SAE Aerospace
An SAE International Group

AEROSPACE INFORMATION REPORT

SAE AIR6027

Issued 2012-05

Considerations for Safe Store Operation on Manned and Unmanned Vehicles

RATIONALE

In discussions between SAE ASD committees and customers, it was apparent that there is a lack of common understanding of matters associated with the safety considerations applicable to weapon operation on aircraft. Although numerous safety standards exist, they cover only specific aspects of the subject and there are often misunderstandings on such matters as independence of functions, implementation of safety critical commands and ensuring that adequate safeguards exist where necessary. A short survey of members of AS-1B revealed that there is no single over-arching and comprehensive standardisation or description of the safety features applicable to weapon operation on aircraft, which would facilitate the design and implementation of safe systems.

This situation was made all the more apparent when AS-1B was requested by the JAUS committee (AS-4) for guidance in their work associated with adding weapon operation capabilities to Unmanned Ground Systems, or robots in the first place, with future consideration in Unmanned Aerial Systems.

This standard is intended to provide an overview of the established safety concepts generally employed on manned combat aircraft for safe operation and release of weapons and to provide recommendations for how these principles may be applied to the operation of weapons on other (unmanned) platforms or robots.

1. SCOPE

The information presented in this AIR is intended to provide designers of armed unmanned systems with guidelines that may be applied to ensure safe integration and operation of weapons on unmanned platforms. The guidelines have been developed from experiences gained in the design and operation of weapons on manned aircraft that have been accepted by relevant safety authorities in the USA and Europe and proven effective over many years. Whilst the guidelines have been developed from experience with aircraft operations, the concepts are considered equally applicable to non-aircraft systems, such as those used on the surface or undersea environments.

This document does not attempt to define or describe a comprehensive safety program for unmanned systems.

System Safety is a system characteristic and a non-functional requirement. It has to be addressed at each level of system design, system integration and during each phase of system operation. System safety is achieved when the system operation does not cause inadvertent personnel injuries, destruction of the system or damage to the environment.

Section 3 of the document contains an introduction to methods by which the safety of a system can be assessed.

Section 4 describes the safety principles commonly applied to the design and operation of weapons on manned aircraft.

Section 5 describes how the safety principles established for manned aircraft may be applied to unmanned systems,

Section 6 provides conclusions and recommendations.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

SAE values your input. To provide feedback on this Technical Report, please visit
http://www.sae.org/technical/standards/AIR6027

2. APPLICABLE DOCUMENTS

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

AS5725 Interface Standard, Miniature Mission Store Interface

AS5726 Interface Standard, Interface for Micro Munitions

ARP4754 Guidelines for Development of Civil Aircraft and Systems

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

2.2 IEEE Publications

Available from Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854-1331, Tel: 732-981-0060, www.ieee.org.

IEEE STD 1228-1994 Standard for Software Safety Plans

2.3 RTCA Publications

Available from Radio Technical Commission for Aeronautics Inc., 1828 L Street, NW, Suite 805, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

RTCA DO-178 Software Considerations in Airborne Systems and Equipment Certification

2.4 U.S. Government Publications

Available from the Document Automation and Production Service (DAPS), Building 4/D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Tel: 215-697-6257, http://assist.daps.dla.mil/quicksearch/.

MIL-STD-882 Standard Practice For System Safety

MIL-STD-1553 Interface Standard For Digital Time Division Command/Response Multiplex Data Bus

MIL-STD-1629 procedures for performing a failure mode, effects and criticality analysis (cancelled)

MIL-STD-1760 Aircraft/Store Electrical Interconnection System

MIL-HDBK 516 Airworthiness Certification Criteria

2.5 Other Publications

N. G. LevinsonA New Approach To System Safety Engineering

Various Authors System Software Safety Handbook (2010)

3. RISK ASSESSMENT, HAZARD ANALYSIS AND SOFTWARE SAFETY CLASSIFICATION

This section provides an overview of the analyses that must be carried out when designing the safety characteristics of a system. It should be noted that there are many documents containing guidelines and requirements applicable to system safety design for the operation of weapons on platforms. Adherence to any one document will not necessarily ensure compliance with others. Documents applicable to the operation of stores on platforms include: MIL-STD-882, IEEE STD 1228, SAE ARP4761 and SAE ARP4754.

In general, it is important that when designing the safety characteristics of any system, reference should be made to the complete set of safety documents relevant to the system. A common understanding of the set of required safety characteristic should be reached with the safety authorities. It should also be noted that there is likely to be more than one safety authority associated with the operation of stores on a platform. There may be separate authorities covering explosives and fuzing, store safety, platform safety, airworthiness and clearances for flying in controlled airspace in the case of air platforms. Each nation or armed service may have its own organization holding these authorities.

In addition, caution should be exercised in the use of terminology due to the lack of commonality across the documents. As an example, MIL-STD-882 Rev D contains very specific definitions of the words ‘hazard’ and mishap’ that are not necessarily contained in other relevant documents. As an example the banana peel is the hazard, slipping on it is the mishap. In this AIR, the term ‘failure’ is used to encompass all instances of the system not operating as expected, including mishaps or the arising of hazards that were (or were not) previously identified, as defined in MIL-STD-882.

The following paragraphs describe some of the approaches and processes commonly used when designing and assessing the safety characteristics of store operation on manned aircraft. They are offered for consideration when designing unmanned systems.

3.1 Risk Assessment Procedure

The system safety assessment is a continuous systems engineering process applied during the whole system life cycle. Hazard Analyses and Safety Assessments using different techniques, including software safety analyses, are performed on all system development levels to the level of rigor required to ensure robustness and correct operation of the system.

