# Safety Metrics for Human–Computer Controlled Systems

## Final Report (Year 1)
## Center Software Initiative

Nancy G. Leveson and Iwao Hatanaka
Massachusetts Institute of Technology

December 16, 2000

As deliverables on this grant for the first year, we promised a survey and evaluation of current accident models and requirements for an "integrative model" (which we now call a "holistic" model), a preliminary proposal for the conceptual framework of an integrated (holistic) accident model, and an end of year report (this report) including a plan for further development and evaluation. As the first two deliverables were part of a master's thesis, we have combined them into one report and are enclosing the thesis to satisfy these two deliverables. In fact, the thesis goes beyond the specified deliverables and outlines the framework for a new model, which was to be part of the second year deliverables.

Although this first year report was supposed to include a plan for the next year, the change in emphasis in the program and our decision not to go for a second year of funding makes that part of the final report meaningless.

## Executive Abstract of Thesis

The rapid growth of computer technology and innovation has played a significant role in the rise of computer automation of human tasks in modern production systems across all industries. Although the rationale for automation has been to eliminate "human error" or to relieve humans from manual, repetitive tasks, various computer-related hazards and accidents have emerged as a direct result of increased system complexity attirbuted to computer automation. The risk assessment techniques utilized for electromechanical systems are not suitable for today's software-intensive systems or complex human-computer controlled systems.

This thesis proposes a new systemic, integrated model-based framework for analyzing risk in safety-critical systems where both computers and humans are controlling safety-critical functions. In order to understand the basis for accidents in today's complex systems, we first investigated the root causes of recent accidents such as the Ariane 5 explosion, the Titan IVB Centaur failure, the Mars Climate Orbiter mishap, and the Mars Polar Lander mission failure. Traditional risk assessment approaches and classic accident models were then studied to survey the existing methodologies and techniques with respect to analyzing risk factors and estimating risk.

Building on this foundation, we defined a model-based framework for a new holistic systems accident model to improve the engineers' ability to assess and reduce risk in the design, development, and operations of complex human-computer systems. The impetus for this systems accident model-based framework was to identify risk factors early in the system design process by considering systemic factors, system attributes, and system processes. Rapid growth in technology today is altering the way in which complex systems must be designed and operated. Projects using our new holistic framework can potentially reduce risk by adhering to systematic design principles and processes. With this upstream, top-down approach, the framework can identify root causal factors and detect potentially detrimental aspects of design decisions and assumptions, organizational culture, management policies, regulations, technology strategy, and system development processes before they lead to accidents. The knowledge gained from the upstream influences and drivers is infused throughout the system design process and is reflected in the resulting system.

To demonstrate the process, the holistic framework is applied to a case study of an experimental NASA robot to service the heat-resistant tiles on the Space Shuttle between launches. The holistic framework for risk assessment was applied to the Mobility and Positioning Software (MAPS) on the robot as well as the human-computer interface to this software and the robot as a whole. The identification and evaluation of MAPS system function hazards, root causes, design constraints, and mitigation factors, along with a viable MAPS human-machine interface design, demonstrate our approach.