



**NOT MEASUREMENT
SENSITIVE**

**DOE-STD-1047-2008
August 2008**

DOE STANDARD

Safety Functions and Other Features of Remotely Operated Weapon Systems (ROWS)



U.S. Department of Energy
Washington, D.C. 20585

AREA SAFT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

TABLE OF CONTENTS

FOREWORD	i
1. SCOPE AND PURPOSE	1
2. APPLICABILITY	1
3. NORMATIVE REFERENCES	2
4. DEFINITIONS	2
5. SPECIFICATIONS	4
Engineered Sector-Limiting Stops	4
Electrical and Optical Circuits	4
Maintenance Functions and Features	5
Lasers (if any).....	5
Aiming Systems and Optics	5
Platform Enclosure (if any)	6
Command and Control Functions	6
Communications and Networking Functions.....	6
Functions and Features Related to Human Factors	7
Training	8
Safety-Critical Software (if any)	8
Testing Functions and Features	8
System Documentation	8
6. SAFETY ACCEPTANCE TESTS.....	9
APPENDIX A. ACRONYMS AND ABBREVIATIONS	10
APPENDIX B. AGENCY-SPECIFIC AND INFORMATIVE REFERENCES.....	11
APPENDIX C. RECOMMENDATIONS FOR PURCHASERS (Informative)	13

FOREWORD

This Department of Energy Standard is for use by all DOE elements.

Beneficial comments (recommendations, additions, and deletions) and any pertinent data that may improve this document should be mailed to the U.S. Department of Energy; Office of Health, Safety, and Security; Office of Technology, GTN/HS-82; 1000 Independence Ave., SW; Washington, DC 20585-1290 or e-mailed to lynne.preston@hq.doe.gov. Please use the Document Improvement Proposal form (DOE F 1300.3) appearing at the end of this document.

DOE technical standards do not establish requirements. However, all or part of the provisions in this standard can become requirements under the following circumstances:

- (1) They are explicitly stated to be requirements in a DOE requirements document (e.g., a purchase requisition); or
- (2) The organization makes a commitment to meet a standard in a contract, implementation plan, or program plan.

Throughout this standard, the words “must” or “shall” are used to denote actions that must be performed if the objectives of this standard are to be met. If the provisions in this standard are made requirements through one of the two ways discussed above, then the “shall” statements would become requirements. Goals or intended functionality are indicated by “will,” “may,” or “should.” It is not appropriate to consider that “should” statements would automatically be converted to “shall” statements as this action would violate the consensus process used to approve this standard.

This standard was prepared following requirements for due process, consensus, and approval as required by the U.S. Department of Energy Standards Program. Consensus is established when substantial agreement has been reached by all members of the writing team and the standard has been approved through the DOE directives approval process (REVCOM). Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

When the writing team reached substantial agreement that this document should be submitted for approval as a DOE standard, it included the following members:

<i>Organization Represented</i>	<i>Name of Representative</i>
U.S. Department of Energy	
Security Technology and Assistance (HS-82)	Lynne Preston
Security Technology and Assistance (HS-82)	Robert Loesch
Office of Security Policy (HS-71)	Dave Dietz
Office of Science, Safeguards & Security Div (SC-31.3) ..	Gary White