The first step in mitigating safety risks is early identification of failure modes to which the design of the aircraft and store system can contribute.

- Causes of potential failures are identified by a combination of activities: analytical methods, including, but not limited to Functional Hazard Assessments, Fault Tree Analysis, Failure Modes, Effects and Criticality Analysis,
- experience from legacy programmes, and
- identification of new failures and their causes during the development of the system.

Risk assessment is performed to establish safety risks to the weapon system caused by functional failure of system component(s) (which includes operator actions) or faults and failure conditions. Functional Hazard Assessments and Preliminary Hazard Analyses, and System safety assessments, using blended approaches and methods from SAE ARP4761, SAE ARP4754, MIL-STD-882, and IEEE STD 1228, when combined with effective system safety techniques should identify failure modes and enable risk mitigation. This is often through derived requirements that specify safety features in the design.

Safety Critical (SC) Functions associated with weapons ready, weapons solutions and/or release and control that are commanded, controlled and monitored by software will require a software safety effort using IEEE STD 1228-1994 or equivalent alternative methods.

Each (system) function must be evaluated with respect to the effect of the function failure on the mission, platform/personnel and environment. The principal failure modes are:

- Loss of function
- Provision of function when not required
- Provision of function incorrectly
- Hazardously misleading information that could lead to malfunction or human error

NOTE: MIL-STD-1629A (cancelled) provides more detailed failure modes:

- Premature operation
- Failure to operate at prescribed time
- Intermittent operation
- Failure to cease operation at prescribed time
- Loss of output of failure during operation
- Degraded output or operational capability
- Other unique failure conditions, as applicable, based upon system characteristics and operational requirements or constraints.

System boundary conditions are established to focus on the relevant activities within the system being analyzed. These activities may include operator actions, and some initial conditions, which best describe the system in a fault-free state. Initial conditions are therefore steady state events, which are normally expected and directly related to the circumstances for which the analysis (e.g., fault tree) is performed.

The effect of the failure on other subsystems must be considered, contributing factors (e.g., maintenance, operational, or environmental influences, etc.) including secondary failures, which may influence the mishap severity must be identified.

The determination of a mishap risk requires consideration of two aspects: the probability of occurrence and the consequences.

Consideration of the consequences of a mishap occuring usually assumes a number of levels of severity. The following levels are extracted from MIL-STD-882:

- Catastrophic: causing death and/or platform loss
- Critical: causing severe injury and/or major platform damage
- Marginal: causing minor injury and/or minor platform damage
- Negligible: causing less than minor injury and/or platform damage

Other standards may expand these definitions; for example, by taking into account the damage to the environment.

Table 1 provides an example of the approval authority required for acceptance of the combination of mishap probabilities and consequences:

TABLE 1 - MISHAP RISK ACCEPTANCE AUTHORITY

	Severity			
	Catastrophic	**Critical**	**Marginal**	**Negligible**
Probability				
Frequent (>= 10^{-1})				
Probable (<10^{-1} to >=10^{-2})				
Occasional (<10^{-2} to >=10^{-3})				
Remote (<10^{-3} to >=10^{-6})				
Improbable (<10^{-6})				

HIGH LEVEL ACCEPTANCE AUTHORITY

MEDIUM LEVEL ACCEPTANCE AUTHORITY

LOW LEVEL ACCEPTANCE AUTHORITY

3.2 Software Safety, Software Functions and Classification

Whilst hardware failures usually have a probability of occurrence, system failures caused by software do not: there either is or is not a software error. The integrity of software is controlled by the software development process, i.e., dependent on the criticality (or failure condition category) of a function realized in software, a software development class is determined, which specifies the application of the respective software development level (see also for example, RTCA DO-178). The mishap severity category "Catastrophic" will always require the highest software integrity level, regardless of the standard. For example DO-178B level A or DEF-STAN -00-56 SIL/SIR 4 is required for any software function that could contribute to a catastrophic failure condition/hazard. Levinson states that most of the system failures caused by software can be derived from failures in the respective requirement(s).

While following DO-178B provides some confidence in software assurance, development, and verification rigor it does little to ensure safety requirements and critical functions implemented in software are implemented correctly and function correctly to prevent, eliminate and control hazards. Safety and airworthiness qualifications and certification shall have objective evidence that software with complexity and criticality have been analyzed and verified from a safety perspective. The safety aspects of software and functions allocated under control of safety-critical software shall follow the industry standard for software safety as promulgated in IEEE STD 1228-1994. These include the following six standard tasks widely used.

1. Software Safety Requirements Analyses (establish safety functions implemented in software)

2. Software Safety Design Analysis (top level and architectural design)

3. Software Safety Design Analysis (detailed functional design)

4. Software Safety Code Analysis (selective at unit level, not pervasive)

5. Software Safety Test Analysis (to ensure test cases for safety verification)

6. Software Safety Change Analysis (to assess safety impacts of software changes)

It should be noted that for airworthiness (MIL-HDBK-516B) and safety aspects of software purposes, following IEEE STD 1228 will help yield objective safety evidence that can be used to meet risk, requirements and airworthiness/certification criteria. Additionally, the software safety analyses along with other detailed system safety documentation can be used in data package submittal to help satisfy the UK MOD and US DoD Ordnance Boards or equivalent. The US Navy Weapon System Explosive Safety Review Board (WSESRB) requires software safety work products be provided to the Software System Technical Review Panel (SSSTRP). The US Air Force Nonnuclear Munitions Safety Board (NNMSB), US Army Fuze Board and MoD Defence Ordnance Safety Group all require substantiating and objective evidence of acceptable safety risk on any weapons and often on the release and control aspects of those weapons. Therefore, if software has a significant impact on system functions, an appropriate software safety effort will be required.

