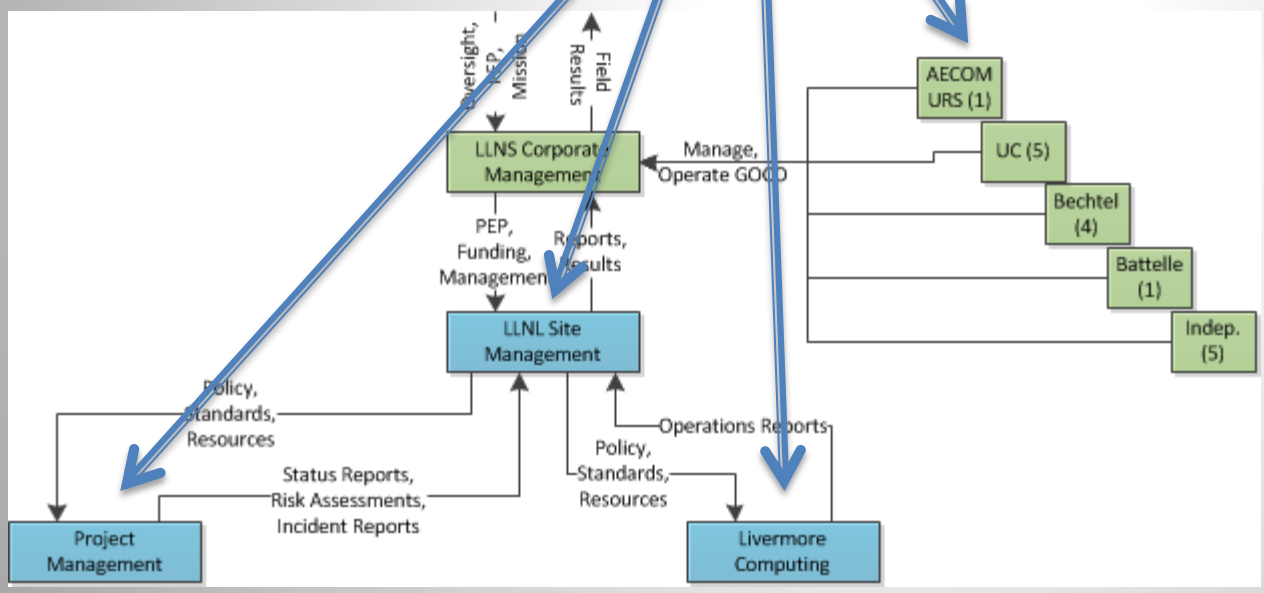
Government, Privatizing, Lab Risks

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

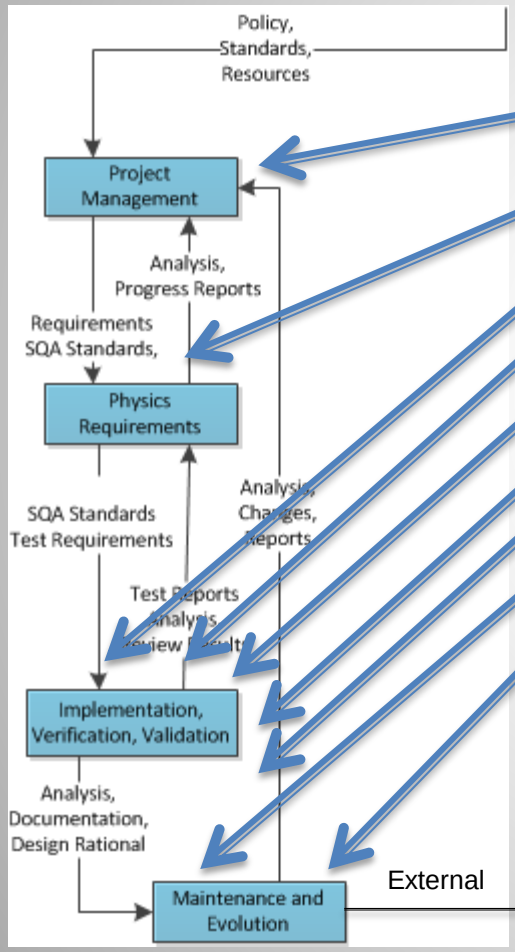


Lab Management Risks

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



Development Risks

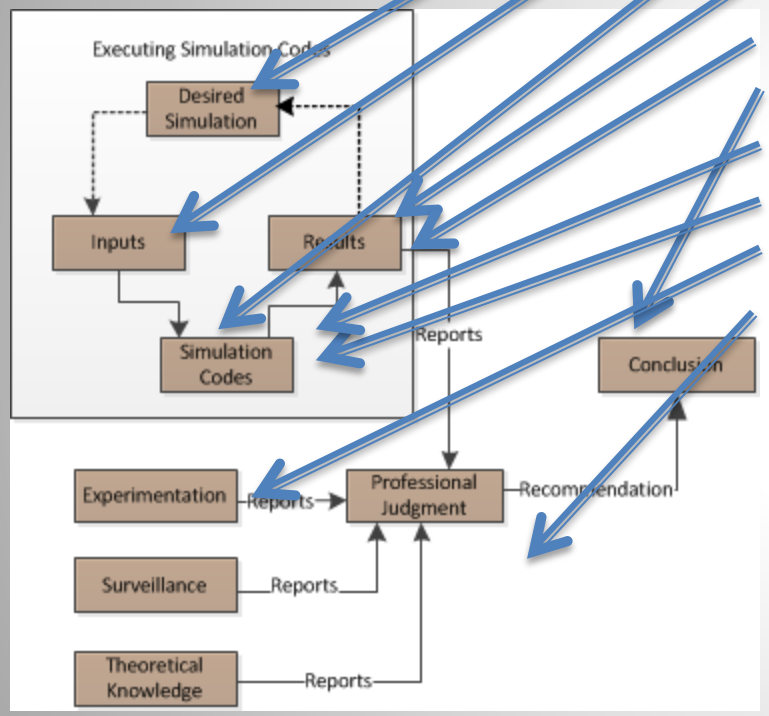


DR1. Overly Rigid S/W Compliance Standards
DR2. Requirements Unclear
DR3. Changing / Expanding Hardware Platforms
DR4. Version Changes: O/S, Libraries, Compilers
DR5. Lack of Standard Tools
DR6. Rare Skill Mix Required, Understaffing
DR7. Retiring Labor Pool
DR8. Competing with Commercial Market for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

