

## **General Disclaimer**

### **One or more of the Following Statements may affect this Document**

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.
- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.
- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.
- This document is paginated as submitted by the original source.
- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

# **A Software Safety Risk Taxonomy for Use in Retrospective Safety Cases**

Janice Hill  
NASA, Kennedy Space Center  
University of Florida  
Janice.L.Hill@nasa.gov

## **Introduction**

### **Safety Standards**

- **Contain Technical and Process oriented safety requirements**
- **Many varieties of Safety Standards, some addressing the system perspective, some just for software**
- **NASA programs/project will have their own set of safety requirements**
- **Industry operates similarly**

## **Introduction, cont.**

### **Safety Cases**

- Documented demonstration that a system complies with the specified safety requirements.
- Evidence is gathered on the integrity of the system and put forward as an argued case. [Gardener (ed.)]
- Problems occur when trying to meet safety standards, and thus make retrospective safety cases, in legacy safety-critical computer systems.

## **Risk Definitions, cont.**

### **Risk:**

A measure of the probability and severity of adverse effects.

### **Software Risk:**

The expected loss that can occur as software is developed, used or maintained. [Sherer]

OR

**Software Technical Risk:** A measure of the probability and severity of adverse effects inherent in the development of software that does not meet its intended functions and performance requirements. [CMU/SEI-96-TR-012]

## **Risk Definitions, cont.**

### **Software Safety Risk:**

**A measure of the probability and severity of adverse effects inherent in the development of software that does not meet *some set of software safety requirements*. [Hill]**

## **Software Risk Evaluation (SRE)**

- **Practice developed by the Software Engineering Institute (SEI)**
- **Formal method for identifying, analyzing, communicating, and mitigating software technical risk.**
- **The Software Development Risk Taxonomy is a construct of risk management that contributes to the SRE practice.**

## **Software Development Risk Taxonomy**

- **Follows the life cycle of software development and provides a framework for organizing data and information.**
- **The taxonomy-based identification method provides the organization developing software with a systematic interview process with which to identify sources of risk.**
- **The taxonomy construct consists of a Taxonomy-Based Questionnaire and a process for its application.**
- **The taxonomy methodology is an instrument with which one can obtain a broad, system level view of risks.**

## **Building and Using the Software Safety Risk Taxonomy**

- ***Safety* Elements and Attributes are added to the Software Development Risk Taxonomy.**
- **A *Software Safety* Taxonomy Based Questionnaire (TBQ) will be used to interview participants on the activities and tasks involved with the maintenance and reuse of legacy real-time *safety-critical* computer systems.**
- ***Software Safety* risk factors will be generated from the TBQ.**

## **The Software Safety Risk Taxonomy**

- **The Software Safety Risk Taxonomy maps the characteristics of *safety-critical* software development and *safety-critical* software, or *software safety* risks.**
- **Additionally, the Elements and Attributes of the new taxonomy maps closely to the requirements of the NASA Software Safety Standard.**

**Questions?**