Office of Science, Safeguards & Security Div (SC-31.3) .. James Lint	
Idaho National Laboratory	
Batelle Energy Alliance of Idaho, ES&H	Bennie Cooley
Los Alamos National Laboratory	
Protection Technology Los Alamos.....	Vern Woodward
MRP Inc.	Jake Sullivan
National Nuclear Security Administration	
Office of Program Requirements (NA-72)	Kevin Leifheit
Office of Program Requirements (NA-72)	Garrett Johnson
Office of Secure Transportation (NA-152.33).....	Bennett R. Davis
Nevada Test Site	
WSI Nevada	Phil Mertz
WSI Nevada	Jeff Herhold
Oak Ridge National Laboratory	
Security Systems.....	John Watson
Security Systems.....	Daron Keesee
Security Systems.....	Leslie (Kim) Engle
Prairie Island Nuclear Generating Plant	David A. Axt
Precision Remotes Inc.....	Mike Hanley
Protection Strategies, Inc.	Bobby Beaty
Recon Optical, Inc.	George Hines
Sandia National Laboratories	
Intelligent Systems, Robotics, and Cybernetics.....	William Drotning
Intelligent Systems, Robotics, and Cybernetics.....	Kristopher Klingler
Advanced Security Systems.....	Steven Scott
Department 6454 – Transportation Assessment	Jack F. Jones, II
Department 6454 – Transportation Assessment	Skip Metcalf
Safety Engineering Program	Willie Johns
Savannah River Site	
Office of Safeguards, Security and Emergency Services ...	William Dennis
Special Technologies Laboratory	Raymond Page
Technical Products Inc.....	Paul Chambers
U.S. Air Force	
642 nd Electronic Systems Squadron.....	Marc von Hahmann
642 nd Electronic Systems Squadron.....	Stephen Bertulli
642 nd Electronic Systems Squadron.....	Jim Maloy
U.S. Nuclear Regulatory Commission	
Reactor Security Licensing and Programs Branch	William D. Smith II
Y-12 Plant	
Safety Analysis Engineering.....	William Moon, Jr.
Security Systems.....	Robert J. Sharp
Security Systems.....	Mike Lowe

1 SCOPE AND PURPOSE

This standard summarizes safety functions and other features of Remotely Operated Weapon Systems (ROWS) requested most frequently by users and safety personnel at sites of the U.S. Department of Energy (including the National Nuclear Security Administration). These design features are intended to improve the safety, reliability, and ease of use of these systems; they may also improve the performance of these systems. The intent is to communicate common requirements to vendors of these systems, so as to ease safety review and use at DOE sites.

This standard applies to remotely operated weapon systems that are aimed at specific points in space (e.g., stun guns, machine guns). Activated denial systems (e.g., foams, explosives) that are triggered to delay or neutralize all inhabitants of a defined volume of space will be discussed in a separate standard.

The overall philosophy for safety of remotely operated weapon systems is that no single action or event can cause inadvertent firing of the weapon. The use of three separate and independent commands reduces the probability of simultaneous failure to less than 10^{-6} , which may negate the need for further safety analysis.

Remotely operated weapon systems must not fire except upon command of a human operator.

2 APPLICABILITY

This standard was written by an inter-agency writing group so that by referring to this standard, vendors can develop systems that will meet the basic safety requirements of all U.S. customers. To enable this, requirements and references specific to the DOE, the U.S. Department of Defense, or the U.S. Nuclear Regulatory Commission are given in Appendix B, "Agency-Specific and Informative References" and Appendix C, "Recommendations to Purchasers (Informative)."

It is recommended that DOE sites use this standard as one of the required elements of a purchase requisition.

The use of this standard is voluntary; its existence does not in any respect preclude anyone, whether he has approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. However, should a manufacturer or vendor of a remotely operated weapon system state to a purchaser that a system meets this standard, the system must meet all specifications and acceptance tests in the standard or the vendor must disclose those that are not met.

The use of this standard does not exempt contractors of the United States government from regulatory requirements as required by contract.

3 NORMATIVE REFERENCES

Remotely operated weapon systems that meet the requirements of this standard must meet the requirements of the following national standards, incorporated by reference. In addition, ROWS must comply with requirements of the purchaser's cognizant regulatory authority (e.g., systems purchased by DOE sites must comply with DOE quality regulations). See Appendix B, "Agency-Specific and Informative References."

- 3.1 ASME Y 14.100, "Engineering Drawing Practices," American Society of Mechanical Engineers.
- 3.2 NFPA 70, "National Electrical Code," National Fire Protection Association.
- 3.3 NFPA 79, "Electrical Standard for Industrial Machinery," National Fire Protection Association.
- 3.4 ANSI Z136.1, "Safe Use of Lasers," Laser Institute of America.
- 3.5 ANSI Z136.6, "Safe Use of Lasers Outdoors," Laser Institute of America.
- 3.6 Applicable standards, 29 CFR Part 1910 (U.S. Department of Labor, Occupational Safety & Health Administration), including:
 - 3.6.1 OSHA Standard 1910.212, "General Requirements for All Machines."
 - 3.6.2 OSHA Standard 1910.147, "The Control of Hazardous Energy (Lockout/Tagout)."
- 3.7 ANSI Z535.4, "Product Safety Signs and Labels," National Electrical Manufacturers Association.

