Systems Safety Analysis Workshop: From Inductive to Deductive Techniques

David Kaber\textsuperscript{a} & Nancy Currie\textsuperscript{b}

\textsuperscript{a}Edward P. Fitts Department of Industrial & Systems Engineering, North Carolina State University, Raleigh, NC, UNITED STATES OF AMERICA;
\textsuperscript{b}NASA Langley Research Center, Hampton Roads, VA, UNITED STATES OF AMERICA

1. Theme

This workshop provides a survey of systems safety engineering processes and methods. Systems safety analysis techniques can be generally classified as inductive or deductive in methodology. Inductive reasoning involves projecting system failures or losses from sources of hazards in the workplace and mechanisms leading to exposures. Deductive methods involve hypothesizing a specific failure or loss state and deducing events/elements in the workplace that might cause the failure. Systems safety techniques can also be classified in terms of stages of the system life cycle to which they are most applicable and impactful. The application of inductive and deductive methods occurs through a systems safety engineering process. This process includes a common approach to risk assessment and a hazard reduction sequence, including a precedence of engineering, administrative and personal protective controls. Such controls are identified through systems safety analysis techniques.

2. Objectives

The primary objective of the workshop is to train attendees on the methodology of specific inductive and deductive techniques, including: preliminary hazard analysis (inductive); failure modes and effects analysis (FMEA; inductive) and fault tree analysis (deductive). In general, these methods make the assumption that inherent dangers or hazard exposures exist in industrial, military, transportation systems and that effective approaches are needed for \textit{a priori} and real-time identification of the range of hazards and interactions that may exist. For example, FMEA is an engineering methodology used to identify and eliminate known and/or potential problems or errors in a system design or process before it reaches an operator. Related to this method, in order for one to know what safety is in a complex system, we must define what constitutes hazard exposure and failure. Structured systems safety analysis techniques are fundamental to this effort.

3. Target Audience and Method

The workshop is directed at practitioners with backgrounds in occupational safety engineering seeking to develop a formal understanding of the systems safety engineering process, hazard reduction technique, and specific hazard, failure mode and fault analysis techniques. These methods are considered fundamental to safe systems design and/or elimination of hazards in existing systems that may pose unacceptable risks to operators. The workshop provides an overview of the systems safety engineering process. Analysis techniques are classified in terms of reasoning approaches and the stages of the system life cycle. The common approach to risk assessment and hazard reduction sequence are covered. Coverage of specific systems safety techniques includes: definitions of relevant terms, identification of the scope of analysis, inputs, information transformation processes, and outputs. Outcomes of these methods range from control recommendations focused at specific system components, subsystems or entire systems with priority for engineering design over administrative mechanisms. Step-by-step method descriptions are provided along with detailed examples of use for real-world systems. Advantages and limitations of each method are also identified with some techniques focusing less on hazards due to interactions among subsystems, etc.

4. Expected Outcomes

Attendees will learn how to apply each systems safety analysis technique and how results can be used to prioritize use of safety resources in real-world hazard prevention or mitigation in systems that pose inherently dangerous energy transfers from a human perspective. Attendees will be able to compare and contrast methodologies in terms of required resources and outcomes as well as identify specific types of systems and processes to which each method is most applicable.