

# SYSTEM SAFETY ENGINEERING

*Training offered by APT Research, Inc.*

## System Safety Engineering Course

The System Safety Engineering training course is designed for safety professionals wanting to advance their skill and knowledge in techniques supporting hazard discovery, assessment and control of risk. The course includes descriptions of methods for establishing and managing a system safety program. A review of the basic principles of the system safety discipline, description of principles of risk acceptance, and the method for reviewing risk analyses performed by others is included. Each of the modules is listed below with representative examples described on the reverse of this sheet:

- Concepts in Risk Management
- Initiating a System Safety Program
- Working with the Risk Assessment Matrix
- Energy Sources
- Preliminary Hazard Analysis
- Operating and Support Hazard Analysis
- Failure Modes and Effects Analysis
- System Safety Risk Assessments
- Safety Assessment Reports
- Working with MIL-STD-882
- Fault Tree Analysis
- Introduction to Software Safety
- Event Tree Analysis
- Introduction to Sneak Circuit Analysis
- Cause-consequence Analysis
- Introduction to Markov Analysis
- Failure Probability Assessments
- Human Factors
- Writing Procedures
- Selected Analysis Methods
- Weighted Scoring
- Risk Management Strategy Selection
- Accepting Risk

## Course Duration and Format

The course is 36 hours over 5 days, with about 6 hours of lecture each day and time for students to complete workshop problems or review course materials with the instructor. Class size will be limited to 30 attendees. Attendees of this course will be credited with 3.0 Continuing Education Units (CEU) upon completion of this course.



## Safety Engineering and Analysis Center

The APT Safety Engineering and Analysis Center (SEAC) is conveniently located in Cummings' Research Park near Redstone Arsenal in Huntsville.

### Where

The APT Research,  
Safety Engineering and Analysis  
Center in Huntsville, AL

### Schedule

See [www.apr-research.com/  
Capabilities/Training.html](http://www.apr-research.com/Capabilities/Training.html)

### Cost

\$2595

### Registration Information

256.327.3370  
[training@apt-research.com](mailto:training@apt-research.com)

### Technical Information

Adriaan Ostrander  
256.327.3398  
[aostrander@apt-research.com](mailto:aostrander@apt-research.com)

### Other Courses Available

- Explosive Safety
- Software Safety
- System Safety for Decision Makers
- Safety for Test Personnel

# GENERIC SYSTEM SAFETY PROCESS

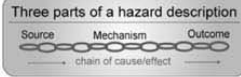


- Element 1  
Program Initiation**
- Plans
  - Authorizations
  - Contract(s)
  - Team
  - Tools

Element 2

## Hazard Identification and Tracking

**1) Process:** The initial step produces a complete definition of the hazards associated with the system. This can be achieved by a variety of methods. Key elements of the risk assessment matrix are also defined.



Understanding of Hazards

- 2) Methods:**
- Checklists
  - System Energy Source Inventory
  - Prior Work with Similar Systems
  - Operating Scenario Walkthroughs
  - Operational Phase Review
  - Codes/Standards/Regulations
- Includes:
- Description
  - Assessed Risk
  - Potential and Selected Countermeasures
  - Accident Experience
  - Lessons Learned

**3) Products:**

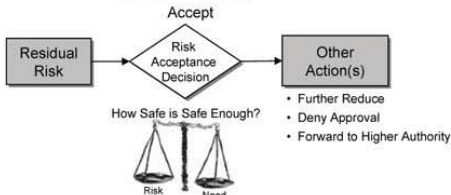


Lifecycle Monitoring

Element 5

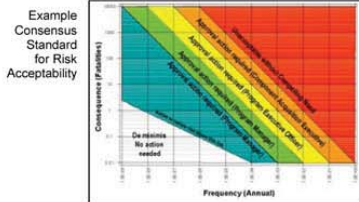
## Risk Acceptance

**1) Process:** Properly designated decision-makers are provided sufficient information to make an informed decision concerning the acceptability of residual risk. All decisions are to be documented.



- 2) Methods:**
- 1) Compare to Consensus Standards for
    - a) Protection of Personnel
    - b) Societal Risk
  - 2) Balance Risk with Needs

**3) Product:**  
Documented Risk-Based Decision



Protected under U.S. Copyright Laws. Copyright © 2005 A-P-T Research, Inc.

Element 3

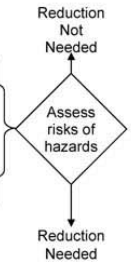
## Risk Assessment

**1) Process:** For each identified hazard the severity and likelihood are established. The Risk Assessment Matrix is used to assess and display the risk.

The matrix defines the "risk space" for a single-system and a declared exposure duration (e.g., 1 year, 1 lifecycle).

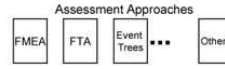
Severity	H7	H2	H3
H6			
H9			
H5			
H8			
H4			

Probability →



**2) Assessment Methods:**

- Expert Judgment
  - Historical Risk Experience
  - System Knowledge
  - Engineering Judgment
  - What is Known/not Known
- Numerical Analysis
- Computer Models



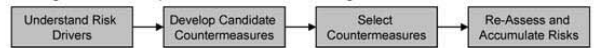
**3) Products:**



Element 4

## Risk Reduction

**1) Process:** Risk Reductions are achieved by understanding the risk, countermeasuring the risk according to an order of precedence, and reassessing risks.



**2) Methods:**

- Understanding risk causation can lead to prioritizing hazard reductions and/or direct countermeasure selection.
- Countermeasure Order of Precedence:
- 1) Design Changes
  - 2) Engineered Safety Features
  - 3) Safety Devices
  - 4) Warning Devices
  - 5) Procedures/Training
- Countermeasures shouldn't:
- 1) Introduce new hazards
  - 2) Unacceptably impair system performance
- Countermeasure Selection Criteria:
- Cost (vs., accepting risk)
  - Effectiveness (In reducing risk)
  - Feasibility
    - Means
    - Schedule
- Accumulate total system risk by proper mathematical protocol
  - Validate Risk Reductions

**3) Products (typical):**



T-04-01100 Strawman 032305

## APT Point of Contact

Adriaan Ostrander  
256.327.3398  
aostrander@apt-research.com



A-P-T Research, Inc.  
4950 Research Drive  
Huntsville, AL 35805  
www.apt-research.com