4 DEFINITIONS

- 4.1 **ARM.** To release safeties and charge the weapon (if chamber is empty).
- 4.2 **BRASS.** The hull or casing of a cartridge.
- 4.3 **BULLET TRAP.** A device to safely stop a bullet in flight.
- 4.4 **BURST.** The number of bullets fired from an automatic weapon by one pull of the trigger.
- 4.5 **CARTRIDGE.** A completed assembly for firing in a weapon, consisting of casing (brass), powder, and primer, with or without one or more projectiles (bullets).

- 4.6 **CENTRAL ALARM STATION (CAS).** The manned location that monitors the site intrusion detection sensors and other alarm systems, and provides command, control, and other support to response forces.
- 4.7 **CHAMBER.** In a rifle, shotgun, or pistol, the rearmost part of the weapon barrel that holds the cartridge ready to fire.
- 4.8 **CHARGE.** To place the bolt of a weapon in firing position.
- 4.9 **CONDITIONS OF ACTIVATION: ENABLE, ARM, FIRE.** The three conditions of the ROWS that must be activated by separate and independent commands or actions in order for the weapon to fire.
- 4.10 **ENABLE.** An action which allows a ROWS to be armed, then fired.
- 4.11 **OPERATIONALLY DEPLOYED.** A system is operationally deployed when it is ready to acquire and engage a target (e.g., system is powered up, enclosure is opened, cameras and control station are operational).
- 4.12 **PLATFORM.** The support structure of the ROWS upon which components are mounted.
- 4.13 **REMOTELY OPERATED WEAPON SYSTEM (ROWS).** A weapon system that is operated from a remote (presumed safe) location. It includes a support structure (platform) and operator control station. The platform may be used to support a variety of electro-optical sensors, and a non-lethal or lethal weapon. (The ROWS does not change the inherent safety or operation of the weapon mounted on the platform.) The platform may be mounted in a variety of configurations at one or more locations within or outside a facility, or upon a vehicle. The electro-optical sensors display to, and the platform and mounted systems are controlled from, one or more control stations remote from the platform.
- 4.14 **SAFE CONFIGURATION.** A configuration of the system where the control station and weapon have safeties applied to prevent an unintentional discharge. (All safeties must be released before a fire command can be executed.)
- 4.15 **SAFETY-CRITICAL SOFTWARE.** Software that controls the enable, arm, or fire commands is considered safety-critical software.

5 SPECIFICATIONS

5.1 ENGINEERED SECTOR-LIMITING STOPS.

- 5.1.1 All fixed and mobile ROWS shall incorporate a capability for adding physical stops, preferably adjustable, that prevent weapon motion (e.g., elevation or rotation) beyond safe limits established by the user.
- 5.1.2 Devices which limit platform motion by means other than physical or mechanical, such as limit switches, may be provided to restrict platform movement.
- 5.1.3 The ROWS shall provide on-site programming of no-fire zones.