For further considerations, it is helpful to distinguish between safety critical functions – in case of a failure, the function directly causes a catastrophic or critical mishap – and safety involved functions – a function, where failure can cause catastrophic, critical or marginal mishaps only in combination with other independent failure(s).

The determination of the classification required to develop safety critical software (e.g., per DO-178) could be enhanced by the introduction of functions or functional contributions realized in hardware: either a single or double software error causes a mishap or the combination of a software error with an independent event (hardware failure or wrong crew action) leads to the mishap. The latter combines e.g., hardware failure rates – the independent event – with software failures causing a specific mishap (i.e., a software error together with a hardware failure causes the loss of the aircraft). The combination of a hardware failure and software error is then transferred into a software safety classification level (see the System Software Safety Handbook for further reference). Where a function causes a specific hazard only in combination with another independent function, the safety criticality can be reduced.

As a core part of the safety assessment, the independence argument for software functions or software functions implemented together with hardware must be prepared.

Functional independence must be addressed and demonstrated for the following cases (Table 2):

TABLE 2 – FAILURE AND SECONDARY FAILURE POSSIBILITIES

Failure Source	Secondary Failure
Pilot or event	Hardware
Pilot or event	Software
Hardware	Software
Software	Hardware
Software	Software

a. Pilot/event and hardware are independent, because neither the hardware nor the pilot is affecting each other. Also environmental/operational events do not affect each other. This is e.g., true for a system, which is ergonomically designed and does not put additional workload on the pilot due to bad design.

b. Pilot/event and software are independent when software failures identified during the requirements hazard analysis does not reduce pilot abilities to perform actions. However, the ergonomics/procedural requirements are also valid for this case.

c. Hardware and hardware are independent, when a failure in hardware 1 does not affect hardware 2 (exclusion of common mode failures).

d. Software and Hardware are independent when a software failure does not cause a hardware failure and vice versa.

e. Software and Software independence is more difficult to determine. The demonstration of independence will be done firstly by establishing the software development process required by the software class, which has been determined based on the severity of a hazard a software failure could cause. Software development may consider the following processes to establish the independence argument:

   1. Diversity

      Independence of two software functions is determined top down, starting from the definition of fundamentally diverse functions, realized in software so that a common fault cannot cause both software functions to fail and therefore cause the hazard.

   2. Top down hazard analysis

      This must be done in order to prevent the diversity of functions by the software. This can be avoided if the hazard analysis is done starting from the requirements hazard analysis down to code level hazard analysis. The following questions arise.

      - are any signals/data common – does the corruption of a common signal cause a hazardous failure of both functions?
      - are software components common – does any combination of software failures cause a hazardous failure?
      - does the software share the same physical environment? For instance in cases where both software functions share the same processor and memory, a failure of the hardware would cause both software functions to fail. Thus the sharing of processor and memory is not an option for safety critical functions, two processor boards with their own memory have to be introduced. However, if the common power supply fails, the issue is still not resolved.

3. Other issues in connection with the points above

   Even if the software functions are determined to be independent and using different processor and memory, they may communicate on a common data bus. A failure of a basic function on the bus (like a simple command/response communication for bus establishment and control) may have an impact on the data exchanged by the two processors and thus cause a hazardous failure.

4. COMBAT AIRCRAFT WEAPON EMPLOYMENT SAFETY

Weapon system safety is manifold. There is a wide range of well-established safety measures that can and/or must be implemented in order to achieve acceptable levels of safety; e.g., for dumb weapon release these safety measures may be realized in hardware (like safety pins or levers on ERUs to prevent premature operation), which must be manually operated or removed prior to take-off to enable weapon operation. To release weapons i.a.w. MIL-STD-1760 a release command implemented in software is protected by additional hardware interlock (like the MIL-STD-1760 Critical Control command 11R together with the Release Consent discrete).

This section addresses common practices used in manned combat aircraft in conjunction with weapon release. The explanation is based on a notional mission in order to cover all phases of weapon employment including ground ops.

The mission phases relevant for weapon operation are:

- Ground operation including handling, loading, unloading and testing of weapon/store
- In-flight air carriage without active weapons operation
- In-flight firing/release including preparation and safe separation
- In-flight jettison

The following table is intended to give an overview of possible safety features using the storyline of a generic combat mission. Neither all of the safety measures are implemented in all aircraft nor will be required for unmanned systems due to its unmanned nature, in which safety critical failures will not have a direct impact on a crew. However, some logical safety measures will be required by the installed interface, e.g., a platform/weapon combination using an interface iaw. MIL-STD-1760 including a MIL-STD-1553 command and control bus must implement the address, interlock, initialization routine, and release sequence. This list is not complete; especially the bus according to MIL-STD-1553 establishes more safety measures by its nature (redundancy, waveform, noise reduction, etc.).

The accepted premise for weapon carriage safety requirements is that no single point failure in the platform can cause the inadvertent release, fire, arming, or the initiation of any safety critical features of a weapon.

NOTE: The following terms are not standardised and may not apply to all implementations in the same way (e.g., Master Arm Safety Switch (MASS) implementation). Interpretation may be subject to a term's definition within a program or entity.

