1. Purpose

This commentary includes additional information that was not captured in any other portal documents, but is believed that a brief further discussion is of value. This commentary covers the following topics:

1. Using the document templates
2. Safety Control Authority and inhibit strategy
3. Software (Sw) hazard analysis, Sw safety criticality matrix, and verification and validation
4. Hazard assessment deliverable reporting and submittal
5. ISO 9001/AS9100 and AFSPCMAN 91-710 Range Safety Requirements

2. Using the Document Templates

Within the system safety document portal are various required deliverable templates. These templates are included to provide an example of a possible deliverable format. If the Range User chooses to use any of these templates as a deliverable format, it is recommended that the pertinent volume and section of the AFSPCMAN 91-710 be thoroughly reviewed and be used as a reference for populating the template sections and subsections, or adding new sections or subsections to the document, as needed. The provided template examples are by no means complete; therefore the Range User should thoroughly review the AFSPCMAN 91-710 sections as the driver for document completion.

Within each template are italicized [*Guidance: comments*]. These are included as simple additional guidance and recommendations that can be used to complete the deliverables.

3. Safety Control Authority and Inhibit Strategy

USSF has expanded Range User responsibilities with respect to Safety Control Authority (SCA). The SCA is discussed in AFSPCMAN 91-710, Volume 1. USSF requirements for hazard assessment, hazard severity classification, safety critical definition, and inhibit design strategy remain unchanged. This section provides guidance in the interpretation of design and risk assessment requirements associated with Range User SCA responsibilities.

The 2019 release of AFSPCMAN 91-710, Volume 1 provided expanded Launch Complex SCA to individual Range Users. It reassigned Launch Complex SCA from Space Launch Delta (SLD) Safety to the Range User. Volume 1 stated that:

> 1. *"Range Users are fully responsible for the safety and health of their employees in leased/licensed launch complexes and facilities, in accordance with Occupational Safety and*

Health Administration (OSHA) regulations, standards and other federal and state safety and health regulations."

2. *"This responsibility extends to government employee visitors when present in those leased/licensed facilities, similarly to when visiting off-base contractor installations."*

3. *"Wing* [SLD] *Safety will continue to have oversight of unique hazards not covered by OSHA and hazardous operations with potential to endanger beyond the boundaries of the launch complex."*

In addition to changes in AFSPCMAN 91-710 Volume 1, the 2019 release of AFSPCMAN 91-710, Volume 3 (paragraph 1.1.2), provides that: *"When government and third party personnel, government resources and/or shared resources with commercial entities are not involved or exposed to hazards from an operation, or when Range User activities are contained within the boundary of their operations space and do not impact areas outside of their control, deviation from these requirements through the tailoring process is permitted."*

These expanded SCA responsibilities from Volume 1, in conjunction with expanded allowance for tailored deviations from the design requirements of Volume 3, has led to the interpretation that there is acceptance for redefining 'safety critical' processes and/or a deviation from the baseline Volume 3 design inhibit requirements. Both of these interpretations are <u>incorrect</u>.

The Range User is responsible for providing design information, hazard analyses and potentially hazardous procedures to SLD Safety for the following:

1. systems which have unique hazards not covered by OSHA and

2. systems/subsystems/facilities/GSE/MHE/operations which, if they fail at any time, can result in a hazard going beyond the fence line.

This will then allow SLD Safety to verify whether these systems/subsystems/facilities/GSE/MHE/operations are compliant with AFSPCMAN 91-710 requirements.

Launch area safety requirements listed in Volume 1, paragraph 3.3, state: *"The ranges shall ensure that all personnel and USAF* [USSF] *or third party resources located on any AFSPC range, including CCAFS or VAFB or on any supporting site within the ER and WR, are provided an acceptable degree of*

protection from the hazards associated with range operations." Acceptable means compliance with AFSPCMAN 91-710 requirements or an equivalent level of safety meeting the baseline risk established by AFSPCMAN 91-710.

Launch area safety and launch complex hazard consequence and probability categories, correlated to different levels of acceptability for prelaunch hazards not associated with launch or Launch Safety launch commit criteria, are listed in Table 3.2 of Volume 1, and reviewed below:

1. Hazard severity is determined through the safety hazard analysis process. Hazard analysis hazard severity classification (Catastrophic, Critical and Marginal) determines the level of inhibit strategy required per Volume 3 (paragraph 3.2):

    a. Catastrophic: three inhibits (dual fault tolerant),
    b. Critical: two inhibits (single fault tolerant),
    c. Marginal: since inhibit (no fault tolerant).

2. Special attention is directed to 'Risk Priority' in Table 3.2, which correlates mishap risk probability to operation permissibility (Unacceptable, Waiver required, ELS required or Permitted). The Equivalent Level of Safety (ELS) is the determinant within the scope of 'Risk Priority' that is allowed for in Volume 3, paragraph 1.1.2.

3. For systems/hazards/operations not covered by OSHA regulations, if the failure's resultant hazards are contained within the operator's boundaries, the appropriate number of AFSPCMAN compliant inhibits, based upon the hazard severity level shall be provided.

4. Software (Sw) hazard analysis, Sw safety criticality matrix, and verification and validation

Ground computer systems and software processes are covered in AFSPCMAN 91-710, Volume 3, Chapter 16, Computer Systems and Software. The requirements are used to control and/or monitor operations identified as "safety critical", and the software safety effort shall be an integral portion of the Range User system safety program. As stated in Volume 3, the relationship between the software safety effort and the other elements of the system safety program will be addressed in a program-specific System Safety Program Plan (SSPP). These requirements are intended to be used in conjunction with the system safety hazard analysis process specified in AFSPCMAN 91-710 Volume 1, Attachment 3, and as detailed in the Range Users' SSPP.