5.2 ELECTRICAL AND OPTICAL CIRCUITS.

- 5.2.1 The system shall ensure that the weapon is operationally deployed only in a safe configuration.
- 5.2.2 Upon loss of power or communication, the system shall default to a safe configuration. Upon recovery of power or communications, the system must remain in its current position and remain in a safe configuration.
- 5.2.3 Separate and independent commands shall be required to enable, arm, and fire the weapon. At least one of these commands shall be by means of closure of a separate and distinct hard-wired electrical or optical circuit. This hard-wired closure shall interrupt power as close as practicable to the weapon trigger. Command signals shall be communicated independently so that a single fault or an unsafe condition cannot initiate or simulate two of the required three commands. Command signals may be transmitted from source to destination by electrical, optical, or wireless communication.
- 5.2.4 Weapon enable/disable, arm, and fire switches shall be configured to prevent inadvertent activation.
- 5.2.5 The system shall include electrical interlocks that prevent the weapon from firing except when operationally deployed.
- 5.2.6 Cables and connectors should be marked with unique permanent identifiers and clearly visible when accessed for maintenance. Each cable and matching receptacle shall be keyed differently or use unique connector types to preclude the possibility of misconnecting cables.
- 5.2.7 The system shall have an emergency stop (E-stop) to disable a platform, stop all moving parts, and prevent activation of the firing sequence. An E-stop must be manually reset per NFPA 79.

- 5.2.8 The control station must include an indicator to alert the operator to power levels which may adversely affect the operation of safety subsystems.

5.3 MAINTENANCE FUNCTIONS AND FEATURES.

- 5.3.1 The platform shall include a local lockout method or lockable on/off switch to isolate power during maintenance (e.g., lock and tag out).
- 5.3.2 The platform shall have a local means (e.g., lockout method or a local/remote switch) that, when used, prevents control from any other location. The intent is to permit maintenance personnel to test powered platform operation.
- 5.3.3 The system shall be configured to minimize pinch, sharp, and mechanical motion hazards in accordance with the OSHA 1910.212 standard for machine guarding.
- 5.3.4 Components that have a potential safety impact shall be labeled where appropriate with safety warnings in accordance with ANSI Z535.4.

5.4 LASERS (if any).

- 5.4.1 All lasers that are not eye safe per ANSI Z136.1 must be provided with a mechanical lockout or a blocking device so that each can be disabled during maintenance, performance tests, and exercises. NOTE: Class 1M and 2M lasers may not be considered eye safe under magnification.

5.5 AIMING SYSTEMS AND OPTICS.

- 5.5.1 The primary camera (area-wide) display shall show the controlled weapon's point of aim.
- 5.5.2 The video sighting system shall be designed to address mechanical shock and vibration so that the operator can identify targets during tracking, aiming and firing.
- 5.5.3 The system or bore sighting position must provide assurance that the aiming system is aligned with the weapon. NOTE: Weapons may be exchanged for maintenance purposes, with the likelihood that aim settings would change. A bore-sighting capability or equivalent is needed for those fixed locations where the weapon cannot be fired except during an attack.
- 5.5.4 Command latency and communication lag between weapon aim and video display shall be considered in the system design. Lag time or latency shall not cause an unsafe condition.

5.6 PLATFORM ENCLOSURE (if any).

- 5.6.1 Weapons stowed within an enclosure must meet the requirements for safe configuration defined in paragraph 4.13 of this standard.
- 5.6.2 Platforms with an enclosure shall communicate to the operator the open or closed status of the enclosure.
- 5.6.3 Platforms mounted in outdoor locations or upon a vehicle operated outdoors shall be designed to withstand expected natural and manmade environmental conditions (e.g., rain, extreme temperatures, icing, winds, lightning, vibration).

5.7 COMMAND AND CONTROL FUNCTIONS.

- 5.7.1 The operator control station shall include an indicator to show that one or more platforms have been enabled.
- 5.7.2 The operator control station shall clearly display when the weapon being controlled is armed and ready to fire.
- 5.7.3 The operator control station shall permit the operator to interrupt weapon deploy and stow commands.
- 5.7.4 Failure of the weapon to deploy or stow shall initiate a motion stop and generate a signal to the operator.
- 5.7.5 Failure of the weapon to pan/tilt to the intended position shall generate a signal to the operator.
- 5.7.6 The operator control station shall permit the operator to interrupt any platform motion command. For example, the operator must be able to interrupt a slew command.
- 5.7.7 The operator control station shall include a control which permits the operator to engage the safety selector on the platform weapon.