TABLE 4-3 – NOTIONAL COMBAT AIRCRAFT MISSION AND SAFETY MEASURES

Mission Phase / Task / Hazard	**Status / Action / Procedure**
Ground Ops: Weapon loading to platform by ground crew Probable Hazards: Unintended weapon arming or release	Platform and weapon electrically grounded and bonded together. S&RE Safe: this state is reached in different ways by different types of Suspension and Release Equipment (S&RE). It may be a Safety Handle[1] in >SAFE< position or a Ground Safety pin inserted that locks the hooks closed (weapon on ERU) and isolates firing power relay to cartridges or other interlocks to lock out the pneumatic firing valve.
Ground Ops: Configuration check Probable Hazards: Unintended weapon arming or release Unitended RF Transmission or Laser Radiation	S&RE in >Safe< state >Store Present on Station< = TRUE MASS[2] >SAFE< LAS (Late Arm Switch)[3] >Guarded< <u>Smart Weapon (MIL-STD-1760):</u> >Interlock<[4] >Address good< Initialization Power Applied Initialization incl. BIT >BIT passed< := TRUE Configuration Check passed Additional possible features: (gear_up[5] := FALSE).AND.CAS[6]<(150kts) or Weight_on_Wheels := TRUE
Ground Ops: Prepare for takeoff Probable Hazards: Unintended weapon arming or release Unintended RF Transmission or	S&RE := >UNSAFE< or >UNLOCKED< >Store on station< := TRUE MASS Master Armament Safety Switch >LIVE< or >ARM< *arming, fuzing, firing, release, jettison power enabled*

[1] Safety Handle: Mechanical handle on ejection and release unit / launcher enables electrical power to release cartridges if in "UNSAFE" position, can only be operated to UNSAFE if weapon is loaded (hooks mechanically closed).

[2] Master Armament Safety Switch (MASS): When set to >LIVE< or >ARM<, makes power available to the safety relays for distribution to fuzing, arming, release and jettison circuits. On some platforms the Switch is protected by a lock (position >LOCK< / >UNLOCK<), which can only be operated with a key. On some platforms the Switch may have 3 positions, >SAFE<, >STANDBY>, >LIVE<, with >STANDBY< for operational power. On other platforms it may be >OFF<, >ARM< or >SIMULATE< and on others it may only be a two position switch >SAFE< and >ARM<. Some implementations allow for jettison with MASS >SAFE< (separate circuits), others do not, i.e, MASS has to be switched before take-off.

[3] Late Arm Switch (LAS): When >Guarded< the weapon release button is de-activated, arming, fuzing, firing and release are inhibited. The switch itself is guarded. However, not all platforms have this switch / feature.

[4] Interlock is not required as a safety measure. It is intended to avoid power switching if the connector is not mated. This mishap will be overcome if the ground crew is involved in power switching after weapon loading. Interlock serves as hardware mated status indication. "Note (MIL-STD-1760): The interlock interface shall not be used as the sole criterion for functions, which could result in an unsafe condition if the interlock circuit fails open."

[5] gear_up: Indication that the aircraft landing gear is in up-position i.e. "in-air" condition. Sometimes the meaning is the reverse as in a "Gear Down and Locked"-indication. May also include a "Weight_on_Wheels"-indicator.

[6] CAS: Calibrated airspeed.

Mission Phase / Task / Hazard	Status / Action / Procedure
Laser Radiation	All weapon operation related systems >healthy<
In flight: Prepare for attack Probable Hazards: Unintended weapon arming or release weapon loss	S&RE := >UNSAFE< or >UNLOCKED< >Store on station< := TRUE MASS Master Armament Safety Switch >LIVE< or >ARM< *arming, fuzing, firing, release, jettison power enabled* LAS (Late Arm Switch) >Guarded< *Operational power to on* *Station/weapon delivery parameters selection* Additional possible features: Further weapon operation only if (gear_up := TRUE).AND.CAS>(150kts) or Weight_on_Wheels := FALSE
In flight: Weapon Release Preparation Probable Hazards: Unintended weapon arming or release weapon loss	S&RE := >UNSAFE< or >UNLOCKED< >Store on station< := TRUE MASS Master Armament Safety Switch >LIVE< or >ARM< *arming, fuzing, firing, release, jettison power enabled* LAS (Late Arm Switch) >LIVE< *weapon release button enabled* All weapon operation related systems >healthy< *Weapon Release Button pressed* Safety Critical Power available Smart Weapon (MIL-STD-1760): Weapon Status Good, alignment good, GPS data good Release Consent Discrete[7] *(enables safety critical command acceptance by store)* Critical Control (CC) 1[8]: 11R, W4, B2 "Commit to Separate Store or Submunition", *CC is only accepted by store if release consent is set at least 20ms prior to the command. Command may be protected by critical authority*[9]. To assure command was received by the store, the platform interrogates Critical Monitor 1: 11T, W4, B10 "Demanded State*", reflects the state required by the previous critical control message from the platform.* Weapon performs irreversible actions (e.g., battery startup) and reports after completion. Critical Monitor (CM) 1: 11T, W4, B2 "Committed to Store or Submunitions Separation". Messages with safety critical content are further protected by checksumming algorithms[10]. Weapon ready, expects release

[7] "Note (MIL-STD-1760): The release consent interface is provided to satisfy an aircraft safety function. Consent shall be enabled only when the aircraft determines that safety criteria for store employment sequence have been met".

