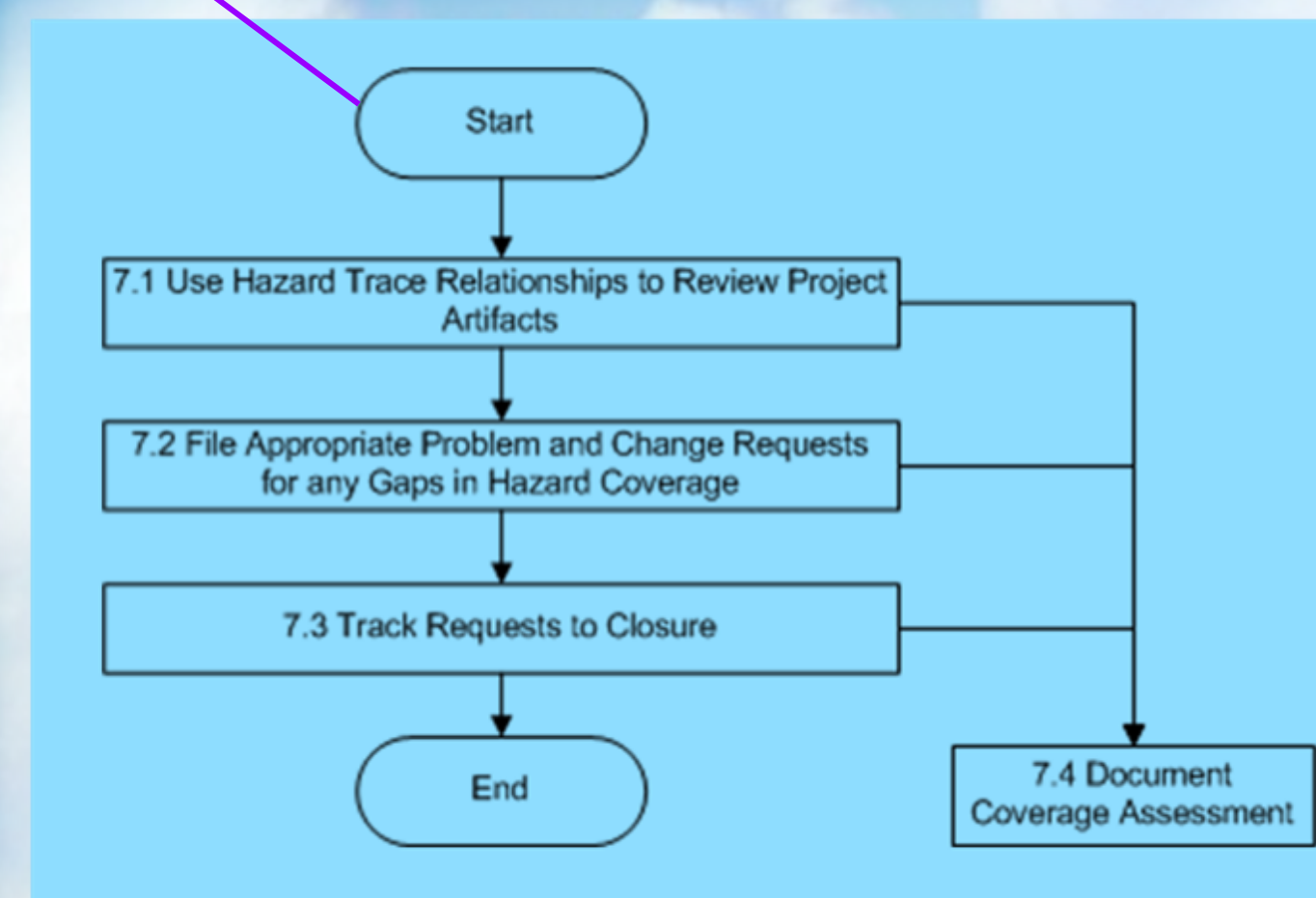