5.8 COMMUNICATIONS AND NETWORKING FUNCTIONS.

- 5.8.1 Wireless capable ROWS shall be resistant to radio frequency interference, jamming, or remote takeover by unauthorized personnel.
- 5.8.2 Wired and wireless systems shall not fire unintentionally when exposed to external radio frequency or electromagnetic interference.
- 5.8.3 A ROWS platform shall not accept commands from more than one operator at a time.

- 5.8.4 Safeties preventing weapon discharge shall be engaged when the weapon platform responds to automated, non-operator initiated system movement commands. Case 1: If a platform is under direct control of a sensor and can move without operator acceptance, then platform response should not be considered operator-initiated movement. Case 2: If an operator accepts a sensor slew command before movement, it is regarded as operator-initiated movement.
- 5.8.5 The system shall permit each operator to fire only at one target at a time. NOTE: A networked system may be preprogrammed to cover a single target with multiple platforms. The system may permit an operator to program sequential fire to address multiple targets only if the operator makes the decision to fire upon each target individually and retains the capability to cease fire when the threat has been neutralized.
- 5.8.6 Weapon safeties shall be automatically engaged when control of a platform is relinquished by an operator. The platform may continue to respond to automated system movement commands from external devices.
- 5.8.7 Safeties preventing weapon discharge shall be automatically engaged when control changes from one operator control station to another.
- 5.8.8 The operator control station shall identify which ROWS platform(s) the operator has control of and has armed.
- 5.8.9 Command latency and communication lag shall be considered in the system design, and whether expected lag times would be sufficient to cause an unsafe condition. In those cases, a safe condition shall be implemented (e.g., by treating excessive lag time as a loss of communication per 5.2.2, or by cancelling commands that exceed the safe lag time).

5.9 FUNCTIONS AND FEATURES RELATED TO HUMAN FACTORS

- 5.9.1 Sensor display brightness and dynamic range shall be adjustable depending upon the brightness of the area being observed and the location of the control station (e.g., in a vehicle during the day or during the night). The refresh rate shall be sufficient so that there is no flickering discernable to the operator.
- 5.9.2 The system shall provide feedback to the controller(s) whenever a command is executed successfully as well as when it is unsuccessful. All fault conditions should display clearly on the screen. These indicators shall not interrupt or delay controller actions.
- 5.9.3 System enable, arm, and fire switches shall be dedicated to fulfilling a single independent command and associated function. A single switch, button, or command shall not perform different actions in different situations. (Each

operator action must have a unique purpose that holds true regardless of the state of the weapon.)

5.10 TRAINING

5.10.1 Vendor-supplied documentation and training shall cover safe operation and maintenance of the ROWS.

5.11 SAFETY-CRITICAL SOFTWARE (if any).

5.11.1 The vendor is responsible for review of proprietary code and for understanding the consequence of failure of commercial off-the-shelf software. The vendor shall provide to the purchaser any known hazards associated with system commercial off-the-shelf hardware and software.

5.11.2 Safety-critical software shall include only required and intended functionality.

5.11.3 Power surges or low or high power levels must not corrupt safety critical software.

5.11.4 Safety critical software must be resistant to accidental modification.

5.11.5 Safety-critical software shall meet agency requirements.

5.11.6 To assist system safety reviews, the vendor shall document safety-critical software ground rules and assumptions.

5.12 TESTING FUNCTIONS AND FEATURES.

5.12.1 The system must have a self-test capability that, when exercised, provides assurance that communications and backup power supply are operating correctly.

5.12.2 The system shall support routine function tests to determine safe operation of the system.

5.12.3 The system shall support routine testing to ensure that the aiming system is aligned with the weapon.

5.13 SYSTEM DOCUMENTATION.

5.13.1 System documentation shall include full software documentation and engineering drawings with a full set of electrical schematics including connector types and identifiers; safety certifications and acceptance test report(s); training, configuration management, and maintenance procedures; and operator's manual.

5.13.2 Hardware and software for purchased ROWS shall be placed in a configuration control program.

6 SAFETY ACCEPTANCE TESTS

The ROWS provider shall provide the purchaser with a testing document that will demonstrate that the system meets the requirements of Section 5. Once the test plan has been approved by the purchaser, tests shall be witnessed or conducted by the purchaser prior to accepting a system.

