

Nominal Program Hazard Analysis

A new approach to
hazard analysis

Presented to: 3rd IAASS Conference

By: Jay Naphas, AST-300

Date: October 21, 2008



Federal Aviation
Administration



Overview

- **Why we need new methods**
 - The trouble with software
 - Handling complexity
- **Requirements for a new method**
- **Nominal Program Hazard Analysis**



Impetus

- **Current hazard analyses have problems**
 - Difficult to conduct
 - Difficult to evaluate
 - Difficult to maintain
 - Different analyses for parts of systems
 - SFMECA
 - Implicitly assume safety = reliability
- **Complex systems are not well handled**

Requirements

- **Must handle all subsystems equally**
- **Must track system goals to component verification tests**
- **Must integrate into safety culture**



Handling Software

- **Violates the central limit theorem**
 - No distribution
 - No randomness
 - No mean, median, mode, etc.
- **Non-random**
 - Software is a mathematical construct
 - Randomness is deliberately removed
- **Software faults cannot be described by statistics**
 - Method must be non-probabilistic

Handling Complexity

- **Reduce analytical complexity**
 - Analysis method supplements analyst's mind
 - Analytical format guides analysis and facilitates cross-checking
- **Preserve system information**
 - Technical details must connect to system behaviors
 - Details must not interfere with understanding of the system

New Theories

- **System Safety for the 21st Century**

“Unfortunately, the state of the art in software hazard analysis appears to be woefully lagging.”

- **STAMP/STPA**

- Systems Theoretic Accident Model and Processes
- Systems Theoretic Process Analysis
- Use systems theory to analyze hazards

STAMP

- **Systems Theoretic Accident Model and Processes**
 - Accidents are violations of safety constraints
 - Not failures
 - Safety is an emergent property
 - Not a component property
 - Use control theory to ensure safety
 - Control theory applies to all systems
 - Electromechanical
 - Software logic
 - Social

NPHA

- **Nominal Program Hazard Analysis**
 - Built on control theory
 - Non-probabilistic
 - Treats all safety systems equally
 - Hardware, software, and human factors
 - Traces system goals to component tests and analyses
 - Connects other hazard analyses to a common reference point
 - Spreadsheet

NPHA Example

<u>System Intent</u>	<u>Sub-Intents</u>	<u>Involved Systems</u>	<u>Involved Subsystems</u>	<u>Control Actions</u>	<u>Intent Failures</u>	<u>Mitigation Measures</u>	<u>Verification Evidence</u>
Must not enter an unintended flight path	Must hold selected altitude	Guidance	GPS	Detects 3-D position of receiver	Receiver moves relative to vehicle	Design GPS mount with safety factor of 5	Finite element analysis
							Non-destructive testing
					Antenna separates from receiver	Soldered connection	Inspect connection before flight
						Mounted on a single bracket	Finite element analysis

NPHA

- **Repetition is expected**
 - Multiple examinations of every subsystem
 - Examination of role variety
- **Probability and severity are ignored**
 - Hazards identified as possible constraint violators are inherently worth mitigating
 - Engineering judgment decides when mitigation is sufficient
 - Judgment is reviewed by checking the spreadsheet

NPHA Continues

- **Connections**

- “System Intents” from mission requirements and regulations
- “Intent Failures” are the beginning of a fault tree or FMECA
 - Check hazard analyses against each other directly
- “Mitigation Measures” is a list of critical components and operations
- “Verification Evidence” is a pre-flight and return-to-service checklist
- Can be implemented as a spreadsheet or database

NPHA Experiment

- **Retrospective hazard analysis**
 - Used NPHA spreadsheet on historical systems
 - Found undocumented hazards
 - GPS sensor displacement may move vehicle
 - Faults not checked for in checklists

NPHA Advantages

- **Clarity**
 - System goals connect directly to details
 - Enables conceptual communication and technical evaluation
 - Format familiar to hazard analysts
- **Continuity**
 - No need for separate software analyses
 - Easy and natural to maintain as systems evolve
- **Control of complexity**
 - Reduces cognitive load on analysts
 - Simplifies analytical process without losing system information

NPHA Advantages

- **Hazard ideation**
 - Improved by referencing goals
 - Column sequence leads analyst to system interactions
- **Maintenance**
 - Hazard analysis is maintained through system changes without separate steps
 - No software to maintain
 - Format comprehensible to all staff

NPHA Limitations

- **Extremely complex systems**
 - Spreadsheets become unwieldy
 - Difficult to find interaction faults without control flow diagrams
 - Require more sophisticated analytical support
 - STPA

- **NPHA designed for**
 - Single-vehicle programs
 - Single-purpose or experimental vehicles

Conclusion

- **NPHA**

- Control theory replacement for PHA
- Improves hazard ideation
- Enables direct cross-referencing of hazard analyses
- Useful in operational environment
 - Checklists derived directly from hazard analysis
 - Easy to use and maintain

Questions?

- **Contact: Jay Naphas**
 - Email: Jay.Naphas@faa.gov
 - Phone: +1-202-493-5459
 - Fax: +1-202-267-5463

- **Reviews, comments, and suggestions are most welcome**