The Safety Engineering & Analysis Center
SEAC
The mission of the SEAC is to support the discipline of safety engineering with nine specific mission areas:

1. Provide world class SMA training
2. Conduct workshops to advance safety disciplines
3. Conduct independent (third-party) safety assessments
4. Support professional societies
5. Develop and apply analytical protocols and tools
6. Assist in developing standards; maintain library of up-to-date standards
7. Conduct research and publish books, proceedings, and relevant documents
8. Prove subject matter expertise to internal and external customers
9. Host customer safety meetings

Selected Profiles

**Saralyn Dwyer, VP, SEAC Director**
- Officer in ISSS, member of executive committee
- Extensive experience with US Army and MDA development programs
- Current Director of SEAC
- 20+ years of experience

**Dusty Nix**
- 10+ years systems engineering experience
- MS Aerospace Engineering; BS Mechanical Engineering

**Megan Stroud**
- 10+ years experience in safety engineering and analyses
- APT Training Coordinator
- MS Engineering Management, BS Engineering
#1: TRAINING

<table>
<thead>
<tr>
<th>System Safety</th>
<th>Software System Safety</th>
<th>Explosives Safety</th>
<th>IMESAFR</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3.6 CEUs*)</td>
<td>(2.4 CEUs)</td>
<td>(2.4 CEUs)</td>
<td>(2.4 CEUs)</td>
</tr>
<tr>
<td>• Concepts in Risk Management</td>
<td>• Risk Management Concepts and Risk Acceptance</td>
<td>• Explosives Basics</td>
<td>• QD Concepts &amp; Background</td>
</tr>
<tr>
<td>• Principles of System Safety</td>
<td>• Principles of System Safety</td>
<td>• Hazardous Stimuli</td>
<td>• QRA Concepts &amp; Background</td>
</tr>
<tr>
<td>• Working with the Risk Assessment Matrix</td>
<td>• Hazard Analyses</td>
<td>• Basic Storage &amp; Transport Principles</td>
<td>• Software Features &amp; Interface</td>
</tr>
<tr>
<td>• Energy Flow-Barrier Analysis</td>
<td>• Human Factors &amp; Operator Errors</td>
<td>• Hazard Classification</td>
<td>• Risk Management</td>
</tr>
<tr>
<td>• Hazard Analyses</td>
<td>• Software Development Overview</td>
<td>• Quantity-Distance</td>
<td>• Architecture – Parts 1 &amp; 2</td>
</tr>
<tr>
<td>• The Operating &amp; Support Hazard Analysis (O&amp;SHA)</td>
<td>• Intro to Software System Safety</td>
<td>• Explosives Item Recognition &amp; Safety</td>
<td>• Linking Architecture to Testing</td>
</tr>
<tr>
<td>• Failure Modes and Effects Analysis</td>
<td>• Software System Safety Analyses</td>
<td>• Personnel Protection</td>
<td>• Advanced Tools</td>
</tr>
<tr>
<td>• Fault Tree Analysis</td>
<td>• System Concepts Refinement Phase</td>
<td>• Reaction Effects</td>
<td>• Approval Process</td>
</tr>
<tr>
<td>• Event Tree Analysis</td>
<td>• Software Requirements</td>
<td>• Insensitive Munitions</td>
<td>• Input Decisions</td>
</tr>
<tr>
<td>• Cause-Consequence Analysis</td>
<td>• Architecture Development Phase</td>
<td>• Electrostatic Discharge Protection</td>
<td>• Protocols</td>
</tr>
<tr>
<td>• Intro to Markov Analysis</td>
<td>• Software Design and Code Phase</td>
<td>• Lightning Protection</td>
<td></td>
</tr>
<tr>
<td>• Making Component Failure Probability Estimates</td>
<td>• Software Test, Verification and Validation Phase</td>
<td>• Electromagnetic Radiation Protection</td>
<td></td>
</tr>
<tr>
<td>• Sneak Circuit Analysis</td>
<td>• SwSS for Software Release</td>
<td>• Standing Operating Procedures for A&amp;E Operations</td>
<td></td>
</tr>
<tr>
<td>• Intro to Software System Safety</td>
<td>• Initiating a System Safety Program</td>
<td>• Quantitative Risk Assessment</td>
<td>• SAFER Features</td>
</tr>
<tr>
<td>• Human Factors &amp; Operator Errors</td>
<td>• Software System Safety Technical Review Panels and Boards</td>
<td>• Explosives Models</td>
<td>• Risk Management</td>
</tr>
<tr>
<td>• Guidelines for Writing Operating Procedures</td>
<td>• Airworthiness</td>
<td>• Intro to Explosive Testing</td>
<td>• Risk Reduction</td>
</tr>
<tr>
<td>• Initiating the System Safety Effort</td>
<td>• Software System Safety Lessons Learned &amp; Summary</td>
<td></td>
<td>• Risk Acceptance</td>
</tr>
<tr>
<td>• Risk Acceptance</td>
<td>• System Safety SSPP Exercise</td>
<td></td>
<td>• Approval Process</td>
</tr>
<tr>
<td>• Furry Slurry Processing</td>
<td>• Traffic Control System at a Major Intersection</td>
<td></td>
<td>• Practice – Defining the Group</td>
</tr>
<tr>
<td>• The Fast Asp™ Missile</td>
<td></td>
<td></td>
<td>• Architecture Overview</td>
</tr>
<tr>
<td>• Automated Inspection Kick-Out System</td>
<td></td>
<td></td>
<td>• Architecture – Science Algorithms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Architecture – Aggregation and Uncertainty</td>
</tr>
</tbody>
</table>
#2: WORKSHOPS