Acceptance tests must meet agency-specific requirements. (See Appendix B.)

APPENDIX A ACRONYMS AND ABBREVIATIONS

ANS. American Nuclear Society.

ANSI. American National Standards Institute.

ASME. American Society of Mechanical Engineers.

DoD. The U.S. Department of Defense.

DOE. The U.S. Department of Energy.

CAS. Central Alarm Station.

CFR. Code of Federal Regulations.

OSHA. The U.S. Department of Labor, Occupational Safety & Health Administration.

NFPA. National Fire Protection Association.

REVCOM. The U.S. Department of Energy Directives Review and Comment System.

ROWS. Remotely Operated Weapon System.

SQA. Software Quality Assurance.

APPENDIX B
AGENCY-SPECIFIC AND INFORMATIVE REFERENCES

- B.1 DOE O 414.1C, “Quality Assurance,” U.S. Department of Energy. Note: This order is mandatory for DOE purchasers.
- B.2 10 CFR 830, Subpart A, “Quality Assurance Requirements,” U.S. Department of Energy. Note: This regulation is mandatory for DOE purchasers.
- B.3 10 CFR 830, Subpart B, “Safety Basis Requirements,” U.S. Department of Energy. Note: This regulation is mandatory for DOE purchasers.
- B.4 MIL-STD-882D, “Standard Practice for System Safety,” U.S. Department of Defense. Note: This standard is mandatory for military purchasers.
- B.5 MIL-STD-1472F, “Design Criteria Standard – Human Engineering,” U.S. Department of Defense. Note: This standard is mandatory for military purchasers.
- B.6 “Unmanned Systems Safety Guide for DoD Acquisition,” 27 June 2007, U.S. Department of Defense.
- B.7 DOE G 414.1-4, “Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance,” U.S. Department of Energy.
- B.8 ANSI/ANS 10.4, “Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry,” American Nuclear Society.
- B.9 IEC 61508:2000, Parts 1-7, “Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems,” International Electrotechnical Commission.
- B.10 NFPA 780, “Standard for the Installation of Lightning Protection Systems,” National Fire Protection Association.
- B.11 DOE-HDBK-1140-2001, “Human Factors/Ergonomics Handbook for the Design for Ease of Maintenance,” U.S. Department of Energy.
- B.12 NISTIR 4909, “Software Quality Assurance: Documentation and Reviews,” U.S. Department of Commerce, National Institute of Standards and Technology.
- B.13 DOE M 470.4-1, Attachment 2, Part 1, Section F, “Performance Assurance Program,” U.S. Department of Energy. Note: This manual is mandatory for DOE purchasers.

- B.14 15 CFR 287, “Guidance on Federal Conformity Assessment,” U.S. Department of Commerce, National Institute of Standards and Technology.
- B.15 “Firearm Safety Rules” and “Glossary,” Sporting Arms and Ammunition Manufacturers’ Institute, Inc. (SAAMI), <http://www.saami.org/index.cfm>.
- B.16 10 CFR 851, “Worker Safety and Health Program,” U.S. Department of Energy. Note: This regulation is mandatory for DOE purchasers.
- B.17 DOE O 440.1B, “Worker Protection Program for DOE (including the National Nuclear Security Administration) Federal Employees,” U.S. Department of Energy. Note: This order is mandatory for DOE purchasers.
- B.18 UL 681, “Standard for Installation and Classification of Burglar and Holdup Alarm Systems,” Underwriters Laboratories, Inc.
- B.19 DOE M 440.1-1A, “DOE Explosives Safety Manual,” U.S. Department of Energy. Note: This manual is mandatory for DOE purchasers.
- B.20 DOE O 420.1B, “Facility Safety,” U.S. Department of Energy. Note: This order is mandatory for DOE purchasers.

APPENDIX C

RECOMMENDATIONS FOR PURCHASERS (INFORMATIVE)

The procurers of remotely operated weapon systems should consider whether their procedures and the systems under consideration include the following minimum safety functions and features.