[8] See MIL-STD-1760

[9] Critical Authority protects integrity of Critical Control words

[10] Message Checksum protects integrity of safety critical Store Control messages

Mission Phase / Task / Hazard	Status / Action / Procedure
	Additional possible features: Further weapon operation only if (gear_up := TRUE).AND.CAS>(150kts) or Weight_on_Wheels := FALSE
In flight: Weapon Release Probable Hazards: Weapon loss[11], Misfire[12], Hangfire[13], Hang-up[14]	MASS Master Armament Safety Switch >LIVE< or >ARM< *arming, fuzing, firing, release, jettison power enabled* LAS (Late Arm Switch) >LIVE< *weapon release button enabled* All weapon operation related systems >healthy< *Weapon Release Button pressed* Platform removes operational power from weapon station And verifies weapon is still powered Cartridges / explosives fired hooks open Weapon separates and disconnects from aircraft >Store on Station< = FALSE (provided no failure) Additional possible features: Further weapon operation only if (gear_up := TRUE).AND.CAS>(150kts) or Weight_on_Wheels := FALSE

Remarks:

"Operational Power" supplies the store station with power to initialize and maintain operation of the store "Safety Critical Power" provides power to the store station and to the store in order to perform safety critical activities (e.g., thermal battery initiation or release).

5. SAFETY IN UNMANNED SYSTEMS WEAPON OPERATION

Safety design features of unmanned armed systems should be based on experience gained with armed manned aircraft, but may be implemented in a different fashion or different location in the system (e.g., on the ground and not in the platform).

Proper design of unmanned armed systems as well as manned aircraft should apply appropriate safety measures and the criteria that a common mode or single failure must not result in a safety critical condition.

The descriptions of characteristics incorporated into manned aircraft/weapon systems to achieve acceptable levels of safety (Section 4) will not all be directly applicable to all unmanned systems. The safest condition for unmanned systems is per definition stationary, unpowered and unarmed, which will be violated during most mission phases. The result of a failure and therefore the required corrective measures will lead to some distinction in aerial, subsurface and ground-based systems, based upon a specific hazard analysis.

[11] Weapon loss: Inadvertent loss during air carriage

[12] Misfire: Firing power is not delivered to station (or weapon?), launch sequence cannot be completed

[13] Hangfire: Due to weapon internal failures resulting in an unexpected delay in the firing sequence, the release of the weapon is delayed or may never occur

[14] Hang-up: Release sequence completed, but the weapon is mechanically retained

Due to the absence of a human operator in the vehicle detailed system status and health indications are required to be provided to the remote operator on the control station of an unmanned armed system. A pilot in some cases would still be able to visually confirm a possible failure (e.g., simply by looking outside the cockpit at the weapon), therefore as much detail as possible is required (e.g., watchdogs) to support safe weapon operation and the situation awareness of a ground-based remote operator.

In case that a vehicle control hand-off is required, the system should allow a safe transition and report overall system status to the new operator.

5.1 System Boundary

The system for which these safety considerations may apply consists of a platform and a control element (an unmanned armed airborne system, a ground-based unmanned weaponized vehicle/weaponized robot or an unmanned armed naval system). In the following we concentrate on unmanned airborne systems. The general principles, however, can be applied to systems operating in all environments.

The airborne element (UAV Air Component) is connected and linked to a ground control station (UAV Surface Component) as shown in Figure 1.

