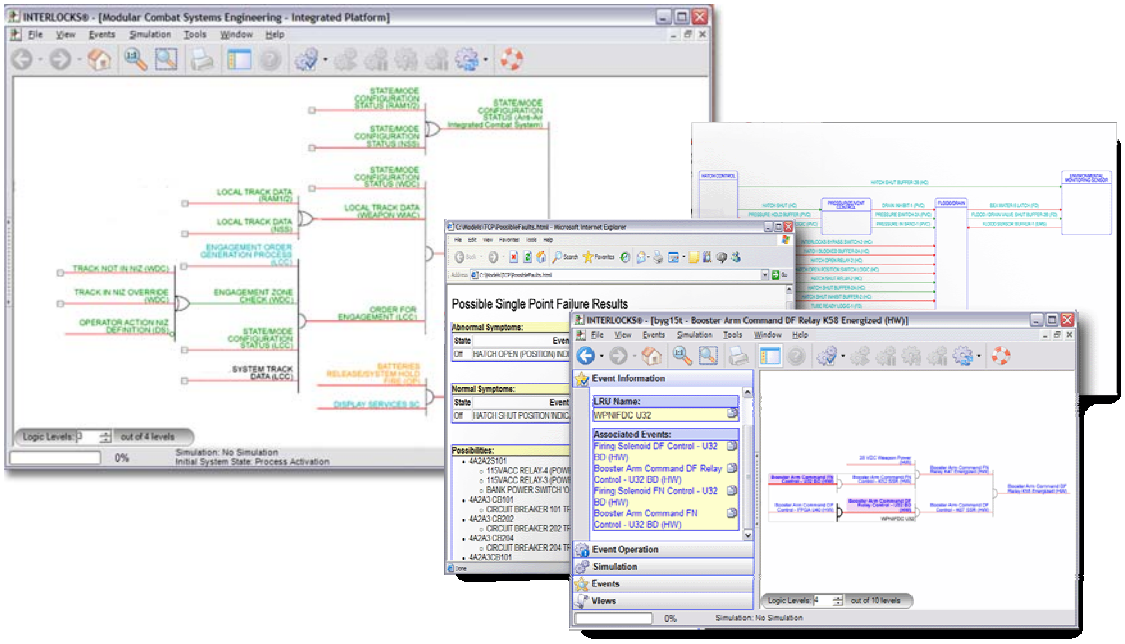
System and Software Safety Analysis

The practice of system and software safety is applied to complex and critical systems, such as commercial airliners, military aircraft, munitions and complex weapon systems, spacecraft and space systems, rail and transportation systems, air traffic control system and complex and safety-critical industrial systems. System safety analysis goals are to prevent, eliminate and control hazards and risks through design influences. As a subset of this discipline, software safety analysis ensures that software cannot contribute to a mishap or have a negative impact on the system's level of assurance. The whole concept of system safety and software safety is to influence safety-critical systems designs by conducting several types of hazard analyses to identify risks and to specify design safety features and procedures to strategically mitigate risk to acceptable levels before the system is certified.



INTERLOCKS® modeling and simulation tool combines the system safety requirements model and the architecture model. This combination provides a complete snapshot of the developing system and the safety positive measures being used for hazard prevention. INTERLOCKS promotes thorough software and system safety analysis by providing:

Analysis framework

INTERLOCKS modeling provides a disciplined approach to analysis. The scrutiny into the system required to simulate critical sequences of events is itself system and software safety analysis. The INTERLOCKS approach uses discrete event modeling to identify the positive measures and system controls being used to prevent a hazard from occurring. This lays the foundation and framework for subsequent safety analysis.

Requirements tracing

A large part of system and software safety analysis is the flow down of safety-critical requirements into the developing system. This includes correct implementation of the requirements into the system architecture. INTERLOCKS modeling and simulation tool captures the design and safety requirements at any phase of the development lifecycle. By combining the system safety model and the architecture model, INTERLOCKS demonstrates how hazard mitigation and the associated controls are being implemented.

Analysis capture and demonstration

System and software safety analysis is successful when the system is certified as meeting the defined safety requirements and ready for use. To achieve this goal, a diverse audience must be convinced that the system implements the necessary safety controls during all modes of operation. INTERLOCKS models the event sequences for each safety critical system process. It uses simple graphics to demonstrate system operation and failure cause and effect. The safety case is captured within a complete system model that has the added benefit of demonstrating how the designed positive measures prevent a mishap from occurring.

Analysis status check

With INTERLOCKS modeling and simulation tool, the system model is your safety analysis. It demonstrates completeness and current findings in a concise and interactive manner. You can depict a defined sequence of events and its safety controls operating as designed- or conversely, failing to perform as required. The fault isolation algorithms demonstrate system vulnerabilities and identify if something is wrong—either with the analysis or with the system itself.