### **Risk Management Using STPA**

### STAMP Workshop, MIT March 24-25, 2015

**Gregory Pope** 

### Lawrence Livermore National Laboratory



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 <u>ISO 31000</u> 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





- 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)

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



## 12. Porting to various platforms

Lawrence Livermore National Laboratory

### **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**

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

Also found with Brainstorming

- 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





### **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)



### **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**



### **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

### **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**



### **Tracking Risks**

Image: state in the s									Mitigation Actions
Image: books of the stand					Magnitude of		Prob of	Risk	
Barbar         Alter offensorgers is enserved y UMAX.         Fragmental Sector		Risk	Description	Status	Impact	Priority	Occurrence	Reponses	
Orient Construct         Performance for the multiple orienge 300 model (see 1) and orienge 30			As the performance goes up as measured by LINPACK						The new machines actually seem to slow the codes down or require wasting resources.
International biology         Decision biology and biology	OR 7		benchmark the number of nodes (blade cards), processors						Next gen HPC moving to heterogeneous platforms and stacked memory which should
Bit     Bit <td>-</td> <td>Scalability OR7</td> <td>per node, cores per node, threads per core increases</td> <td>Active</td> <td>2 - High</td> <td>1 - Highest</td> <td>1 - Highest</td> <td>Mitigate</td> <td>neip with this issue. However it will create new challenges in converting codes to take</td>	-	Scalability OR7	per node, cores per node, threads per core increases	Active	2 - High	1 - Highest	1 - Highest	Mitigate	neip with this issue. However it will create new challenges in converting codes to take
Photom     Instruction     Instruction     And     And     And     And     And     And       Particle     Second	GR 5,	DOF and MMCA averaging	I urnover in NNSA Software SME's is creating a SQA						Educate and create virtual auditing capabilities through automation. Moved
Sector         Sector<	GR 7	DOE and NNSA oversight	interpreting guidance as requirements. Calling non-safety	Active	2 - High	2 Medium	2 - Medium	Monitor	efforts as required, such as Filen and Natalia working on templates. The templates will
Diaz         Diaz <thdiaz< th="">         Diaz         Diaz         <thd< td=""><td>-</td><td>capability</td><td>Dragant trand is to reduce mamony par processor and add</td><td>Active</td><td>2 - High</td><td>5- Weuluill</td><td>5- Weululli</td><td>WOITTO</td><td>Accomplish software impact analysis as part of the system design tradeoffs for future</td></thd<></thdiaz<>	-	capability	Dragant trand is to reduce mamony par processor and add	Active	2 - High	5- Weuluill	5- Weululli	WOITTO	Accomplish software impact analysis as part of the system design tradeoffs for future
Image         Construction	DR 3	Changing/Expanding Hardware	requirement to thread software to take advantage of multi						platforms. Fund next gen team to proactively determine tool sets and development
Beside in the sector is and the sector is aff the sector is a		Platforms	core processors. These transitions software projects have	Active	2 - High	3 - Medium	2- High	Mitigate	environments before new hardware gets to the floor. Look for porting tools to
Bit         Bit <td></td> <td></td> <td>Recent actions in congress have questioned the need for</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Size of SQE group reduced by two slots. Skill mix moved toward developer and SQA</td>			Recent actions in congress have questioned the need for						Size of SQE group reduced by two slots. Skill mix moved toward developer and SQA
Marketing         Marketing <t< td=""><td rowspan="2">GR 1, GR 2</td><td>Congressional Budget</td><td>the current size of the weapons complex and have began</td><td></td><td></td><td></td><td></td><td></td><td>skills to reflect embedded nature of work. (Some development and some SQE). More</td></t<>	GR 1, GR 2	Congressional Budget	the current size of the weapons complex and have began						skills to reflect embedded nature of work. (Some development and some SQE). More
Bar         Bar <td>Reductions, Sequestration</td> <td>reducing funding for stockpile stewardship. Reducing the</td> <td>Active</td> <td>2 - High</td> <td>2- High</td> <td>3 - Medium</td> <td>Mitigate</td> <td>part time assignments. Increase institutionalization of SQA role among developers</td>		Reductions, Sequestration	reducing funding for stockpile stewardship. Reducing the	Active	2 - High	2- High	3 - Medium	Mitigate	part time assignments. Increase institutionalization of SQA role among developers
Bit         Description         Descripion <thdescription< th=""> <thdesc< td=""><td></td><td></td><td>The "one off" nature of the platforms and changing of</td><td></td><td></td><td></td><td></td><td></td><td>Bill working on platform diversity of Ale3d. ATS stakeholders meeting under Stephanie</td></thdesc<></thdescription<>			The "one off" nature of the platforms and changing of						Bill working on platform diversity of Ale3d. ATS stakeholders meeting under Stephanie