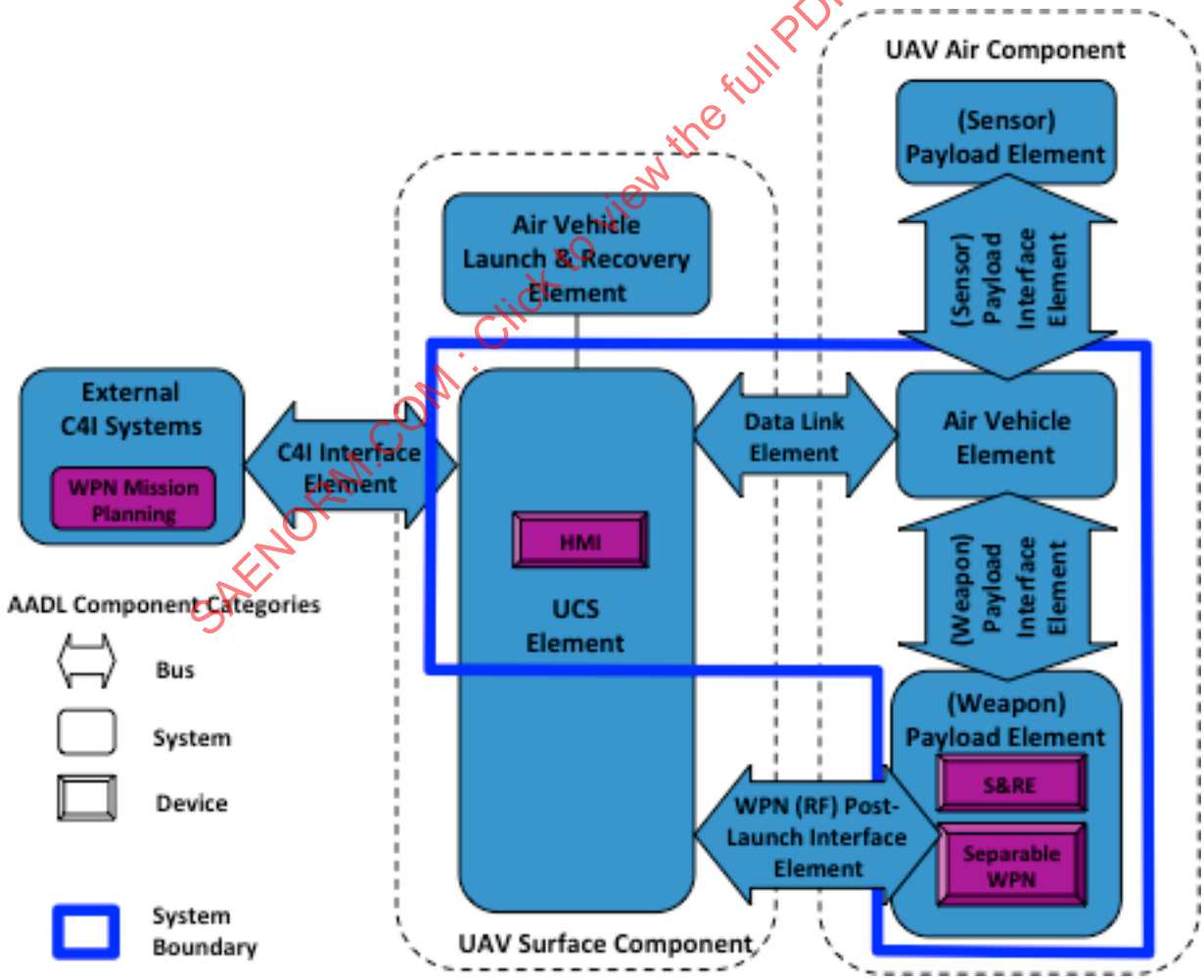

FIGURE 1 - ORGANIZATION OF AN UNMANNED AERIAL SYSTEM (DERIVED FROM NIAG SG125)

5.2 Allocation of Function and Responsibility

5.2.1 General

The following allocations are regarded essential for unmanned systems weapon operation:

- Due to doctrine and Rules of Engagement, target and aimpoint selection will be made or approved by a human operator in the control element.
- Due to doctrine and Rules of Engagement, weapon release will always be initiated by an operator in the control element.
- Following a weapon release decision, a time period may be required to allow the platform to manoeuvre to an acceptable release point and/or an appropriate release speed and attitude. That time period must be accommodated by either (a) providing the operator with sufficient situational awareness and/or software constraints that he will wait until those conditions are reached before initiating weapon release, or (b) that timeline must be included as an allocation of the time limit between operator initiation of weapon release and the release itself.
- UAV must be in a controlled flight envelope applicable to safe weapon release.

5.2.2 Timing Considerations

Operation of unmanned vehicles inevitably introduces timing delays not encountered with manned vehicles. Many of the delays generated within the UCS element and the vehicle will be similar to those in manned systems and will therefore be relatively predictable. Additional delays introduced by communications between the UCS and vehicle may be long and/or unpredictable relative to other system timings. It is essential that the following timing factors are considered when specifying, designing and operating unmanned weapon systems:

- Timing of operations within the UCS must be closely defined;
- Timing of operations within the vehicle must be closely defined, especially for irreversible actions or actions associated with weapon release;
- Allocating end-to-end timing delays among elements within the UCS, vehicle, weapon, and UCS-to-vehicle communications. These total delays are measured from operator physical action at the user interface to final responsive event in the weapon (including its release), and from event in the weapon to confirming display or alert at the operator interface;
- Minimum time needed for communications between transmitters and receivers located in both the UCS and the vehicle, including multi-hop transfers where applicable;
- Maximum time allowed for timing delays and/or loss of communication before initiation of measures in the UCS, vehicle and/or weapon necessary to ensure safe and predictable vehicle behaviour.

5.2.3 System Status and Situational Awareness

The design of the complete system should include consideration of the operator uncertainty that would arise from relatively long intervals between UCS operator commands and confirmatory responses from the vehicle. This is particularly essential when the commands are irreversible, including the possibility of weapon release.

All involved parties shall have full situational awareness; e.g., two-way communication link between ground crew and operator.

5.3 Suggested Safety Measures for Unmanned Armed Systems

When being carried by an aircraft, stores are required to carry out operations in support of the mission that range from carrying out self-test, receiving mission and navigation data, providing status reports, initiating safety critical or irreversible functions in preparation for release and signalling that it is safe and ready for release by the aircraft.

These actions can be split into two types: those that have no association with safety critical or irreversible functions, and those that are directly associated with these functions and are carried out only as part of operational deployment. Aircraft and stores are designed with additional safeguards to reduce the probability of inadvertent initiation of these functions to acceptable low levels. Examples include additional encoding for certain commands transferred by data buses, and the presence of a discrete signal (see 5.3.2) on the interface to authorise store use of the data bus command – as discussed in 5.3.2.

The following sections elaborate safety measures regarded typically for an unmanned aerial system as derived from manned aircraft safety measures. Appendix A.1 provides a notional mission course of events based on the suggested safety measures.

MIL-STD-1760, AS5725, AS5726 include the following interfaces, that can be used as part of a safe weapon interface

- DC#2/Safety Enable Power
- Release Consent/Safety Enable Discrete
- Subaddress 11 Critical Control Message (SA11R)

All the three of the above controls are recommended for the activation of safety critical and irreversible functions and they are usually required in a predefined sequence. The primary interlock in this set is Release Consent/Safety Enable Discrete. Without this discrete in the enable state, the store must not perform safety critical functions commanded over the data bus in SA11R or make use of DC#2 to initiate such functions.

Currently, manned aircraft implementations employ multiple independent control mechanisms for these three interfaces.

Unmanned armed systems should implement equivalent independent mechanisms to control similar type functions for armament interfaces.