One of the SEAC missions is to advance the state of the discipline in SMA. This is accomplished by hosting workshops wherein experts in the field are invited to collaborate. Workshops have been attended by personnel from NASA, MDA, AMCOM Safety, DoD, Industry, as well as other agencies.

- “Good System Safety Practices” Workshop, 2006
- “Web-Based Risk Assessment Tool” Workshop, 2008
- “Risk Summing” Workshop, 2010
- IAASS Launch Risk Workshop #1, 2010
- “Safety Case” Workshop, 2013
- IAASS Launch and Re-Entry Workshop #7, 2016
#3: INDEPENDENT SAFETY ASSESSMENTS

APT Analysis Process:
Applies multiple state-of-the-art methods

- Develop Plan
  - Define Question
  - Clarify: Suspense, Products
  - Assign RA
  - Security
  - ID Protocol
  - ID Data Rqts
  - ID Tool Mods
  - Draft Schedule
  - Kick Start Meeting

- Collect Data
  - Finalize Rqts
  - Availability
  - Collection
  - Development
  - Verification
  - Data Review

- Prepare Tools
  - Review Tools
  - ID Mod Rqts
  - Verification Rqts
  - Modify Tools
  - Verify Mods
  - Config Mgt
  - Tool Review
  - Use Release

- Conduct Analysis
  - Format Data
  - Build Inputs
  - Run Codes per Protocol
  - Build Archive
  - Sanity Checks
  - Post-process

- Interpret Results
  - Review: Archive, Question, Inputs/Outputs
  - Form Conclusions
  - Internal Review

- Document Findings
  - Complete Customer Products
  - Compile Archive

Complex Systems:
SEAC conducts numerous independent safety analyses of large, technically complex facilities

Example Independent Study Sponsors:
- Disneyland
- Air Force Safety Center
- Raytheon – Tucson

Typical Products:
- Hazard Analyses
- Event/Fault Trees
- Quantitative Risk Assessment (QRA)/Probabilistic Risk Assessment (PRA)
- Explosive Effects Models
- Flight Safety Modeling
- Training
#4: PROFESSIONAL SOCIETIES

A substantial responsibility for any professional is to give back to the profession via their ideas for improvement. APT encourages this involvement via at least four substantial investments.

- **G-48 System Safety Committee** (currently under the Aerospace Council of SAE International).
  - The G-48’s mission is to develop, publish, promote, and improve best practices in system safety.
  - G-48 members are key system safety leaders from industry, military, and civilian government agencies, including NASA.
  - APT and SAIC have been active G-48 contributors for over 10 years.
  - APT collaborates with G-48 and represented organizations on workshops and initiatives that advance the state-of-the-art in system safety.