$ \begin{array}{                                    $	DR 5		platforms and/or multi-platform requirements creates the						to gather use cases and determine common set of reporting and comparing libraries.
Max and marks where many structures is larged in it under a larged for the last version of marks where marked in the last version of marked where were marked in the last version of marked where were were marked in the last version of marked where were were were were were were wer		Lack of standard tools	need for complex build and make scripts. The platforms are	Active	2 - High	2- High	2- High	Mitigate	Tammy using pyunit for UQ pipeline. Jenkins tool added to automate building. Test
Desc         Control (LP)         Process (LP)         Markey manufactor (LP	LMR 3,		hardware without as much regard for software impacts						forward. Use the software reliability and quality arguments. Look for new tools to
Image: construction of Linking and Linking	OR 8	Contending Priorities HW/SW	New hardware requiring software changes retards the	Activo	2 - High	2. High	2- High	Mitigate	automate as much code porting as possible
Display         Even change (3), Lume, larger)         Field of the second particle (3), Lume, larger)         Accord (3), Lume, larger)		contending ritorities rive/sw	Not all versions or the latest version of compilers and third	Active	2 - 11gn	2- 11g1	2- High	wittgate	Work with I C to make latest versions of compilers and libraries available. Prioritize
Image: Second	DR 4	Version changes O/S. Libraries.	party software available from LC. LC tends to have older						need. Before using latest features in design phase assure that LC supports them. List
Bits         Huder and huder to find 15 citizen with advanced gene sin scientific analysis.         Active         3. Medium         2. segh         Multigate matching         Huder and huder before graduating has each server as perinding has each server and citizen as the server as perinding has each server and citizen as the server as perinding has each server as perinding has each server and citizen as the server as perinding has each as provide an appartment and administration fees in the server as perinding has each as provide and perinding has each as provide and perinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding systems, tanded to bits, Create upperinding has each as provide and perinding has each as the system of the system as part to bits, the system to bits and advances and as provide and perindic has each as provide and perindic has each as the system of the system as as as the system one perindic distributed on the system as as the system one perindic has each as the system one perindic has each as a peri		Compilers, Version Availability	versions available for use but not the latest. Version	Active	3 - Medium	3 - Medium	2 - High	Unassigned	unsupported features for developers. Use of cmake templates to standardize and
Bes         Bes <td></td> <td></td> <td>Harder and harder to find US citizens with advanced</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Using summer intern programs to identify candidates and find talent before</td>			Harder and harder to find US citizens with advanced						Using summer intern programs to identify candidates and find talent before
Beta Ball mix understaffer         Control         Autor         S. Medium         S. Medium         Magene         Performance         Performance           PRASE         Provertation of LLN         Optimized wars 7 years ago with BF. Now the impacts         No.         S. Medium         S. Medium         Performance           Provertation of LLN         Optimized ago monits esterning for service registerning for se	DR 6		degrees in scientific areas.						graduating. Right sizing estimates a few years ago helped somewhat from further
General problem         Major impact way 7 years ago with BF. Now the impact is construction for S (weith a second provide properties of maximum function for second projects may second projects. Here required for the second provide projects may second provide projects. Here required for the second provide projects may second provide projects. Here required for the second provide projects may second provide projects. Here required for the second provide projects may second provide projects. Here required for the second provide projects may second provide provid		Rare skill mix, understaffing		Active	3 - Medium	3 - Medium	2 - High	Mitigate	reductions. However next gen funding has eaten into V&V budget. Need to push for
Markate of management adaministration fees         Markate of management adaministration fees         Markate         Ander	GR /		Major impact was 7 years ago with RIF. Now the impact is						Reduced group size and part time assignments.
Production of LNL         Catiling info discretionary funds for research project. Hyper required         Andrew         3. Medium         3. Medium         2. High         Migger         Commodity hardware, use standard language features, standard operating systems, standard tools. Create customer lialoon position. Examine actemate companies to take and the system action mathematican from Andrew           011         increases functionality / increases functionality increases functin anonon distremationa	GPLR 2		high overheads of management and administration fees						