5.3.1 Consideration of DC#2/Safety Enable Power Supplies

For those safety-related or irreversible functions that are not implemented in software, an additional power source (sometimes referred to as safety power) is provided on the interface. This power is present only at times that system operation requires the safety-related or irreversible functions to be carried out. One example of such an operation is the ignition of thermal batteries as part of the launch sequence. Depending on the precise nature of the battery igniters, the supply may be required to provide pulses of current in excess of 10 A for periods of 10 to 20 ms, or for up to 1 s should the igniters create a short-circuit to the battery case.

Several interface standards derived to define aircraft-store interfaces include the requirements for the provision of a safety power source. Common examples are:

- Aircraft/store Electrical Interconnect System (MIL-STD- 1760) has a ‘28 V DC Power 2’.
- Interface Standard, Miniature Mission Store Interface (AS5725) has a ‘Safety Enable Power’.
- Interface Standard, Interface for Micro Munitions (AS5726) has a ‘Safety Enable Power’.

The requirements for use of these three supplies are all very similar and can be summarised as follows:

- The safety power source is applied only when the aircraft (or carriage store) considers it safe to do so, as defined and agreed in the system ICD.
- The duration of application of the safety power source may be restricted. For example, power application defined in AS5726 is limited to no greater than 2 s per application, although power may be applied more than once.
- Stores are not required to use the safety power source if sufficient interlocks exist in the store to achieve the required levels of safety.
- Stores are not permitted to activate any safety critical function simply as a result of the provision of the safety power supply.

Although not a requirement of the standards, it is recommended that where possible, provision to stores of the safety power source be as a result of direct operator action, such as setting a switch to a specific position as part of the release sequence for the store.

5.3.2 Release Consent/Safety Enable Discrete

This signal is historically called Release Consent, although a better name for it is Safety Enable Discrete as used in recent platform/store interface standards like AS5725 and AS5726.

Release Consent/Safety Enable has an enable and an inhibit state. It is the pre-requisite for all safety critical commands from the platform to the store; without the signal in the enable state the store must not accept safety critical commands from the platform. Such commands may include preparation for release leading to the initiation or irreversible processes by the store or arming presets; e.g., transferred in the Critical Control Message to subaddress 11R in MIL-STD-1760 (see next section). Whilst the platform is required to provide this capability, for the store the signal state is only mandatory when Bit 0 (Fire, Launch, or Release) or BIT 2 (Commit to Separate Store or Submunition) in the Critical Control Word 1 in SA11R are commanded over the data bus.

The signal state is usually related to intended operator action; e.g., it is set to the enable state once the release button is pressed. Even in the case of operator action the discrete is only switched "when the aircraft determines that it is safe to do so;" i.e., the system's overall condition allows the execution of safety critical functions.

The combination of a discrete hardwired signal independent from the data bus improves the safety of the overall system and facilitates safety analysis.

It is typically implemented as a discrete low power signal(MIL-STD-1760 specifies 100mA@28VDC).

5.3.3 Subaddress 11 Store Control Message

Subaddress 11 Store Control Message is defined in MIL-STD-1760 as a means to initiate safety critical and irreversible functions in a store. The safety critical functions are allocated in two critical control words and include:

- Store Arming Authority or Preset Arming (a store is never armed when connected to the platform, but preparatory commands; e.g., to select specific fuzing capabilities are permitted)
- Store Launch, Fire, Release or Jettison
- Initiation of Safety Critical Irreversible Functions (Commit to Separate Store or Submunition) associated with preperation to launch, fire or release (e.g., thermal battery ignition)

- Initiation of Interruptive Built In Test
- Erasure of critical data
- RF Transmission authority (transmissions that maybe hazardous)
- Aborting Launch, Fire, or Release
- Activation of Non-Safety Critical Release Irreversable Functions

The MIL-STD-1553 data bus subaddress 11 was chosen after an analysis of the probability of a software error generating the specific bit pattern associated with subaddress 11 was lower than any of the other 31 possible subaddress assignments. The MIL-STD-1553 data bus standards use a parity bit on each word transmission to identify any bit swaps that occur in the transmission medium. MIL-STD-1760 additionally adds an extensive checksum of the entire data message, Invalidity words, critical authority words which use a the BCH Polynomial check procedure to verify the specific bit pattern, and embedded store address fields to verify the command was intended for the specific addressed store. This layering of error detection capability is to prevent an inadvertent activation of a safety critical command by software error or processing error. The probability of inadvertent generation of a valid critical control word with a valid critical authority word and with a data field requesting critical action should not exceed 1 in 10^5 operation hours per data field combination. Any data communication path (data bus, data link, etc.) that carries data that is a safety critical command or data that results in the generation of a safety critical command should take into consideration similar type of measures to verify the integrity of the data. Of note is that safety organizations typical do not accept the use of techniques that “correct” detected data errors in safety critical command data paths.

5.4 Unmanned Ground Systems and Unmanned Maritime Systems

The principles as described in 5.3 apply also to the other kind of unmanned systems, however, they need to be applied to the relevant robot weapon systems (e.g., a safeguard on a gun mounted on the robot instead of a safety switch on the aircraft). Concerning the remote operation, the safety measures associated with the design of the robot control are similar. Appendix A.1 provides an example for a notional unmanned systems mission and provides a proposal for safety measures.

6. CONCLUSIONS AND RECOMMENDATIONS

It is not the intention of this paper to impose a system architecture. However, the safety criticality of weapon operation functions prescribes design measures including the inherent requirement that single or common mode failures causing catastrophic events must be avoided. As stated above, no single point failure should cause the inadvertent employment or release of any weapon.