External

DOD and Beltway Bandits

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

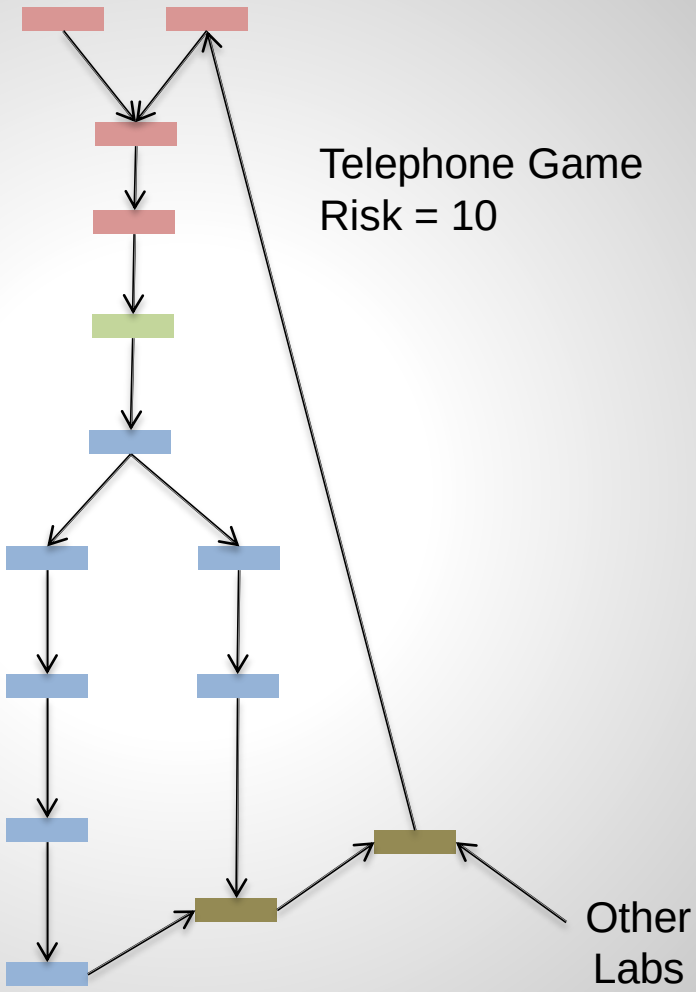
Also Found with Brainstorm

STPA Approach – Operational Risks

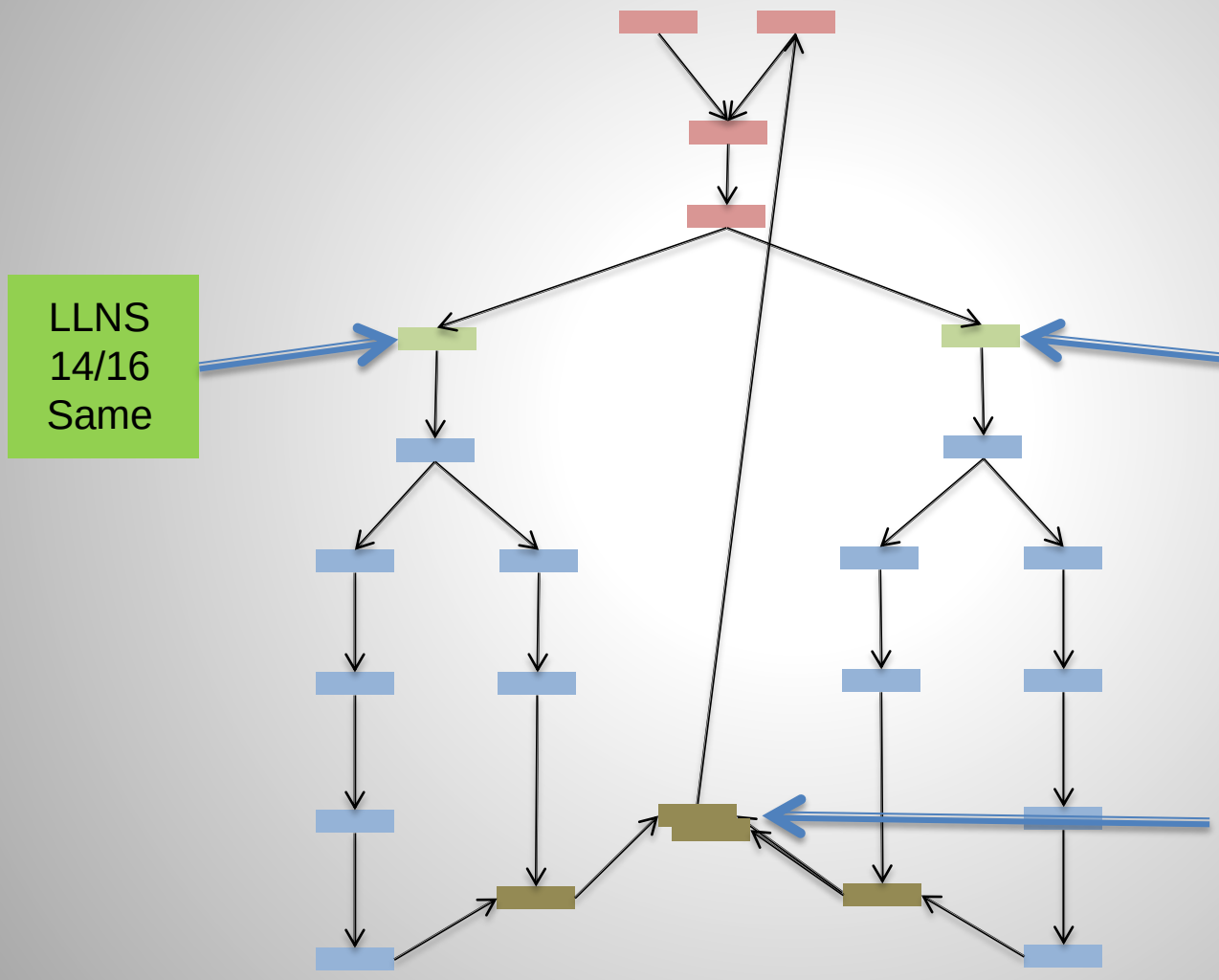
OR1. Increased Functionality / Fidelity R2,1,2
OR2. Input Correctness R2,1,2
OR3. Quantifying Simulation Uncertainty R4,1,2
OR4. Validating Results Against Experiments R4,1,2
OR5. Over Reliance on Simulation S/W R2,1,5
OR6. Group Think 4,5,5
OR7. Future Power Resources (Less Memory/Core) R2,3,1
OR8. 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