Bit Increase functionality / increase jationary is accurate agrowing external contraptise with increase jationary is supported. New required privates, statistical operating systems, statistical operatind systems, statistical operating systems, statistical	OF ENTE	Privatization of LLNL	cutting into discretionary funds for research projects. High	Active	3 - Medium	3 - Medium	2 - High	Mitigate	
Diff       Increase of Functionality       Increase of Functionality </td <td></td> <td></td> <td>has caused a growing external customer base which</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Commodity hardware, use standard language features, standard operating systems,</td>			has caused a growing external customer base which						Commodity hardware, use standard language features, standard operating systems,
Incluity       Unprise failures added, pairing to work primary process with memory barry work of the primary primany primany primary primary primany primary primary p	OR 1	Increased Functionality /	increases platforms to be supported. New required				a		standard tools. Create customer liaison position. Examine external companies to take
Derly Ridged S/W Compliance       mipboing Antery Weight Order (Single Single Sin		Fidelity	physics features added, desire to inform simulation from	Active	3 - Medium	3 - Medium	2 - High	Mitigate	Discrete includes review by demain expects before use. Separate V/8V group and SOA
Image: a yriny houses of yriny houses of yriny houses and yring houses and yring houses and yring houses. Simulation uncertainty. Distribute white ageer to push back on sfer yithele ageer hybrid house in the yring house and yring houses. Simulation uncertainty. Distribute white ageer to push back on sfer yithele age of push back o	DR 1	Overly Ridged 5 /M Compliance	excessive documentation requirements would discourage						group oversee software process and V&V of results. LIO Pineline software available to
Dress         One code distributed extranily to Dia and subcontractors for the DO. The DO That contains which and ess encrypted, a key is sent separately. Agreements must be distributed excel.         Sentering and comparison with sentering and comparison which and ess encrypted, a key is sent separately. Agreements must be distributed excel.         Sentering and comparison with and ess encrypted, a key is sent separately. Agreements must be distributed excells         Sentering and comparison with and ess encrypted, a key is sent separately. Agreements must be distributed excells         Sentering and comparison with and ess encrypted, a key is sent separately. Agreements must be distributed excells         Sentering and comparison with agree excelling is a comparison on epistrom.           DR 8         Competing with commercial marketplace fortalent marketplace f	DKI	Standards	researchers from wanting to work on the project.	Active	3 - Medium	3 - Medium	3 - Medium	Monitor	measure simulation uncertainty. Distribute white paper to push back on safety label
BA1D         Protecting external and explosed is distributed code.         Protecting external is distributed code.         Protectis distributed code.         Protecting external is distri		Standards	One code distributed externally to DoD and subcontractors	rictive	5 Mcdidin	5 Medium	5 Mcalan	monitor	See if the key can be date bounded. Explore the use of Flex LM to lock the code to a
Identified code       Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary survey of market to be competitive. Increased enphasis on salary surve	DR 10	Protecting externally	for the DoD. The DVD that contains only binaries is						platform suing the MAC address. This assures the code stays on one platform.
DR8         Commercial frms are recruiting lab computer scientists marketplace for talent marketplace for talent marketplace for talent         Increased emphasis on salary surveys of market to be competitive. Increased use of stay bouses. Continue to find ways to ut through bureaucacy. Use stay bouses.           DR 8         Competing with commercial marketplace for talent         Not to maintain older codes who may have had author retire. If a natural disaster strikes will be codes and documentation by distruct?         Active         3 - Medium         Mitigate         Off site facilities are used to back up ASC codes after six months of on-site back up.           0R 10         Support external users, platforms         One of the hallenges with scientific research code is that they may need to be used by persons not collocated with developers ow white straining in code operation.         Active         3 - Medium         3 - Medium         Mitigate           0R 2         One of the hallenges with scientific research code is that they may need to be used by persons not collocated with developers ow white straining in code operation.         Active         3 - Medium         3 - Medium         3 - Medium         Mitigate           0R 2         The simulation codes are very dependent not on suster banks uses tall canks yre tools. Instatic analysis tools. Instatica analysis tools. In		distributed code.	encrypted, a key is sent separately. Agreements must be	Identified	3 - Medium	3 - Medium	3 - Medium	Mitigate	