As a general guideline, redundancy for safety critical functions in the form of at least two independent signals should be utilized. This means, for instance, that a safety critical command over a data channel (data bus or data link) should not only include measures to detect possible data errors in processing or transmission but should also be validated by an associated independent signal. On the other hand this must not be confused with a requirement for two independent channels of a data link (or two different transfer paths/two modulation schemes, etc.) for the transmission of the signal. This is not considered necessary, as long as the two validated signals are received without errors in the right order within the required timeline. The extension of the manned aircraft/weapon interface safety approach to the unmanned armed system is not necessarily a direct correlation for all applications. For example, implementation of a release consent with a digital data fire command relative to a machine gun may be translated into a power enable and power application circuit to enable a solenoid to pull a trigger. In another case, with a weapon that has an electrical interface to the unmanned system, the approaches described in Section 5 may be directly applicable.

The safe design of the weapon operation must include recovery measures for loss of communication and for vehicle hand-off to another vehicle control unit.

APPENDIX A

A.1 NOTIONAL UNMANNED SYSTEMS MISSION EXAMPLE

The following example shows the usage of the previously discussed safety measures in an example UV mission.

Mandatory and optional safety measures are discussed based upon the experience from manned aircraft and under consideration of the safety precepts.

A wide range of unmanned systems in all sizes and the trend to miniaturized (micro-) weapons will not necessarily allow for safety measures similar to a manned combat vehicle. The stores management functionality may be distributed between the control station and the vehicle dependent on the size and complexity of the system. The following example is intended for a complex US.

The platform structure and the weapon size drive the requirement for smaller connectors, which reduces the signal set. Therefore the following examples should be weighted against the effort of technical realization and specific system architecture.

Some of the footnotes are copied from Section 4 and are repeated here for a better understanding of the concept.

TABLE 6-4 – WEAPONIZED UNMANNED VEHICLE SAFETY MEASURE PROPOSAL

Mission Phase / Task	Procedure / Measure Combat Aircraft	Procedure / Measure Unmanned System	Proposal
Ground Ops: Weapon loading to platform	Platform and weapon electrically grounded and bonded together	Platform and weapon grounded	
	S&RE Safe: this state is reached in different ways by different types of Suspension and Release Equipment (S&RE). It maybe a Safety Handle in >SAFE< position or a Ground Safety pin inserted that locks the hooks closed (weapon on ERU) and isolates firing power relay to cartridges or other interlocks to lock out the pneumatic firing valve.	S&RE present:Prevent inadvertent firing power to cartridges: Safety Handle in >SAFE< Alternative carriage system: Protected switch in >SAFE< (to be operated by ground crew)	Safety handles[15] or similar device on S&RE installation
Ground Ops: Configuration check by ground crew and/or operator	S&RE in >SAFE< state >Store Present on Station< = TRUE	Operational power on by ground crew → (switch on external power or platform power)	Operational power switch accessible by ground crew
		Safety critical power off, routing to station disabled Safety Switch[16] on platform >SAFE< >Store on station< = TRUE	Ground test capability to allow weapon configuration and system health check Safety critical power protected by guarded safety switch accessible to ground crew

[15] Safety Handle: Mechanical handle on ejection and release unit / launcher enables electrical power to release cartridges if in “UNSAFE” position, can only be operated to UNSAFE if weapon is loaded (hooks mechanically closed).

[16] NIAG SG125 / NATO JCGUAV ST suggest two switches for safety critical power: one protected switch accessible to ground crew as a safety interlock (without switch lo >LIVE< routing of safety critical power is disabled) and a MASS on the ground control station panel.

Mission Phase / Task	Procedure / Measure Combat Aircraft	Procedure / Measure Unmanned System	Proposal
	MASS Master Armament Safety Switch >SAFE< LAS (Late Arm Switch) >Guarded<	MASS on ground control station >SAFE<	MASS switch on ground control station, MASS status visible to ground crew, safety switch status visible to operator
			Remote check capability for operator, reflects health status in ground station MASS status included in communication data set
			Additionally required status: Communication Line = GOOD
	Smart Weapon (MIL-STD-1760): >Interlock< >Address good< Initialization (Operational) Power >ON< Initialization incl. BIT >BIT passed< := TRUE	Smart Weapon (MIL-STD-1760): >Interlock[17]< >Address good< Initialization (Operational) Power Applied Initialization incl. BIT >BIT passed< = TRUE Information about weapon mechanical mated status (e.g., interlock) to ground crew and/or operator	Information exchange between operator and ground crew
	Configuration Check passed	Configuration Check / System Health Check passed	
	Additional possible interlock features: (gear_up := FALSE).AND.CAS[18]<(150kts) or Weight_on_Wheels = TRUE	Additional possible interlock features: (gear_up[19] := FALSE).AND.CAS<(150kts) or Weight_on_Wheels = TRUE	Wheel status indication
			Further weapon operation only if all systems healthy

[17] Interlock is not required as a safety measure. It is intended to avoid power switching if the connector is not mated. This mishap will be overcome if the ground crew is involved in power switching after weapon loading. Interlock serves as hardware mated status indication.
"Note (MIL-STD-1760): The interlock interface shall not be used as the sole criterion for functions, which could result in an unsafe condition if the interlock circuit fails open."

[18] CAS: Calibrated airspeed.

[19] gear_up: Indication that the aircraft landing gear is in up-position i.e. "in-air" condition. Sometimes it is the reverse as in a Gear_Down_and_Locked indication. May also include a Weight_on_Wheels or Weight_off_Ground indicator.