Criticality Assessment Definitions
(Ref. MIL-STD-882E)

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

SOFTWARE CONTROL CATEGORIES		
Level	**Name**	**Description**
1	**Autonomous (AT)**	Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard.
2	**Semi-Autonomous (SAT)**	Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence.
3	**Redundant Fault Tolerant (RFT)**	Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault-tolerant mechanisms for each defined hazardous condition.
4	**Influential**	Software generates information of a safety-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap.
5	**No Safety Impact (NSI)**	Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data.

DoD_MIL-STD_882E

Assessment – Severity vs. Criticality

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SCC	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

The Software Criticality Index of 1 through 5 dictates the Level of Rigor requirements for the specific function.

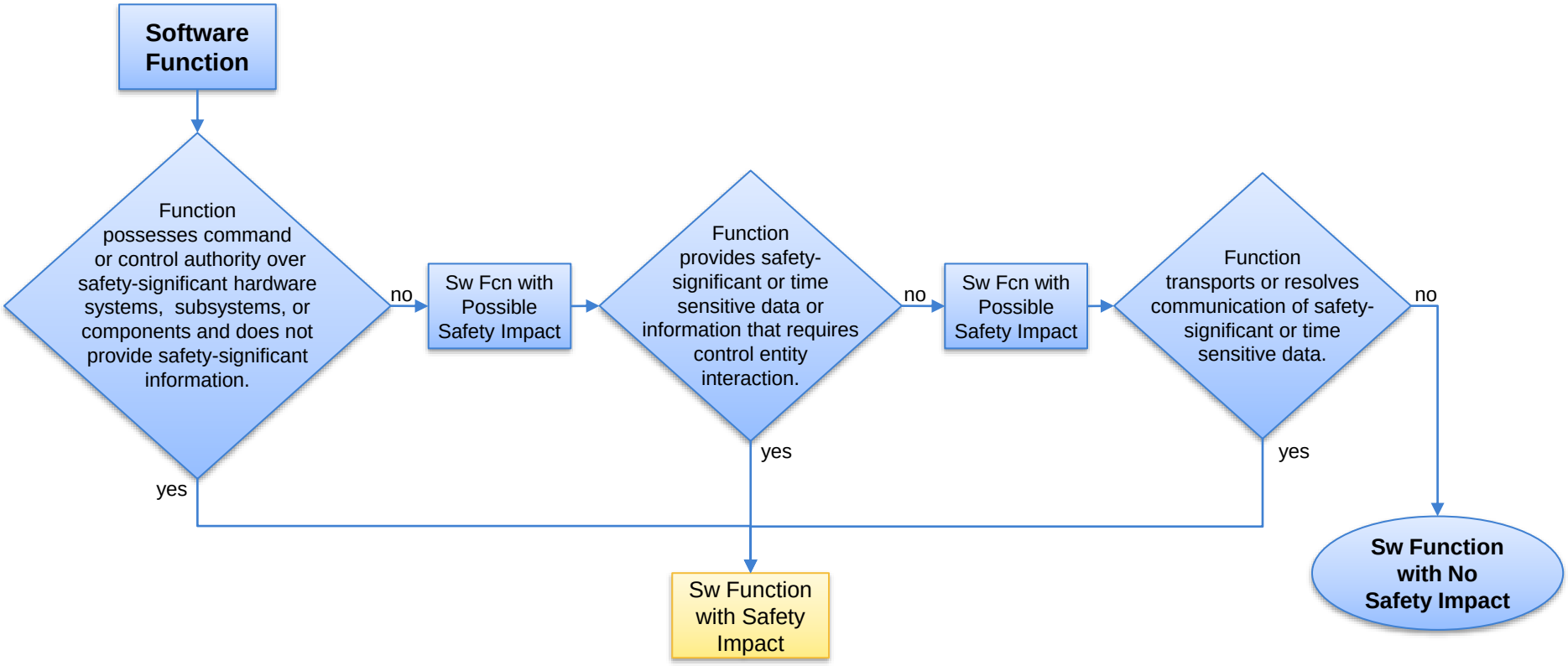
Assessment

- **TABLE VI. SwCI, risk level, LOR tasks, and risk***

