The SSHA documents how the software performs its intended function safely. It does this by:

- Ensuring that the safety design criteria identified in the software requirement specifications have been satisfied and
- Ensuring that the implementation choices have been evaluated so no unsafe conditions have been introduced.

3.4 Other Considerations

- The PO must refer to the program-specific Program Safety Plan (PSP) approved by the ATO Chief Safety Engineer to determine which safety assessments must be conducted during a system acquisition.
    - The PO may use methods other than SSHA to capture required information or may prepare a combined SSHA / System Hazard Analysis (SHA) to meet AMS requirements only if such alternatives have been approved in the PSP.
- The system safety process is a set of analyses that starts at the PHA and continues through the SSHA, SHA, and Operating and Support Hazard Analysis. Each analysis gets more discrete as more design details are known.
    - The basis of each analysis is a Hazard Analysis Worksheet (HAW). The HAW, initially developed early in the system lifecycle (i.e., during the PHA), is further developed, modified, and enhanced as subsequent analyses are conducted.
    - Each subsequent analysis has a slightly different focus but is essentially a HAW that builds on a previously developed HAW.
    - An SSHA is considered to be an update to the previous SRM document prepared for the acquisition system.
- SSHAs are developed for new systems; however, many acquisition programs deploy their capabilities incrementally over time and have an Initial Operating Capability date for each capability. In lieu of a new SSHA, additions to previously developed systems may require either updates to existing SSHAs, supplemental hazard analyses, or new hazard analyses. The specifics of such analyses must be defined in the approved PSP.
- Using a Commercial Off-the-Shelf (COTS) product with a very high reliability as a sub-system or component of a sub-system will not automatically ensure a safe system, as reliability does not account for interactions with other system components. This is particularly important to remember with software because it usually controls many, if not all, of the interactions among system components. Simply equating software reliability or specification conformance with safety will not ensure an acceptable safety level of the system. There may be times when it is less expensive and safer to provide special-purpose software rather than a COTS product; using COTS may amount to a false economy.
- There are other times where COTS components may have adequate system safety. In these cases, the producer of that component must provide the prime contractor with either a complete “black box” behavior specification or an analysis that shows the component design allows protection against any possible hazardous software behavior. This information must be provided for a complete SSHA to be performed.