BR8       Competing with commercial       way, such as Net Flix, Google, Intel, Cray.       Active       3 - Medium       3 - Medium       Mitigate         Image: Competing with commercial mathematics for communication and public stray for the strain and stars strikes will be codes and the strain and stars strikes will be codes and the strain and stars strikes will be codes and the strain and strain and stars strikes will be codes and the strain and stars strikes will be codes and the strain and the stars strike strain and the stars strikes will be codes and the strain and the stars strike strain and the stars strike strain and the strain and strain a			Commercial firms are recruiting lab computer scientists						Increased emphasis on salary surveys of market to be competitive. Increased use of
marketplace for talent         Active         3 - Medium         3 - Medium         Mitigate           Biggory code maintenance, Box Ups, docuemtation         How to maintain older codes who may have had author ups, docuemtation by distryed? Documentation for ASC documentation active active active active active active active active active platforms         Antelian         Antelian         Antelian         Mitigate           OR 2         One of the challenges with icess training in Code operation. Input Correct results. Input parameter set is large. Autonomous agency and either eliminating NNSA as autonomous agency and either eliminating in NNSA autonomous agency and either aliminating NNSA as autonomous agency and either eliminating in NNSA autonomous agency and either eliminating in NNSA autonomous agency and either eliminating in NNSA autonomous agency and either eliminating in NNSA an	DR 8	Competing with commercial	away, such as Net Flix, Google, Intel, Cray.						stay bonuses. Continue to find ways to cut through bureaucracy. Use stay bonuses.
Legacy code maintenance, Back         Now to maintain older codes who may have had author         OFF site facilities are used to back up ASC codes after six months of on-site back up. Off site facilities are used to back up ASC codes after six months of on-site back up. Off multiple are used to back up as for two every. Back up as rest twice a years. Back up as rest twice a years and there serve as rest twice a yeare ye		marketplace for talent		Active	3 - Medium	3 - Medium	3 - Medium	Mitigate	
DR 9       Ups, docuentation       refire. If a natural disater strikes will the codes and documentation by distoryed Documentation for ASC       Active       3. Medium       3. Medium       Site back ups for two years. Back ups are sent twice ayear. Back up confirming test is documentation by distoryed Documentation pressons not collocated with platforms         OR 10       Support external users, platforms       they may need to be used by persons not collocated with developers or with less training in code operation.       Active       3. Medium       3. Medium       Move       on issues found by Klocvork static analyzer tool. Runs tabic analyze breach.       DBC added to Ale3d code by Natalica analyze persons not collocated with a set of the complexity of the complexit		Legacy code maintenance, Back	How to maintain older codes who may have had author						Off site facilities are used to back up ASC codes after six months of on-site back up. Off
maintenance.       Odocumentation by distroyed? / Documentation for ASC       Active       A. Medium       S. Medium       Medium <th< td=""><td>DR 9</td><td>Ups, docuemtnation</td><td>retire. If a natural disaster strikes will the codes and</td><td></td><td></td><td></td><td></td><td></td><td>site back up is for two years. Back ups are sent twice a year. Back up confirming test is</td></th<>	DR 9	Ups, docuemtnation	retire. If a natural disaster strikes will the codes and						site back up is for two years. Back ups are sent twice a year. Back up confirming test is
ONE 00       Support external users, platforms       Onle of the challenges with scientific testandhouse is that they may need to be used by persons on collocated with platforms       Active       3 - Medium       3 - Medium       Move on issues found by Klocovork static analysis periods had on sizues found by Klocovork static analysis periods had platforms       Input dexts, input analysis that out by persons not collocated with platforms         OR 20       Input dexts, input analysis that out by persons not collocated with for correct results. Input parameter set is large.       Active       3 - Medium       3 - Medium       Input dexts, set set of in CMool. New dexts are created from copies of previous dexts. Heavy reliance on skilled users to determine correctness of results. Future input dexts, users to end in the challenge with scientific test set for correct results. Input parameter set is large.       Active       3 - Medium       3 - Medium       Leave It       Input dexts, may represent on contractual requirements. This may have a positive impact. Distribute White Paper on Safeness of Safety (Montor         GR 8       ODE to cont so taff positions with little regard for software quality experience. This lack of experience can cause miccommunication and focus on non-important issues.       Active       3 - Medium       4 - Low       Monitor       Continue to educate DOE staff in the principles of software quality experience. This lack of experience can cause miccommunication and focus on non-important issues.       Active       3 - Medium       4 - Low       Mitigate         GPL3       Work to Performance miccommunication and focus on non-importan		maintenance.	documentation by distroyed? Documentation for ASC	Active	3 - Medium	3 - Medium	3 - Medium	Mitigate	done once yearly and coordinated with LC. Details in DRPs for each code team. L2