C.1 ENGINEERED SECTOR-LIMITING STOPS.

- C.1.1 Hardware limit stops should be implemented to protect no-fire zones within the weapon's primary engagement sector (e.g., restrict platform movement in applications where the full range of elevation/depression and slew is not required).

C.2 ELECTRICAL CIRCUITS.

- C.2.1 If operated near other electronic equipment or systems, the ROWS should not emit electromagnetic interference that adversely affects these systems nor should the ROWS electronics be affected by other electronic equipment.
- C.2.2 ROWS placed in elevated positions external to a building should be protected against lightning as required by NFPA 780, "Standard for the Installation of Lightning Protection Systems."
- C.2.3 Backup power should be provided to critical fixed ROWS platforms and operator control stations to support operation in case of loss of power. Systems should be protected against power surge.
- C.2.4 The ROWS should allow the operator to remotely charge a weapon.
- C.2.5 For systems to be installed in nuclear material storage vaults, the purchaser should evaluate the effect of radiation upon ROWS semiconductors and electrical circuits.
- C.2.6 For systems to be installed near explosives operating areas, the purchaser should review and ensure compliance with electrical grounding requirements.
- C.2.7 A review should be conducted to ensure that safety-critical circuits do not contain malicious components.
- C.2.8 A vulnerability analysis should be conducted to determine whether electronic and optical components or circuits contain a vulnerability which could be exploited by an adversary.

- C.3.3 For systems to be installed in nuclear material process areas, the purchaser should evaluate the effect of process chemicals (e.g., acids) upon ROWS hardware.

C.3 MAINTENANCE FUNCTIONS AND FEATURES.

- C.3.1 Components should be easily accessible for maintenance.
- C.3.2 ROWS utilized on the range should allow the operator to remove brass and debris without having to climb into the enclosure.

C.4 LASERS (if any).

- C.4.1 If the system includes one or more lasers (e.g., for range finding), it may be necessary to designate a “laser safe” zone around the platform when it is in its normal operating mode.

C.5 AIMING SYSTEM AND OPTICS.

- C.5.1 The aiming system shall be compatible with engagement simulation systems (ESS) and other performance testing equipment.

C.6 PLATFORM ENCLOSURE (if any).

- C.6.1 Stationary ROWS platform enclosures should provide tamper detection capability. Tamper alarms should meet requirements of UL 681.

C.7 COMMAND AND CONTROL FUNCTIONS.

- C.7.1 The operator’s control station should employ locks, passwords, or other means to prevent unauthorized control of the weapon platform. Setup and maintenance screens should be password protected to allow access by maintenance personnel only.
- C.7.2 The system may include a 2-person enable capability.
- C.7.3 Combat damage to the system should not result in inadvertent firing of the weapon.

C.8 COMMUNICATIONS AND NETWORKING FUNCTIONS.

- C.8.1 For systems to be installed near explosives operating areas, the purchaser should evaluate the effects of wireless communications systems (if used) upon explosive components sensitive to static or electromagnetic radiation.

C.9 FUNCTIONS AND FEATURES RELATED TO HUMAN FACTORS.

- C.9.1 Human factors should be considered in the design of the system. See DOE-HDBK-1140-2001, “Human Factors/Ergonomics Handbook for the Design for Ease of Maintenance.”
- C.9.2 Displays should employ color coding and symbolic representation that improves controllers’ abilities to respond effectively.

C.10 TRAINING.

- C.10.1 Training requirements for electronic technician maintenance personnel should be documented and implemented as specified by the manufacturer.
- C.10.2 Operational and training ROWS should be functionally identical units.
- C.10.3 The vendor should support purchasers’ training programs.
- C.10.4 The purchaser should have a documented training and qualification process, which includes safety requirements, for personnel who maintain or operate the ROWS.

C.11 SAFETY-CRITICAL SOFTWARE (if any).

- C.11.1 A review should be conducted to ensure that code is not retained that could cause malfunction (e.g., dead code, virus code, malicious code, ghosting, spoofing).