Chapter 16 was written based on lessons learned to address the most common issues that have been encountered in the past with software development and implementation. Chapter 16 uses the MIL-STD-882E - System Safety[1], the Joint Software Systems Safety Engineering Handbook (JSSSEH)[2], the JS-SSA-IG - Software System Safety Implementation Process and Tasks[3] (implementation guide), as well as including specific test and verification and validation (V&V) requirements.

Acquisition Programs unfamiliar with software safety find it difficult to extract software safety techniques and processes in order to satisfy MIL-STD-882E Software Level of Rigor (LOR) requirements and will often default to only referencing or reusing the LOR table from MIL STD 882E (Table V) as their software safety approach in their System Safety Program Plans (SSPPs)[4]. The MIL STD 882E references consultation with the JSSSEH, which contains detailed guidance for software safety. The JSSSEH includes specific details, but not in a specific location.

The implementation guide provides implementation guidance for Software System Safety program requirements specified in MIL STD 882E and guidance detailed in the JSSSEH using implementable process task requirements that are presented as a decomposition of parent and children activities, similar to a Work Breakdown Structure (WBS), as Tasks and Subtasks (i.e. from the development of a System Safety Management Plan, to the identification of Software Significant Functions (SSF), to the Assessment of Safety Risk, etc.)

Appendix A of this document is a LOR task table that should be used to develop the defined process tasks necessary to meet MIL-STD-882E Table V LOR requirements. The LOR task table also supports accomplishment of the MIL-STD-882E Tasks. The LOR can also be assessed for tailored implementation for any given program, and tailoring is permitted as long as the tailored LOR tasks are approved by both the Range Safety and the Range User. (Reference SEAL-SSD-006, Tailoring Example.)

Critical to the Software System Safety process are the identification of Software Control Categories (SCC), software criticality indices (SwCIs), and the safety-significant software functions (SSSF) that may contribute to software mishap risk. SSSF are those that are safety-critical and safety-related.

1. MIL-STD-88E System Safety, DoD Standard Practice. 11 May 2012.
2. Joint Software Systems Safety Engineering Handbook, Version 1.0. DoD. August 27, 2010.
3. JS-SSA-IG, Rev. B. Software System Safety - Implementation Process and Tasks Supporting MIL-STD-882E. Joint Services - Software Safety Authority. 14 March 2018.
4. Robert E. Smith, CSP. Joint Software Systems Safety Engineering Handbook Implementation Guide Presentation. 20th Annual NDIA Systems Engineering Conference. 25 October 2017.

Lastly, on the topic of software is the approach to hazard analysis. Each credible software SSSF shall have the required number software inhibits (or controls) based on the associated hazard severity (see section 3 above). Software mitigations to SSSF should not depend on mechanical inhibits, as this would indicate that the software would be allowed to initiate a credible mishap, unmitigated; therefore, the inhibits/controls should be within the software logic (i.e, not relying on say, RV setting, prop tank FS, etc.). These latter mechanical inhibits are still required, but are inhibits for the mechanical side of the hazard (i.e. failures in the pressure regulators, valves, flow controls, etc.).

5. Hazard assessment deliverable reporting and submittal

AFSPCMAN 91-710, Volume 1, Attachment 3, details the SLD30 System Safety Program Requirements. Specific Tasks under this section call out the requirements for Preliminary Hazard Analysis, Subsystem Hazards Analysis, System Hazard Analysis, and Operating and Support Hazard Analyses, with the following deliverable schedule:

- PHA shall be submitted to Range Safety at least 45 days prior to the cDR or equivalent program design activity.
- Range User shall submit their plan for developing their SSHA at the PDR or equivalent program activity. The Range User shall submit a draft of their SSHA 45 days prior to the CDR or equivalent program activity.
- The Range User shall submit their plan for developing the SHA at the PDR or equivalent program activity if a PDR is not held. A draft SHA shall be submitted 45 days prior to the CDR or equivalent program activity if a CDR is not held. The final SHA shall be provided with the final MSPSP
- The Range User shall submit their plan for developing their O&SHA submittal at the PDR or equivalent program activity if a PDR will not be held. A draft O&SHA shall be submitted 45 days gprior to the CDR or equivalent program activity if a CDR will not be held.

An often asked question is how best to submit the hazard analysis, whether a single report for each of can individual analysis be submitted as they are completed. A possible approach is to develop a top level document that describes the methodology used to develop each hazard analysis at the pertinent stage of development (Reference SEAL-SSD-012/013/014) with the associated hazard risk assessment process. Then the individual hazards analyses can be submitted in sequential fashion, traceable preferably through the MSPSP, FSDP and GOP.

6. ISO 9001/AS9100 and AFSPCMAN 91-710 Range Safety Requirements

Most aerospace companies engaging in launch services with the US Space Force are certified to ISO 9001 Quality Management Systems, or the aerospace standard AS9100, or plan to become certified. Certification to either system recognizes the organization as meeting the requirements for the implementation of a Quality Management System (QMS), having the policies, processes, and procedures necessary to provide products and services to meet customer and regulatory needs.[5]

The AFSPCMAN 91-710 Range Safety Requirements are a set of safety related requirements that form the basis of the Range Users safety management system. This safety management system is defined by the Range Users' System Safety Program Plan, which emphasizes safety management as a fundamental business process.

The QMS is not a substitute for a safety management system, but the safety management system and the QMS are highly complementary and the QMS can be used as a tool to achieve the overall safety goals.[6] This is realized by understanding that the safety management system requirements, such as management review, analysis of data, corrective action, and internal audits have already been established in the QMS.

5. What is ISO 9001? https://advisera.com/9001academy/what-is-iso-9001/

6. Safety Management System (SMS). https://www.faa.gov/about/initiatives/sms/