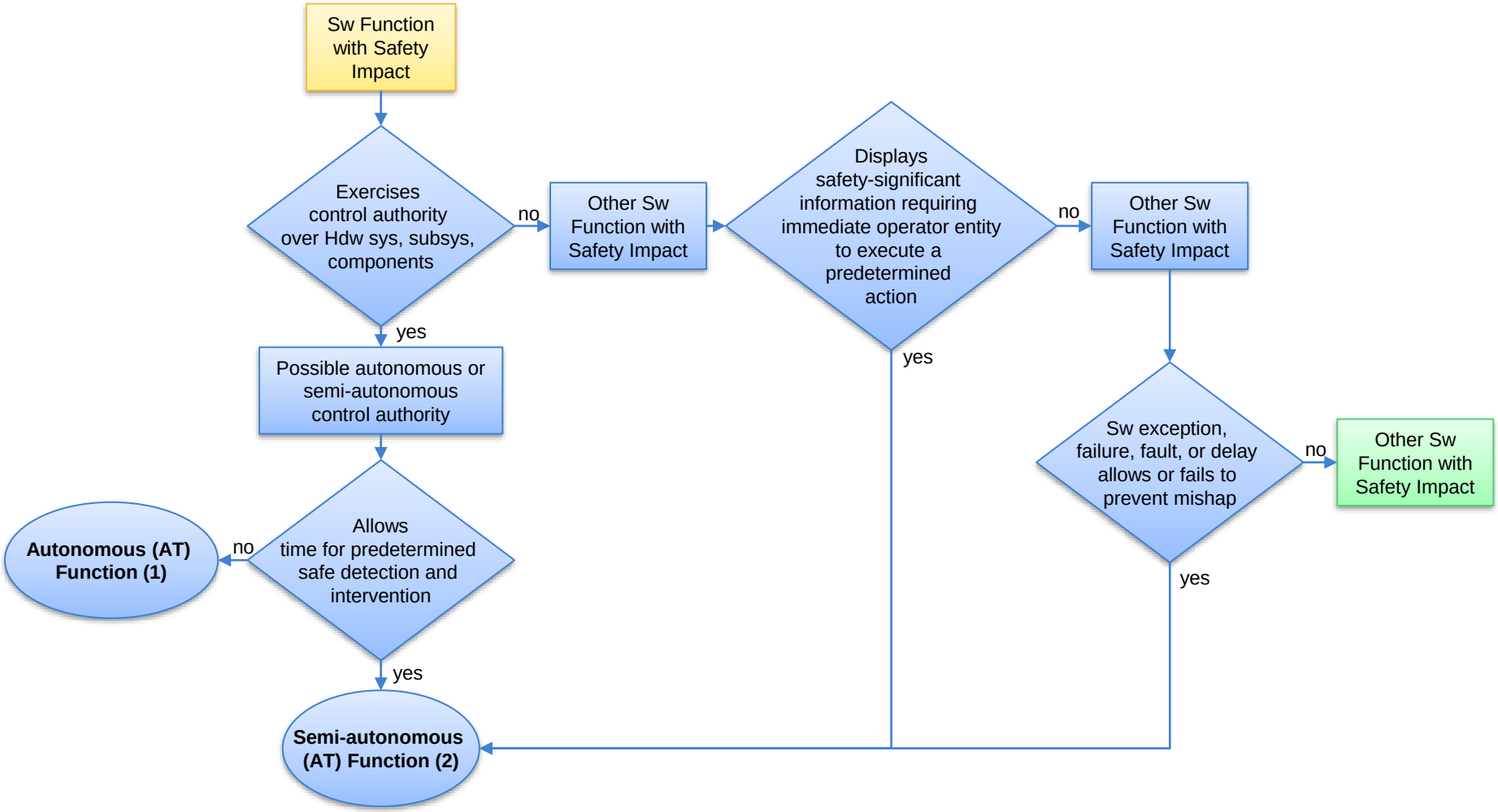
RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LOR Tasks, AND RISK		
SwCI	**Risk Level**	**Software LOR Tasks and Risk Assessment**
SwCI 1	**High**	If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 1 LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
SwCI 2	**Serious**	If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 2 LOR tasks or prepare a formal risk assessment for acceptance of a SERIOUS risk.
SwCI 3	**Medium**	If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 3 LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
SwCI 4	**Low**	If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 4 LOR tasks or prepare a formal risk assessment for acceptance of a LOW risk.
SwCI 5	**Not Safety**	No safety-specific analyses or testing is required.

***DoD_MIL-STD_882E**

Software Control Categories (SCC); MIL-STD-882E Decision Flow Developed by APT Research, Inc.



Software Control Categories (SCC); MIL-STD-882E Decision Flow Developed by APT Research, Inc.



Software Control Categories (SCC); MIL-STD-882E Decision Flow Developed by APT Research, Inc.