Group Think, Same Board Members



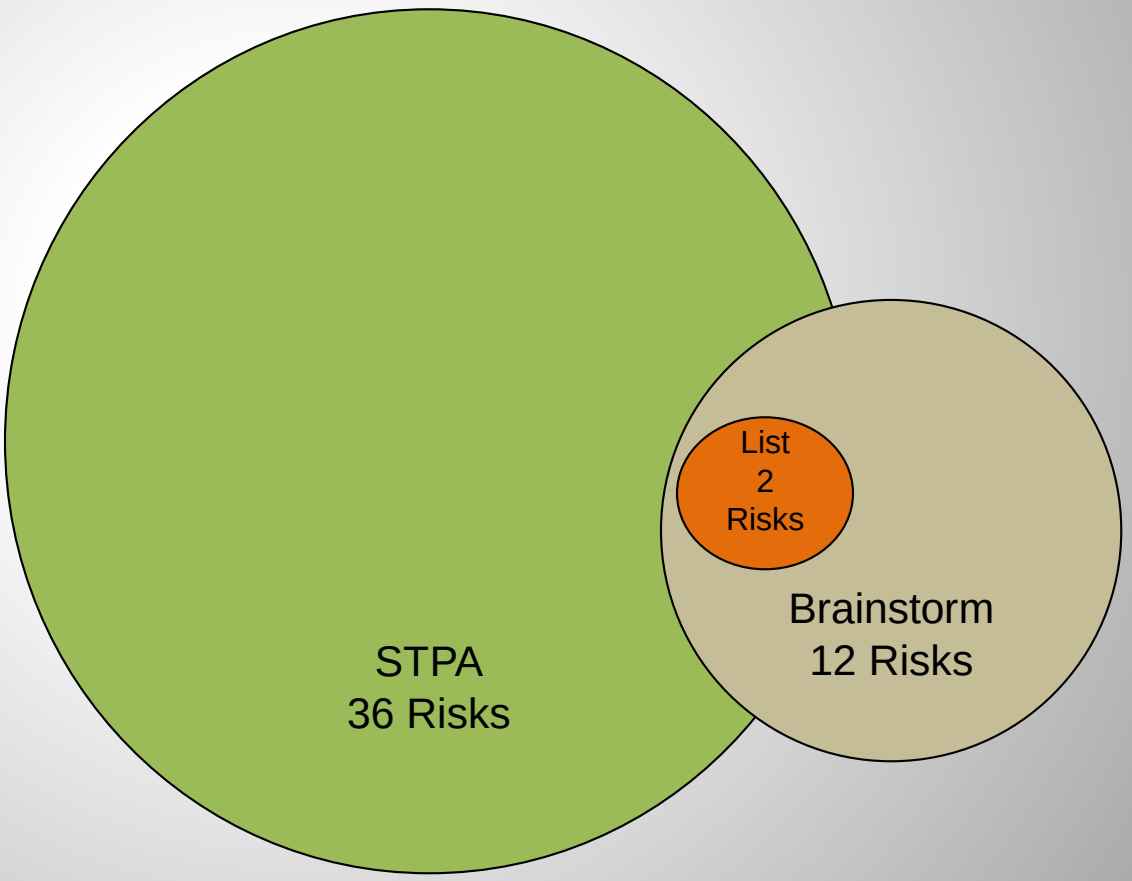
Original Idea of Two Weapon Labs was to get independent opinions

