NAVAL POSTGRADUATE SCHOOL

UNCLASSIFIED

Results of the First IEEE International Workshop on Safety of Systems

Bret Michael

Chair, IEEE Technical Committee on System Safety

Professor, Naval Postgraduate School

Tel. (831) 656-2655

bmichael@nps.edu

20th Annual Systems and Software Technology Conference

May 1, 2008, Track 1, 11:25 AM - 12:10 PM

UNCLASSIFIED

Disclaimer

- **The views and conclusions in this presentation are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government**

Background

- **IEEE Technical Committee on System Safety (TCSS), sponsored by the IEEE System Council, held its first international workshop on issues relating to safety of systems of national and global significance**
  - Open working forum for obtaining a holistic view of system safety for a better understanding of the system safety discipline
  - Much of the discussion that took place during the workshop
- **Participants at the first workshop focused their attention on the relationships between safety and the other areas of dependability, such as security and reliability**
  - They expressed interest in leveraging these relationships to build **trustworthy systems**

Workshop discussion items

1. **What are the three fundamental limitations and knowledge barriers for safety of systems today?**
2. **What are the three most important research challenges?**
3. **What are promising innovations and abstractions for building future high-confidence safety systems?**
4. **What are possible milestones for the next five to ten years?**

Fundamental knowledge barriers for safety of systems today

- How to measure safety, security, and other "ilities" for stovepipe and system of systems
- How to make weightings explicit for tradeoff analysis, and are those the correct weights
- Need for both concepts and definitions to be understood by safety, security, and other communities
- We are unable to describe uncertainty in common terms
- Misunderstanding of what standards provide
- Practitioner competence
- Realistic expectations on practitioners
- Risk management, such as how to model security problems
- Understanding the roles and responsibilities of each discipline, and how they fit together
- What decisions are we trying to support from our analyses of systems

Fundamental limitations for safety of systems today

- **Limitations**
  - A mindset of evolving vice building dependable systems
  - Influences of organizational culture and established work practices
  - Problem-solving approaches resulting in unnecessarily complex systems
  - Lack of integration among policy, guidance (how to do it), standards and compliance enforcement
  - Defining the system boundary
  - Lack of codification within standards
  - Unknowns: very large number of possible vulnerabilities, hazards, etc.
  - Incentives are not congruent with the risks; identify what causes those factors to be in the decision formula (not defined in the standards today)
  - System integration is done poorly, partly due to the lack of tool support
  - Turf issues, such as between IEEE technical committees, societies, and councils

Most important research challenges

- There needs to be an as-is report of the safety and security domains
- Create the to-be report for both the safety and security domains, including the mission and sustainment domain
- Perform the gap analysis
- Assurance cases
- Automation support for building and analysis of architectures on an ility-basis
- Composition of systems into system of systems, including across organizations
- How do you specify uncertainty for security?
- Establish a sub grand challenge on dependability

Promising innovations and abstractions for building high-confidence safety systems

- **Assurance cases that are usable across domains**
- **Tools interoperability**
  - Tools that reuse existing data rather than rely on translating data between tools, analyses, etc.
- **Formalize system of systems engineering techniques, concepts, etc., via means such as**
  - DoD Guidebook on SoSE effort
  - IEEE International Conference on System of Systems Engineering (will be held in Monterey, CA in June 2008)
- **Formalize the as-is availability and data trades between safety and security**
- **Formally codify precepts (programmatic, design, operations guidelines) for both safety and security, and cross compare**

Things IEEE could do for us now

- **Establish avenues for members of the community of interest (COI) on dependability to share ideas and documents**
  - Encourage IEEE HQ to foster cooperation across societies, councils, technical committees to address system dependability
  - Encourage the IEEE Computer Society, International System Safety Society, and RAMS to re-establish joint conferences between safety and security; for international coverage: SAFECOM, IEE Software Safety Symposium
- **Establish a column editor for *Security & Privacy*, *Software*, or some other IEEE magazine to address the role between safety, security, and other ilities in building trustworthy systems**
  - A first step in this direction has occurred—the Computer Society and Reliability Society now jointly own Security & Privacy and have expanded the magazines scope to include trustworthy systems

Possible milestones for the next five years

- **Finalize the**
  - As-is report of the safety and security domains
  - To-be report for both the safety and security domains, including the mission and sustainment domain
  - Gap analysis
- **Standards on assurance that span safety, security and other aspects of dependability, such as ISO/IEC 15026, and safety standards such as AOP 52 and MIL-STD-882**
- **Have a roadmap of the body of knowledge**
  - Provide help to the engineers, program managers, and others on how to and what to apply to develop dependable systems
- **Making the accreditation more standard and visible**
- **Have a body of knowledge for assurance, in addition to having a breakdown of skill sets against roles**
- **Have cooperation with the IEEE Product Safety Engineering Society and other societies to build a safety-security accreditation program**

Possible milestones for five years and out

- Risk-decisions are made across all types of risk, risks throughout the lifecycle
- User high-quality software engineering methodologies
- Meet much higher expectations for dependability of systems (i.e., ultra-high dependability)—raise the bar

Themes for next workshop

- **Applying autonomic and biological computing (e.g., swarms) to address safety and security**
- **Certification of systems and people**
- **Roadmap—address what was brought up during the first workshop**
  - Relate safety and security to one another in the system-dependability context
  - Look into processes
- **Facilitation of communication between security and safety practitioners**

Things to do until the next workshop

- Identify interests of TC members
- Start a reading list
- Weekly posting of definitions and concepts for feedback—set up a wiki for the TC
- Invite papers that address integration of safety and security
- Put together a panel: Can safety and security be hooked up: Is there any relationship between the two?

To learn more…

- **Contact me about the upcoming workshop to be held later this year**
  - Take a brochure with you
- **Proceedings from first workshop available online**
  - http://bosun.nps.edu/uhtbin/hyperion-image.exe/NPS-CS-07-006.pdf