Appendix E

System Safety Principles

System Safety Principles	• System safety is a basic requirement of the total system. • System safety must be planned - Integrated and comprehensive safety engineering effort - Interrelated, sequential, and continuing effort - Plan must influence facilities, equipment, procedures, and personnel - Applicable to all program phases - Covers transportation and logistics support - Covers storage, packaging, and handling - Covers Non-Development Items (NDI). • MA provides management of system safety effort Managerial and technical procedures to be used must be for MA approval. - Resolves conflicts between safety and other design requirements - Resolves conflicts between associate contractors. • Design safety precedence: - Design to minimum hazard - Use safety devices - Use warning devices - Use special procedures. • System Safety requirements must be consistent with other program requirements. Performance, cost, etc., requirements may have priority over safety Requirements. • System analyses are basic tools for systematically developing design specifications. Ultimate measure of safety is not the scope of analysis but in satisfied Requirements. - Analyses are performed to: ▪ Identify hazards and corrective actions ▪ Review safety considerations in tradeoffs ▪ Determine/evaluate safety design requirements ▪ Determine/evaluate operational, test, logistics requirements ▪ Validate qualitative/quantitative requirements have been met. - Analyses are hazard not safety analyses

	• Level of risk assumption and criteria are an inherent part of risk management. • Safety Management - Defines functions, authority, and interrelationships - Exercises appropriate controls. • Degree of safety effort and achievements are directly dependent upon management emphasis by the FAA and contractors. • Results of safety effort depend upon MA clearly stating safety objectives/requirements. • MA responsibilities: - Plan, organize, and implement SSP - Establish safety requirements for system design - State safety requirements in contract - Requirements for activities in Statement of Work (SOW) - Review and insure adequate and complete system safety program plan (SSPP) - Supply historical data - Review contractor system safety effort/data - Ensure specifications are updated with test analyses results - Establish and operate system safety groups. • Software hazard analyses are a flow down requirements process followed by an upward flow verification process • Four elements of an effective SSP: - Planned approach to accomplish tasks - Qualified people - Authority to implement tasks through all levels of management - Appropriate manning/funding.