OR UD       Support externing in does do y performs       Intery may need to be used by performs on controctual operation.       Active       3 · Medium       3 · Medium       on issues found by Kloczwick Risc analyzer of the control. Rus static analysis periodically until it is the previous decks. Heavy reliance on skilled users to one input area decking in simulation codes.         OR 2       The simulation codes are very dependent on correct inputs for correct results. Input Correctness       Active       3 · Medium       3 · Medium       Mole until it is the control input area decking in simulation codes.         MR 8       NNSA Longevity Concerns       under DOE       Identified       3 · Medium       3 · Medium       Monitor       Software.         OF 10       DOE transe       under DOE       Identified       3 · Medium       4 · Low       3 · Medium       Monitor       Software.         R 8       NNSA Longevity Concerns       under DOE       Identified       3 · Medium       4 · Low       3 · Medium       Monitor       Software.         GR 6       DOE turnover       miscommunication and focus on on-important issues.       Active       3 · Medium       4 · Low       Active       Advice uper analysis periodically until it / for periodical uperiodical	00.10	C	One of the challenges with scientific research codes is that						Static Analysis run on all codes, issues triaged, most serious fixed. SQL nave been
Decision       Decision <th< td=""><td>0110</td><td>platforms</td><td>developers or with less training in code operation</td><td>Active</td><td>3 - Medium</td><td>3 - Medium</td><td>3 - Medium</td><td>Move</td><td>on issues found by Klocwork static analyzer tool. Run static analysis periodically until it</td></th<>	0110	platforms	developers or with less training in code operation	Active	3 - Medium	3 - Medium	3 - Medium	Move	on issues found by Klocwork static analyzer tool. Run static analysis periodically until it
OR 2       The simulation codes are very dependent on correct inputs       Active       3 - Medium       3 - Medium       Active       Case it       functionality to indude more input same checking in simulation codes.         GR 8       NNSA Independent study suggests eliminating NNSA as uatonomous agency and either eliminating NNSA in uatonomous agency and eliminating NNSA in uatonomous agency and eliminating NNSA in uatonomous agency and eliminating NNSA in uatonomous agency eliminater eliminating NNSA in		plationity		riceive	5 mean	5 Medium	5 Mcalan	more	Input decks are stored in CM tool. New decks are created from copies of previous
Input Correctness       for correct results. Input parameters et is large.       Active       3 - Medium       3 - Medium       Leave It       functionality to indude more input range checking in simulation codes.         GR 8       MNSA indomous agency and either el ininiting NDSA is autonomous agency and either el ininiting to puting autonomous agency and either el ininiting to puting autonomous agency and either el ininiting to puting initiating NDSA is autonomous agency and either el ininiting to puting initiating NDSA is autonomous agency and either el ininiting to puting initiating NDSA is autonomous agency and either el ininiting to puting initiating NDSA is autonomous agency and either el ininiting to puting initiating NDSA is autonomous agency and either el initiating NDSA is a sub advise and is a sub advise autonomous advise advise and is autonomous advise ad	OR 2		The simulation codes are very dependent on correct inputs						decks. Heavy reliance on skilled users to determine correctness of results. Future
GR 8       NNSA independent study suggests eliminating NNSA as autonowos agency and either eliminating in ynSA as autonowos autonowos adency and either eliminating in ynSA as adency and either eliminating eliminating in y		Input Correctness	for correct results. Input parameter set is large.	Active	3 - Medium	3 - Medium	3 - Medium	Leave It	functionality to include more input range checking in simulation codes.
GR 8       autonomous agency and either eliminating it or putie       Image and the elimit or putie       Image and the eliminating i	GR 8		NNSA independent study suggests eliminating NNSA as						DOE has been more reasonable in there interpretation of contractual requirements.
NNSA Longevity Concerns       under DOE       Identified       3 - Medium       Monitor       Software.         GR 6       DOE Turnover       DOE toris to staff positions with little regard for software quality experience. This lack of experience can cause quality. This provide the experiment could favor experiment could favor experiment can charace quality experience. This lack of experiment could favor experiment can charace quality experiment experiment data experiment data experimentation experimentatis data. Actitie quality experiment experiment and experimentation			autonomous agency and either eliminating it or putting						This may have a positive impact. Distribute White Paper on Safeness of Safety
