



## Fault Analysis

The determination of how well the system controls potential hazards is a central part of any system and software safety analysis. Several fault analysis tools have been developed based on failure modeling (e.g. fault tree analysis, event tree analysis) to identify the possible failures that could contribute to such a mishap.

The INTERLOCKS® approach differs from traditional fault analysis tools and models the normal safety-related operation of the system. It captures all aspects of the system that control hazards (hardware, software, operator actions) into a discrete event logic model.

The screenshot displays the INTERLOCKS software interface. On the left, a window titled 'Possible Single Point Failure Results' shows a list of 'Possibilities' including components like '4A2A2S101', '115VAC RELAY-4 (POWER)', and 'CIRCUIT BREAKER 101 TRIP'. The main window, titled 'INTERLOCKS® - [byg15t - Booster Arm Command DF Relay K58 Energized (HW)]', shows 'Event Information' for 'WPNIFDC U32'. It lists 'Associated Events' such as 'Firing Solenoid DF Control - U32 BD (HW)' and 'Booster Arm Command DF Relay Control - U32 BD (HW)'. On the right, a logic diagram shows the flow of events, with nodes like '28 VDC Weapon Power (HW)' and 'Booster Arm Command DF Relay K58 Energized (HW)'. The bottom status bar indicates 'Simulation: No Simulation' and 'Logic Levels: 4 out of 10 levels'.

The modeling and simulation tool automatically analyzes all paths of system operation to find potential failures. Any inadequate safety controls and system failures are identified to the individual casual factor. The findings report details the system operational state, the potential hazard event(s), and all possible faults and initiating events that could inadvertently cause the mishap to occur. The interactive logic diagrams provide the analyst with detailed understanding of system behavior by depicting and emulating the results of the identified failures.