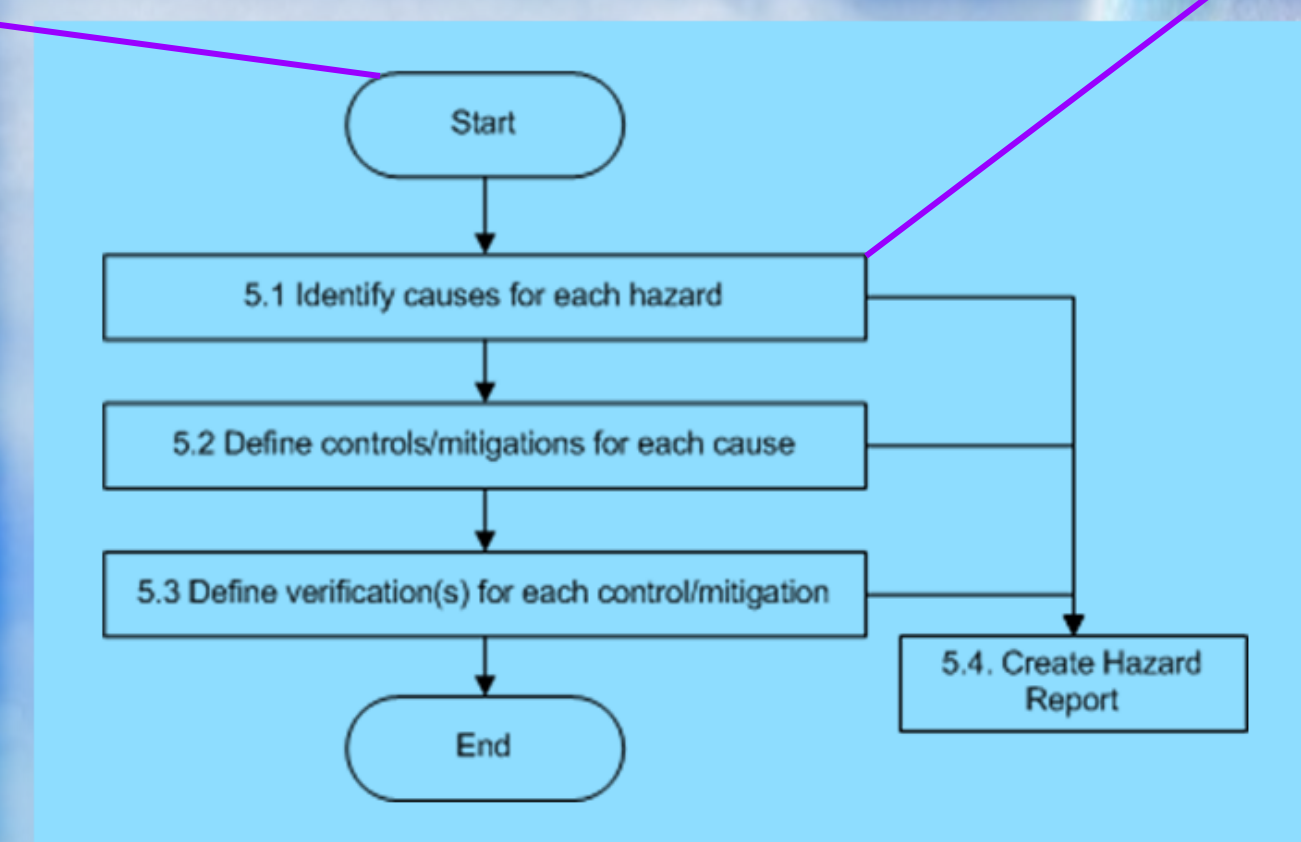
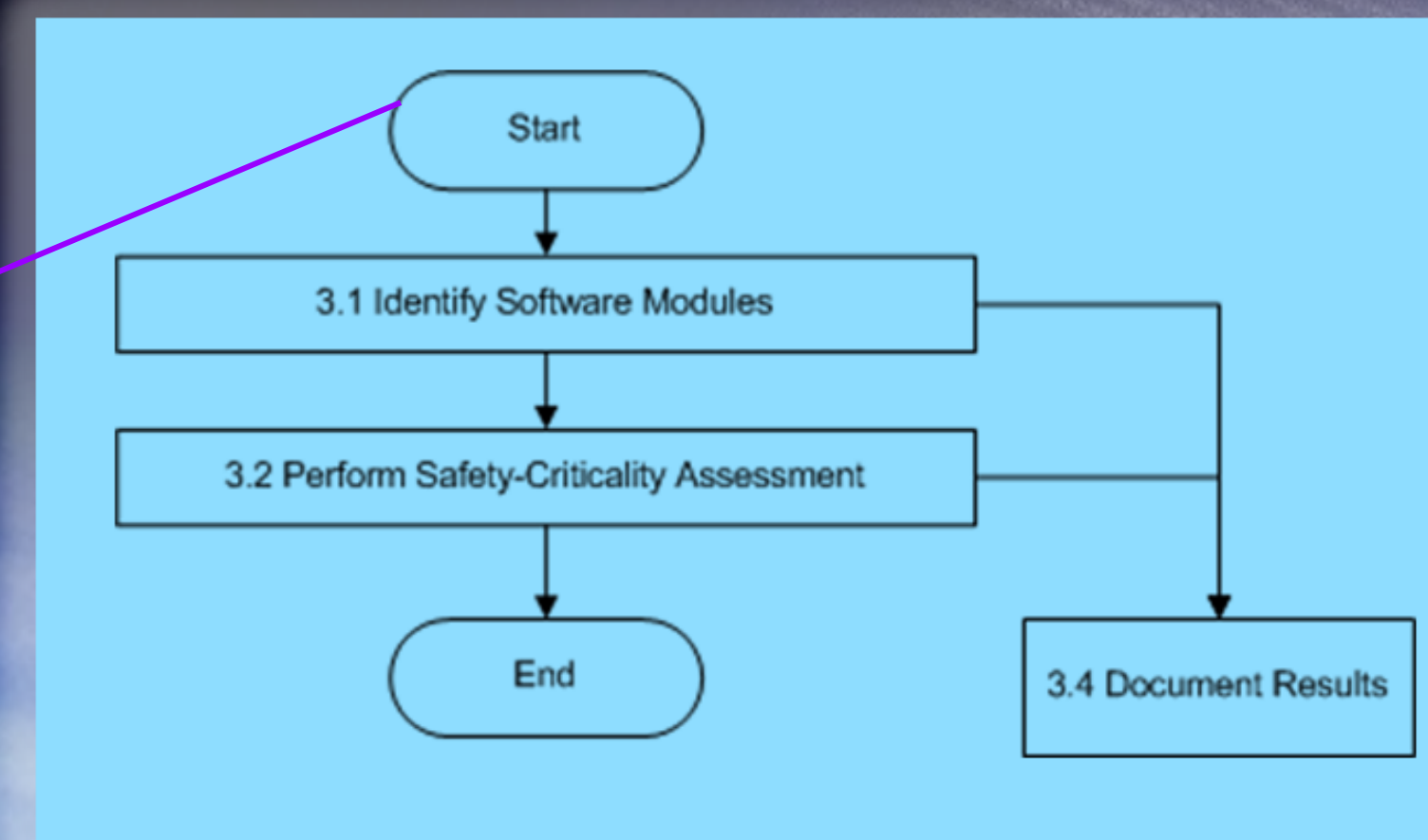