C.12 TESTING FUNCTIONS AND FEATURES.

- C.12.1 The system should include a built-in test capability that can monitor the functional status of system components (e.g., platform controllers, communications cables, batteries and devices, etc.).
- C.12.2 Whenever the weapon is changed on the ROWS platform, the functionality of the system should be tested (e.g. test the trigger and safety solenoid, ensure the aiming system is aligned correctly).

C.13 SYSTEM DOCUMENTATION.

- C.13.1 The vendor’s software quality assurance documents (e.g., system requirements, project planning and development documentation, review reports) should be examined.
- C.13.2 Each DOE purchaser submitting a “lessons learned” or accident/incident report involving the malfunction of a ROWS should use the word “ROWS” in the title,

so that this information is easily retrieved by other organizations and during revision of this standard.

- C.13.3 Upon request, DOE purchasers should provide other DOE contractors with approved documentation confirming compliance with the requirements of this standard in accordance with 15 CFR Part 287, “Guidance on Federal Conformity Assessment.”
- C.13.4 A manuscript or electronic logbook should be maintained to document operator logons, system maintenance, and system performance tests. If installed, the system should have the capability to automatically provide an electronic record of operator actions, including time, platform commands, and weapon condition data for training and system performance analysis.

DOE F 1300.3 (01-94)		U.S. DEPARTMENT OF ENERGY DOCUMENT IMPROVEMENT PROPOSAL (Instructions on Reverse)		OMB Control No. 1910-0900 OMB Burden Disclosure Statement on Reverse	
1. Document Number		2. Document Title			
3a. Name of Submitting Organization			4. Type of Organization (Mark one)		
3b. Address (Street, City, Zip Code)			☐ Vendor		
			☐ User		
			☐ Manufacturer		
			☐ Other (Specify: _____)		
5. Problem Areas (Attach extra sheets as needed.)					
a. Paragraph Number and Wording					
b. Recommended Wording					
c. Reason/Rationale for Recommendation					
6. Remarks					
7a. Name of Submitter (Last, First, MI)			7b. Work Telephone Number (Include Area Code)		
7c. Mailing Address (Street, City, State, Zip Code)			8. Date of Submission		



Printed with soy ink on recycled paper

DOE-STD-1047-2008

DOE F 1300.3
(01-94)

OMB Control No.
1910-0900

INSTRUCTIONS: In a continuing effort to improve the U.S. Department of Energy (DOE) Technical Standards, this form is provided for use in submitting comments and suggestions for improvements. All users of DOE Technical Standards are invited to provide suggestions. This form may be detached, folded along the lines indicated, taped along the loose edge (DO NOT STAPLE) mailed to the address indicated or faxed to (615) 574-0382.

1. The submitter of this form must complete blocks 1 through 8.
2. The Technical Standards Program Office (TSPO) will forward this form to the Preparing Activity. The Preparing Activity will reply to the submitter within 30 calendar days of receipt from the TSPO.

NOTE: This form may not be used to request copies of documents, nor to request waivers, deviations, or clarification of specification requirements on current contractors. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management Policy, Plans, and Oversight, Records Management Division, HR-422 - GTN, Paperwork Reduction Project (1910-0900), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-0900), Washington, DC 20503.

U.S. Department of Energy Technical Standards Program Office
c/o Performance Assurance Project Office
P.O. Box 2009, Bldg. 9201-3
Oak Ridge, Tennessee 37831-8065

CONCLUDING MATERIAL

Review Activities:

DOE
HSS
EM
FE
MA
NE
NNSA
RW
SC

Preparing Activity:

DOE/HS-82

Project Number:

SAFT-0116

Area and Site Offices

Carlsbad Field Office
Chicago Operations Office
Idaho Operations Office
Kansas City Site Office
Livermore Site Office
Los Alamos Site Office
Nevada Site Office
NNSA Service Center
Oak Ridge Operations Office
Pittsburg Naval Reactors Site Office
Richland Operations Office
Sandia Site Office
Savannah River Operations Office
Schenectady Naval Reactors Site Office
Y-12 Site Office