Tracking Risks

	Risk	Description	Status	Magnitude of Impact	Priority	Prob of Occurrence	Risk Reponses	Mitigation Actions
OR 7	Scalability OR7	As the performance goes up as measured by LINPACK benchmark the number of nodes (blade cards), processors per node, cores per node, threads per core increases	Active	2 - High	1 - Highest	1 - Highest	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
GR 5, GR 7	DOE and NNSA oversight capability	Turnover in NNSA software SME's is creating a SQA knowledge gap between LLNL and NNSA. Auditors interpreting guidance as requirements. Calling non-safety	Active	2 - High	3 - Medium	3 - Medium	Monitor	Educate and create virtual auditing capabilities through automation. Moved documents to be confluence wiki based as well as in WCIDMS. Lend support to ISQAP efforts as required, such as Ellen and Natalia working on templates. The templates will
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 - Medium	2- High	Mitigate	Accomplish software impact analysis as part of the system design tradeoffs for future platforms. Fund next gen team to proactively determine tool sets and development environments before new hardware gets to the floor. Look for porting tools to
GR 1, GR 2	Congressional Budget Reductions, Sequestration	Recent actions in congress have questioned the need for the current size of the weapons complex and have began reducing funding for stockpile stewardship. Reducing the	Active	2 - High	2- High	3 - Medium	Mitigate	Size of SQE group reduced by two slots. Skill mix moved toward developer and SQA skills to reflect embedded nature of work. (Some development and some SQE). More part time assignments. Increase institutionalization of SQA role among developers
DR 5	Lack of standard tools	The "one off" nature of the platforms and changing of platforms and/or multi-platform requirements creates the need for complex build and make scripts. The platforms are	Active	2 - High	2- High	2- High	Mitigate	Bill working on platform diversity of Ale3d. ATS stakeholders meeting under Stephanie to gather use cases and determine common set of reporting and comparing libraries. Tammy using pyunit for UQ pipeline. Jenkins tool added to automate building. Test
LMR 3, OR 8	Contending 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 retards the	Active	2 - High	2- High	2- High	Mitigate	Develop and support efforts to proactively prepare for changes to platforms moving forward. Use the software reliability and quality arguments. Look for new tools to automate as much code porting as possible.
DR 4	Version changes O/S, Libraries, Compilers, Version Availability	Not all versions or the latest version of compilers and third party software available from LC. LC tends to have older versions available for use but not the latest. Version	Active	3 - Medium	3 - Medium	2 - High	Unassigned	Work with LC to make latest versions of compilers and libraries available. Prioritize need. Before using latest features in design phase assure that LC supports them. List unsupported features for developers. Use of cmake templates to standardize and
DR 6	Rare skill mix, understaffing	Harder and harder to find US citizens with advanced degrees in scientific areas.	Active	3 - Medium	3 - Medium	2 - High	Mitigate	Using summer intern programs to identify candidates and find talent before graduating. Right sizing estimates a few years ago helped somewhat from further reductions. However next gen funding has eaten into V&V budget. Need to push for
GR 4, GPLR 2	Privatization 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	3 - Medium	2 - High	Mitigate	Reduced group size and part time assignments.
OR 1	Increased Functionality / Fidelity	has caused a growing external customer base which increases platforms to be supported. New required physics features added, desire to inform simulation from	Active	3 - Medium	3 - Medium	2 - High	Mitigate	Commodity hardware, use standard language features, standard operating systems, standard tools. Create customer liaison position. Examine external companies to take on distribution and support. Expand platform testing.
DR 1	Overly Ridged S/W Compliance Standards	Imposing a heavy weight development process with excessive documentation requirements would discourage researchers from wanting to work on the project.	Active	3 - Medium	3 - Medium	3 - Medium	Monitor	Process includes review by domain experts before use. Separate V&V group and SQA group oversee software process and V&V of results. UQ Pipeline software available to measure simulation uncertainty. Distribute white paper to push back on safety label