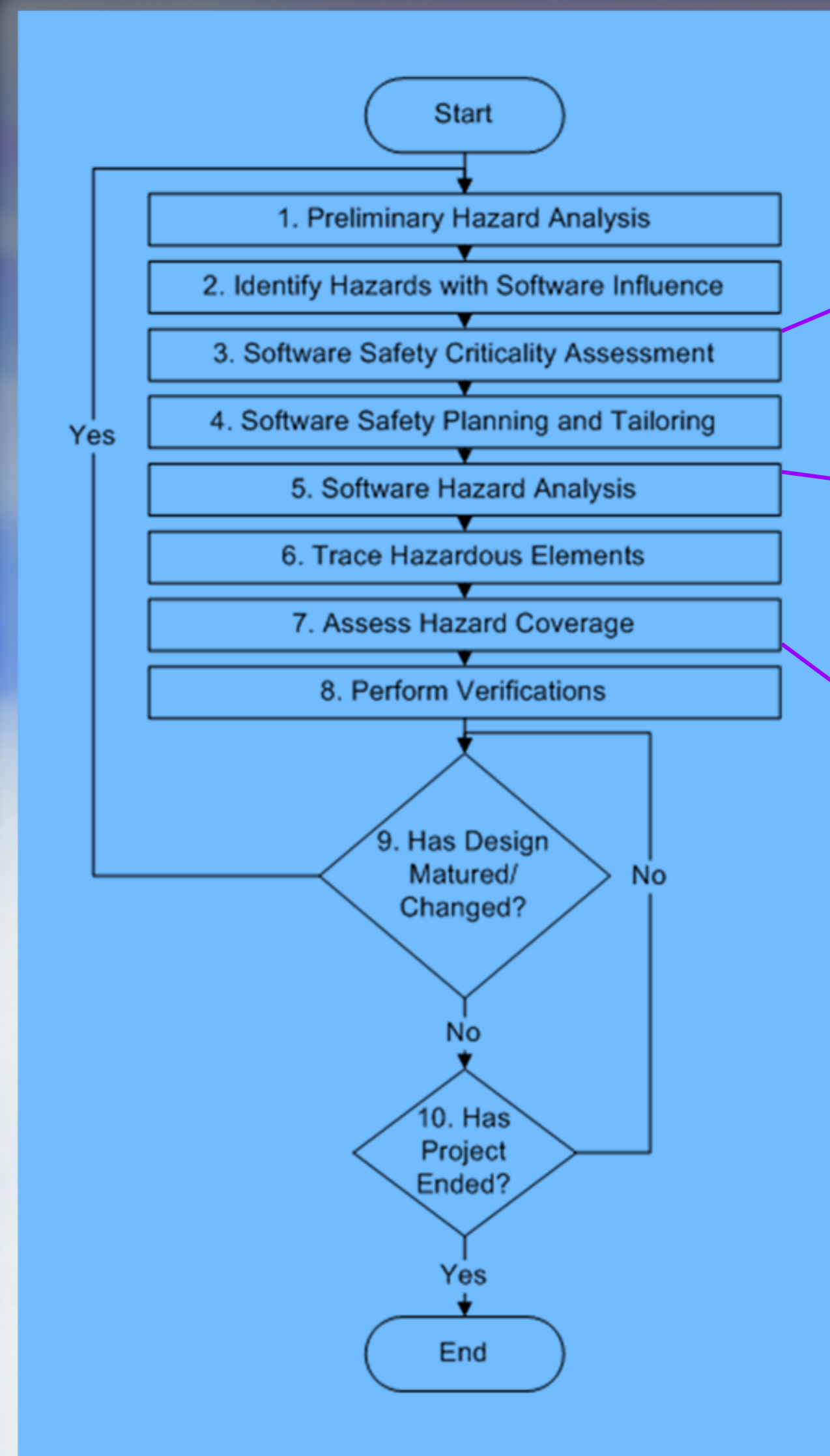