- For the ISSS, APT hosted the “Bringing Discipline to Our Discipline” panels at the International System Safety Conference from 2004 to 2009.

- APT is collaborating with the ISSS to produce a volume entitled *The System Safety Handbook*.

- For the IAASS, APT chairs the Launch and Re-entry Safety Committee. This committee hosts international workshops every nine months as part of its charter to publish a text documenting the quantitative methods of achieving risk basis of launch and reentry risk management.

1st IAASS International Experts Workshop on Public Safety Risk of Space Missions, 2010


“Bringing Discipline to Our Discipline” expert panels held at the ISSC 2004-2009
#5: TOOLS

**Classical System Safety Tools**
- Failure Mode and Effects Analysis
- Fault Tree Analysis
- Event Tree Analysis

**Range Safety Tools**
- RA PIEC
- RA FIP
- KIDD
- BREEZE
- TRAX
- FAIL
- CORAL
- DAMP
- STK
- DispDR
- CORiDOR
- PIRAT
- FRANG
- DeBRA
- Auspex
- TRAIL DISP
- SHOCK
- FRAG
- Aurora
- SARA
- RFHAZ
- RSIP
- IMPACT
- Horizons
- MUDEMIMP
- GRM
- SAFER

**Risk Management Tools**

**Tailored Risk Management Applications**
- NASA
- SMD C
- ARMY
- Others

**Tailored RAC Matrix Options**
- NASA
- MIL-STD-882E
- FAA
- Others

**ART – APT Risk Management Tool**

**HTS – Hazard Tracking System**

**Flight Safety Tools**
- DebRA
- STK
- SARA
- SDZ Calc
- GRM
- BREEZE
- Others

**Explosives Safety Tools**
- IMESAFR
- SAFER
- DIRE

**Analysis Tools**
- RF Analysis
- Toxic Analysis
- Laser Analysis
#5: TOOLSET

**APT Explosives Safety Models**
- IMESAFR – Institute of Makers of Explosives Safety Analysis for Risk
- SAFER – Safety Assessment for Explosives Risk
- DIRE – Analysis of Deaths and Injuries Resulting from Explosions

**Primary Flight Safety Models**
- SAFELAB – Range Safety Toolkit
- DebRA – Debris Risk Assessment
- KIDD – Kinetic Intercept Debris Distribution
- MILS – Multiple Impact Location Simulator
- GenCon – Aircraft Risk Assessment
- STK – Satellite Toolkit
- SARA – Satellite Risk Assessment
- Risk Based Range Assessment Tool
- Surface Danger Zone (SDZ) Calculator
- DASP – Debris Analysis for Satellite Programs
- TVIP – Turning Vehicle Impact Predictor
- Ascent – Trajectory Modeling, End Condition Targeting, Optimization Capabilities
- LiMAns – Link Margin Analysis
- GRM – Debris Risk Assessment
- BREEZE – Toxic effects model
- AFTOX – Air Force toxics model

**System Safety Tools**
- ART – APT Risk Tool
- HTS – Hazard Tracking System

**APT Internal Launch Area Risk Models**
- TRIAL – Trajectories for Risk Investigations at Launch
- FRAG – Solid Rocket Motor Fragmentation
- FAIL – Vehicle Failure Filter
- PADPOP – Pad Populations
- RAFIP – Random-Attitude Failure Impact Points
- SHAPE5 – Shaping Constants for Mode 5 Impact Distribution
- DAMP – Facility Damage and Personnel Injury
- DISP – Impact Locations and Dispersions for DAMP
- Contour – Generate Equi-valued Contour Lines
- GenDeb – Generates Debris Classes for Liquid-Propellant

**APT Internal Overflight Risk Models**
- CORAL – Collective Overflight Risk Analysis Tool
- CORIDORE GIS – Corridor Risk Estimation
- RAPIEC – Random-Attitude PI and EC
- TRAX – Trajectories for Risk Analysis Extended
- GreenN – Computations of Green Numbers
- AC-HIT – Aircraft Hazards from Impact
- HITP – Ship Hit Probability Computations
- PIRAT – Propellant Impact Response Assessment Team
- INCCA – Interactive Coordinate Calculator