DR 10	Protecting externally distributed code.	One code distributed externally to DoD and subcontractors for the DoD. The DVD that contains only binaries is encrypted, a key is sent separately. Agreements must be	Identified	3 - Medium	3 - Medium	3 - Medium	Mitigate	See if the key can be date bounded. Explore the use of Flex LM to lock the code to a platform suing the MAC address. This assures the code stays on one platform.
DR 8	Competing with commercial marketplace for talent	Commercial firms are recruiting lab computer scientists away, such as Net Flix, Google, Intel, Cray.	Active	3 - Medium	3 - Medium	3 - Medium	Mitigate	Increased emphasis on salary surveys of market to be competitive. Increased use of stay bonuses. Continue to find ways to cut through bureaucracy. Use stay bonuses.
DR 9	Legacy code maintenance, Back Ups, docuemtnation maintenance.	How to maintain older codes who may have had author retire. If a natural disaster strikes will the codes and documentation by distroyed? Documentation for ASC	Active	3 - Medium	3 - Medium	3 - Medium	Mitigate	Off site facilities are 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 DRPs for each code team. L2
OR 10	Support external users, platforms	One of the challenges with scientific research codes is that they may need to be used by persons not collocated with developers or with less training in code operation.	Active	3 - Medium	3 - Medium	3 - Medium	Move	Static Analysis run on all codes, issues triaged, most serious fixed. SQE have been involved doing easier fixes, retest, and check in. DBC added to Ale3d code by Natalia on issues found by Klocwork static analyzer tool. Run static analysis periodically until it
OR 2	Input Correctness	The simulation codes are very dependent on correct inputs for correct results. Input parameter set is large.	Active	3 - Medium	3 - Medium	3 - Medium	Leave It	Input decks are stored in CM tool. New decks are created from copies of previous decks. Heavy reliance on skilled users to determine correctness of results. Future functionality to include more input range checking in simulation codes.
GR 8	NNSA Longevity Concerns	NNSA independent study suggests eliminating NNSA as autonomous agency and either eliminating it or putting under DOE	Identified	3 - Medium	4 - Low	3 - Medium	Monitor	DOE has been more reasonable in there interpretation of contractual requirements. This may have a positive impact. Distribute White Paper on Safeness of Safety Software.
GR 6	DOE Turnover	DOE tends to staff positions with little regard for software quality experience. This lack of expereince can cause miscommunication and focus on non-important issues.	Active	3 - Medium	4 - Low	4 - Low	Mitigate	Continue to educate DOE staff in the principles of software development and quality.
GPLR 3	Work to Performance Incentives (PEPs)	Annual goals set for high level management could favor efficiency at expense of safety and security.	Active	3 - Medium	4 - Low	2- High	Mitigate	Advise upper management of conflict of safety or security with a PEP. Continue to work for PEP bonuses to direct funded employees who do the work..
OR 5	Over Reliance on simulation codes	PMP and SCMP suites continually run again simulation codes to determine validation to experimental data.	Active	3 - Medium	4 - Low	2- High	Monitor	DRP added for important data (PMP and SCMP) . Continual reminder that codes need professional judgement to interpret results.
DR 2	Requirements Unclear	Requirements for developing simulations informed by different scales requires more resources than currently available. Requirements contain unknowns up front and	Active	3 - Medium	2- High	2- High	Mitigate	Issue tracker use for requirement tracking. Close relationship between designers and users. Agile process allowing experimentation and changes. Continuous integration or nightly testing for earliest detection of errors.
OR 3	Uncertainty Quantification	Code use for answering questions which do not have corresponding experiemntal data require simulation to provide a measure of uncertainlty.	Active	3 - Medium	2- High	2- High	Mitigate	SQE staff deployed to assist in improving UQ Pipeline code and documention for users of the code. Also emphasiss on reporting tools to allow easier interpretation of results.

Comparison of Approaches: Venn Diagram

- List
- Brainstorming
- STPA



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