NASA Software Safety Process

(Visual Representation based on NASA Software Safety Guidebook)



- Process for discovering possible failures and faults for hazards with software influence

Process
Perform a FTA on each hazard with software influence. Perform at system level. Time permitting perform FMEA, ETC...

Outputs (from SA Std products table)
List of causes for each hazard

5.1 Identify Causes for Each Hazard

Purpose
Identify all possible failures and faults that could cause hazards with software influence.

Driving Requirements
NPR 8715.3C
2.5.2.2 System engineers shall:
a. Ensure that system safety models use systematic, replicable, and scenario-based techniques to identify hazards, to characterize the risk of accidents, to identify risk control measures, and to identify key uncertainties (Requirement 32122).
f. Maintain an up-to-date database of identified hazards, accident scenarios, probabilities and consequences, and key uncertainties throughout the life of the program (Requirement 25093).
NASA-STD-8719.13B
4.2.1.1 Identified hazards associated with a specific requirement, design concept and/or operation shall be evaluated for software's contribution to hazard causes, controls, or mitigations.
4.2.2.1 Identified software safety requirements and software hazard causes, contributors, and controls shall be recorded in an appropriate document and referenced in a safety plan. The requirements are usually documented in a section of the software requirements specification. The safety plan can be part of a system safety plan, a software management development plan, a software or system assurance plan, or when warranted, in a standalone software safety plan.

Roles/Responsibility
Systems Engineer (Responsible)
Software Safety Engineer (Responsible)
Subject Matter Expert (Support)

Inputs

- PHA
- List of hazards that may be influenced by software



The SMA Support Office is gathering software safety best practices and documenting the detailed steps to be distributed to help improve the practice. This poster describes the framework chosen to capture and communicate this information.