Continue to educate DDE tanks to start positions with inthe regard for software development and quality.       Continue to educate DDE start in the principles of software development and quality.         GPLR 3       DOE Turnover       miscommunication and focus on non-important issues.       Active       3 - Medium       4 - Low       Mitigate         GPLR 3       Work to Performance incentives (PEP)       Annual goals set for high level management could favor efficiency at expense of safety and security.       Active       3 - Medium       4 - Low       Advise upper management of conflict of safety or security with a PEP. Continue to work for PEP bonuses to direct. Tunded employees who do the work.         OPR 3       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       Mitigate       OPR added for important data (PMP and SCMP). Continual reminder that codes need professional judgement to interpret results.         0R 2       Requirements for developing simulations informed by availables. Requirements for developing simulations up front and Active       3 - Medium       2 - High       Mitigate       Issue tracker use for requirement tracking. Close relationship between designers and users. Aglie process allowing experimentation and changes. Continuous integration or inpitty testinger caniets development and dualer.         0R 3       Medium Requirements Unclear       Active       3 - Medium       2 - High       Mitigate <td></td> <td>NNSA Longevity Concerns</td> <td>under DOE</td> <td>Identified</td> <td>3 - Medium</td> <td>4 - Low</td> <td>3 - Medium</td> <td>Monitor</td> <td>Software.</td>		NNSA Longevity Concerns	under DOE	Identified	3 - Medium	4 - Low	3 - Medium	Monitor	Software.
Option	CD C		DOE tends to staff positions with little regard for software						Continue to educate DOE staff in the principles of software development and quality.
Operation       Instrument of construction and rocus of information informatindin information informatindin information in	GK b	DOF Turpower	quality experience. This lack of experience can cause	Activo	2 Madium	4 100	4.100	Mitigato	
GPLR 3 Incentives (PEPs)       Work to Performance Incentives (PEPs)       efficiency at expense of safety and security.       Active       3 - Medium       4 - Low       2 - High       Mutigate       work for PEP Donues 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         DR 2       Requirements for developing simulation codes       Active       3 - Medium       4 - Low       2 - High       Monitor         DR 2       Requirements for developing simulation to code scond the requirements for developing simulation to different scales requires more resources than currently available. Requirements tonchair unknows up front and Active       3 - Medium       2 - High       Monitor       Issue tracker use for requirement tracking. Close relationship between designers and users. Agile process allowing experimentation and changes. Continuous integration or nightly testing for arritise detection of errors.         OR 3       Code use for answering questions which do not have corresponding experimental dat arequire simulation to provide a measure of uncertainity.       Active       3 - Medium       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.			Annual goals set for high level management could favor	Active	3- Weurum	4-20W	4 - LOW	wiitigate	Advise upper management of conflict of safety or security with a PFP. Continue to
Incentives (PEPs)     Active     3-Medium     4-Low     2-High     Mitigate       OR5     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     DRP added for important data (PMP and SCMP). Continual reminder that codes need professional judgement to interpret results.       DR 2     Requirements for developing simulations informed by available. Requirements for developing simulations informed by codes to determine validation to experimental data.     Active     3-Medium     4-Low     2-High     Mitigate       DR 2     Requirements for developing simulations informed by available. Requirements on developing simulations informed by available. Requirements on developing up for to and corresponding experimental data require simulation provide a measure of uncertaintly.     Active     3-Medium     2-High     Mitigate     Issue tracker use for requirement tracking. Close relationship between designers and users. Aglie process allowing experimentation and changes. Continuous integration or nightly testing for earliest detection of errors.       QR 3     Code use for answering questions which do not have corresponding experimental data require simulation of provide a measure of uncertainity.     Active     3-Medium     2-High     Mitigate       QR 3     Code use for answering questions which do not have corre	GPLR 3	Work to Performance	efficiency at expense of safety and security.	1					work for PEP bonuses to direct funded employees who do the work
OR 5         Over Reliance on simulation codes to determine validation to experimental data.         Active         3 - Medium         4 - Low         DRP added for important data (PMP and SCMP). Continual reminder that codes need professional judgement to interpret results.           DR 2         Requirements for developing simulations informed by different scales requires more resources than currently available. Requirements contain unknowns up front and Uncertainty Quantification Uncertainty Quantification DR 3         Active         3 - Medium         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 aerise talecticin of errors.           OR 3         Code use for answering questions which do not have provide a measure of uncertainity.         Active         3 - Medium         2 - High         Mitigate         SQE staff deployed to assist in improving UQ Pipeline code and documention for results.		Incentives (PEPs)		Active	3 - Medium	4 - Low	2- High	Mitigate	