**3rd Party Overflight Risk Models**
- POST – Program To Optimize Simulated Trajectories
- ALE3D – Arbitrary Lagrange/Eulerian Hydrodynamics Code
- TAOS – Trajectory Analysis and Optimization Software

**Secondary Flight Safety Models**
- DBRISK – Distribution-Based Risk
- Minimax – A process of minimizing the maximum risk
- VeSA – Velocity Search Algorithm
- ASAP – Artificial Satellite Analysis Program
- Test Requirements Allocation Database
- CASA – Casually areas for impacting debris

**Flight Safety Utilities**
- PACISLD – A plot file of Pacific islands to supplement existing world map plot files.
- POPDb – Population Database is a database of Pacific islands which complements the PACISLD plot file.

**Ground Safety Models**
- RF Hazards
- FaulTrease – Supports Fault Tree Analyses for use in safety and reliability analyses

**Secondary Explosives Safety Models**
- FRANG
- MUDEMIMP – The Multiple Debris Missile Impact Simulation model
- SHOCK

**Environmental Engineering Models**
- SATT – Site Assessment of Tornado Threat

**GIS Mapping**
- ArcView GIS – Computer Aided Design package by Autodesk Inc. used widely throughout government and industry
#5: SPECIAL PROJECTS

The Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs Task Force funded the following projects through the SEAC:

- **System Safety Performance Level Model (2007):** The model serves as a useful tool to gauge the health of a safety program at any stage of the program's lifecycle.

- **Risk Summing Guide (2009):** A guidebook that enables risk acceptance authorities to judge risk acceptability on the basis of its true total value rather than on a view of the many individual risks embedded within a system.

- **CREATe (2012):** Composite Risk Evaluation and Assessment Tool electronic (CREATe) is a web-based software tool to be used by safety analysts to perform hazard analyses and risk assessments. The tool provides standardization of data tracked and allows management real-time visibility into risk assessments.
#6: STANDARDS DEVELOPMENT

- **RBESCT.** Assisted in gaining consensus for evolving practices of risk-based methods for explosives safety in DoD.
- **Yuma Risk-Based Approach.** Assisted in policy development for risk-based analysis of test events.
- **NATO.** Assisted in the development of Allied Ammunition and Storage Publication (AASTP)-4, Part I (Risk Analysis Manual), and Part II (Explosives Safety Risk Analysis).
- **RCC.** Technical secretariat in the development of Range Commanders Council (RCC) 321-97 and updated RCC 321-00.
- **TM5-1300.** Compiled comments from government and industry for rewrite.
APT conducts substantial internal and customer funded research into safety methods and emerging practices.

Recent Publications

- Fragmentation Characteristics of Steel Structures with Low Loading Density for Fast-Running Models, 2015
- Use of Unified Modeling Language (UML) in Model Based Development (MBD) for Safety-Critical Applications, 2013
- What Would Pascal Think About Space Safety?, 2013
- Fleet Failure “Clusters” Can Belie Truth, 2013
- Preparing to Undertake the System Safety Analysis, 2013
- The Science of Quantitative Risk Assessment for Explosives Safety, 2012
- Defining a “Safety Center of Excellence, 2009
- Do QRAs Produce Music or Noise?, 2009
- The 8 Important Ideas Imbedded in the ANSI Standard, 2009
#7: OTHER PUBLICATIONS

- The URS addresses “How safe is safe enough?”
- Risk tolerance for warnings and stoppages
- System Safety Scrapbook
- Component Failure Probability Information Handbook

**URS Scale – Public Risk (Involuntary)**

<table>
<thead>
<tr>
<th>Regulatory Standards</th>
<th>Annual Risk</th>
<th>Actual Risk Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nuclear Power Plants (UK HSE)</td>
<td>10^2</td>
<td>MR (Australia – 2000-02) 14</td>
</tr>
<tr>
<td>Swiss Ammunition Storage</td>
<td>10^3</td>
<td>MR (Heart Disease NY City – 1990) 11</td>
</tr>
<tr>
<td>Non-commercial Ammunition Storage</td>
<td>10^4</td>
<td>MR (Heart Disease UK – 1990) 11</td>
</tr>
<tr>
<td>Future Nuclear Power Plants (Dutch)</td>
<td>10^8</td>
<td>MR (Military Warnings – 1990) 11</td>
</tr>
</tbody>
</table>