OR5       Over Reliance on simulation codes       PMP and SCMP suites continually run again simulation codes to determine validation to experimental data.       Active       3-Medium       4-Lew       2-High       Monitor         DR 2       Requirements for developing simulations informed by different scales requires more resources than currently variable. Requirements tonchar unknown sup front and variable. Requirements tonchar unknown sup front and corresponding experimental data require simulation to Uncertainty Quantification provide a measure of uncertainity.       Active       3-Medium       4-Lew       2-High       Monitor       Issue tracker use for requirement tracking. Close relationship between designers and users. Agile process allowing experimentation and changes. Continuous integration or nightly treating for carritical detection of errors.         0R 3       Code use for answering questions which do not have corresponding experimental data require simulation to uncertainty Quantification provide a measure of uncertainity.       Active 3-Medium       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.									DRP added for important data (PMP and SCMP) . Continual reminder that codes need
Codes     Codes to determine validation to experimental data.     Active     3-Medium     4-Low     2-High     Monitor       DR 2     Requirements for developing simulations informed by different scales requires more resources than currently available. Requirements contain unknowns up front and Uncertainty Quantification     Active     3-Medium     4-Low     2-High     Monitor       DR 2     Requirements for developing simulations informed by available. Requirements contain unknowns up front and Code use for answering questions which do not have Uncertainty Quantification     Active     3-Medium     2-High     Mitigate     Insue 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     Code use for answering questions which do not have Uncertainty Quantification provide a measure of uncertainity.     Active     3-Medium     2-High     Mitigate	OR 5	Over Reliance on simulation	PMP and SCMP suites continually run again simulation						professional judgement to interpret results.
DR 2       Requirements for developing simulations informed by different scales requires more resources than currently available. Requirements contain unknowns up front and corresponding experiemnal data requires minutation to Uncertainty Quantification       Active       3 - Medium       2- High       Mitigat       Injuty testing for earliest detection of errors.         OR 3       Code use for answering questions which do not have Uncertainty Quantification       Code use for answering questions which do not have corresponding experiemnal data requires imulation to provide a measure of uncertainty.       Active       3 - Medium       2- High       Mitigat       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.	L	codes	codes to determine validation to experimental data.	Active	3 - Medium	4 - Low	2- High	Monitor	
Un 2     uniferent suns requires more resources than currently available. Requirements to onch any support and corresponding experimentation and dnages. Continuous integration or any support and the support of the suppor	DR 2		Requirements for developing simulations informed by						Issue tracker use for requirement tracking. Close relationship between designers and
Description         presentation         Presentation </td <td>Requirements Linclear</td> <td>uniferent scales requires more resources than currently</td> <td>Active</td> <td>2 - Madium</td> <td>2- High</td> <td>2- High</td> <td>Mitigate</td> <td>users. Agrie process allowing experimentation and changes. Continuous integration or</td>		Requirements Linclear	uniferent scales requires more resources than currently	Active	2 - Madium	2- High	2- High	Mitigate	users. Agrie process allowing experimentation and changes. Continuous integration or
OR 3 Corresponding experiemental data require simulation to detain documentation to detain a corresponding experiemental data require simulation to detain documentation to detain a corresponding experiemental data require simulation to detain documentation to detain a corresponding experiemental data require simulation to detain a corresponding experiementation and the corresponding experimentation of results. Active 3 - Medium 2 - High Mitigate		nequirements onciear	Code use for answering questions which do not have	Active	5- Weurdm	2" riigii"	2º High	wingard	SOF staff deployed to assist in improving UO Pipeline code and documention for users
Uncertainty Quantification provide a measure of uncertaintly. Active 3- Medium 2- High 2- High Mitigate	OR 3		corresponding experiemntal data require simulation to						of the code. Also emphasiss on reporting tools to allow easier interpretation of results.
		Uncertainty Quantification	provide a measure of uncertainlty.	Active	3 - Medium	2- High	2- High	Mitigate	

## **Comparison of Approaches: Venn Diagram**



### **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