**Road Signs for Risk Space**

- Road signs prescribe actions, provide information, and define limits.
  - Risk is too high
  - Proceed only with significant need
  - Properly authorized approval required
  - ALAP required

- Risk is a concern
- ALAP required

References:
- "Road Signs in Risk Space," Tom Pilop, Bill Pilop, Meredith Hardwick, Briefing, August 2004
#8: SUBJECT MATTER EXPERTISE

### SEAC Fellows with MS or PhD and Deep Expertise

<table>
<thead>
<tr>
<th>Name</th>
<th>Expertise</th>
<th>Background</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tomlin</td>
<td>System safety</td>
<td>Chief Safety SMDC</td>
</tr>
<tr>
<td>Tom DeLong</td>
<td>System &amp; missile safety</td>
<td>US Army</td>
</tr>
<tr>
<td>Barry Hendrix</td>
<td>SMA management</td>
<td>LMCO SMA Fellow</td>
</tr>
<tr>
<td>Tom Pfitzer</td>
<td>Risk management, QRA</td>
<td>Range Safety Officer</td>
</tr>
<tr>
<td>Pete Yutmeyer</td>
<td>Hazard classification</td>
<td>Army/DDESB</td>
</tr>
<tr>
<td>Bob Baker</td>
<td>Aerospace math models</td>
<td>APT Chief Analyst</td>
</tr>
<tr>
<td>Dr. John Hall</td>
<td>Quality</td>
<td>APT Technical Director</td>
</tr>
<tr>
<td>John Frost</td>
<td>Risk management</td>
<td>NASA ASAP</td>
</tr>
<tr>
<td>Dr. Tyler Ross</td>
<td>Risk management</td>
<td>US Navy</td>
</tr>
<tr>
<td>Eric Olson</td>
<td>Weapons safety</td>
<td>Top civilian at AFSEC</td>
</tr>
<tr>
<td>Mike Swisdak</td>
<td>Explosion effects</td>
<td>US Navy</td>
</tr>
<tr>
<td>Paul Lahoud</td>
<td>Structural effects of blast</td>
<td>USACE Chief, Facility design</td>
</tr>
<tr>
<td>Dr. Frank Tatom</td>
<td>Modeling explosions</td>
<td>Chief engineer SAIC</td>
</tr>
</tbody>
</table>

The SEAC is recognized as a national Center of Excellence providing deep expertise to multiple SMA needs.

---

### SMEs with National Recognitions

- Two time ASAP member on Board of Directors (John Frost)
- Former Chief Engineers at AFSC (Eric Olson, Paul Price)
- Former Chiefs of Safety MICOM, SMDC (Max Tomlin, Phil Owen)
- Directors/Officers in ISSS (Saralyn Dwyer, Melissa Emery, Barry Hendrix)
- Fellows in ISSS (Tom Pfitzer, Barry Hendrix)
- Board Member on IAASS, Chair of Launch Safety Committee (Tom Pfitzer)
- Former Lockheed Martin Technical Fellow for System Safety (Barry Hendrix)
- Former Director of Safety, Quality & Mission Assurance for USA Space Shuttle Operations (Jimmy Rudolph)
- Former Explosives Hazard Classification Authority for US Army (Pete Yutmeyer) and US Air Force (Eric Olson)
- International experts in modeling explosives effects, and range safety (Dr. Frank Tatom, Mike Swisdak, Bob Baker)
#9: FACILITIES

- The SEAC facility, located in Huntsville’s Cummings Research Park, provides substantial meeting amenities and is used by our customers to host technical working meetings and training courses.
- Approximately 170 technical meetings per year are held at the SEAC at no charge to our customers.
- The SEAC provides local safety professionals with references, training, and meeting space to resolve safety issues.