



National Aeronautics and
Space Administration

Moon to Mars

M2M-30043

INITIAL RELEASE

RELEASE DATE: MAY 7, 2024

MOON TO MARS (M2M) CROSS PROGRAM UTILIZATION PAYLOAD SAFETY REQUIREMENTS

This document has been reviewed for Proprietary, CUI, and Export Control (ITAR/EAR) and has been determined to be non-sensitive. It has been released to the public via the NASA Scientific and Technical Information (STI) Process DAA 20240007393.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 2 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

REVISION AND HISTORY PAGE

Revision No.	Change No.	Description	Release Date
-	CR ACD-C0052 Rev A	Initial Release, approved by the M2MCB OSB (Reference M2M-D0052, dated 5/7/24)	05/07/24

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 3 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE OF CONTENTS

SECTION	PAGE
1.0 INTRODUCTION	11
1.1 PURPOSE.....	11
1.2 BACKGROUND	11
1.3 SCOPE.....	11
1.4 REQUIREMENT CONVENTION AND NOTATION	13
1.5 TERMINOLOGY	14
1.6 MEASUREMENT UNITS	14
1.7 CHANGE AUTHORITY/RESPONSIBILITY	15
2.0 DOCUMENTS.....	16
2.1 APPLICABLE DOCUMENTS.....	16
2.2 REFERENCE DOCUMENTS	18
3.0 SAFETY REQUIREMENTS FOR CROSS-PROGRAM UTILIZATION PAYLOADS... 20	
3.1 CORE SMA REQUIREMENTS.....	20
3.2 FAILURE TOLERANCE.....	21
M2M-SMA-UTIL-R-2001 Failure Tolerance to Catastrophic Hazards	21
M2M-SMA-UTIL-R-2002 Failure Tolerance to Critical Hazards	22
M2M-SMA-UTIL-R-2003 Redundant Paths	23
M2M-SMA-UTIL-R-2003-1 Redundant Paths – Separate Connectors	23
M2M-SMA-UTIL-R-2003-2 Redundant Paths – Separation Distance	23
M2M-SMA-UTIL-R-2004 Capability without Emergency Equipment and Systems	23
M2M-SMA-UTIL-R-2005 Safe Without Services	23
M2M-SMA-UTIL-R-2006 Failure Propagation	23
M2M-SMA-UTIL-R-2007 Payload Controls for Human Error	24
3.3 ENVIRONMENTAL COMPATIBILITY	25
M2M-SMA-UTIL-R-2008 Safe in All Natural Environments	25
3.3.1 PLASMA	25
M2M-SMA-UTIL-R-2009 Plasma Environments	25
M2M-SMA-UTIL-R-2010 Ionizing Radiation	25
M2M-SMA-UTIL-R-2011 Inadvertent Activation Protection	26
M2M-SMA-UTIL-R-2012 Induced Environments	26
3.4 STRUCTURES AND FASTENERS	26
M2M-SMA-UTIL-R-2013 Payload Structural Design	27
M2M-SMA-UTIL-R-2014 Safety Critical Structures	27
M2M-SMA-UTIL-R-2015 Payload Glass or Ceramic Structures	27
M2M-SMA-UTIL-R-2016 Payload Fasteners	27
3.5 MECHANISMS.....	27
M2M-SMA-UTIL-R-2017 Payload Mechanisms	27
3.6 PRESSURE SYSTEMS/VESSELS	28
M2M-SMA-UTIL-R-2018 Payload Pressure System	29

Revision: Initial Release (Draft)		Document No: M2M-30043
Release Date: TBD		Page: 4 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements		
M2M-SMA-UTIL-R-2019	Payload Thin Walled Flexible Pressure Boundary Hardware	29
M2M-SMA-UTIL-R-2020	Sealed Payload Containers for Ascent or EVA	29
M2M-SMA-UTIL-R-2021	Vented Payload Containers	30
M2M-SMA-UTIL-R-2022	Unintentionally Sealed Payload Containers	30
3.7	ELECTRICAL	31
M2M-SMA-UTIL-R-2023	Payload Circuit Protection	31
M2M-SMA-UTIL-R-2024	Payload Safe State Indication	31
M2M-SMA-UTIL-R-2025	Separation of Redundant Safety Critical Circuits	31
M2M-SMA-UTIL-R-2026	Protection of Critical Payload Controls	32
M2M-SMA-UTIL-R-2027	Electrical Connector Scoop Proof Design	32
M2M-SMA-UTIL-R-2028	Bonding and Isolation	32
M2M-SMA-UTIL-R-2029	Electrolytic Capacitors	33
M2M-SMA-UTIL-R-2030	IVA/EVA/EVR Connector Mate/Demate Inhibit and Design	33
M2M-SMA-UTIL-R-2031	IVA 2nd Verifiable Upstream Inhibit for Mating/Demating Electrical Power Connectors	34
M2M-SMA-UTIL-R-2032	Extravehicular 2nd Inhibit for Mating/Demating Electrical Power Connectors (Voltage >= 200 Vdc/RMS or Current >= 67 Amps)	34
M2M-SMA-UTIL-R-2033	Extravehicular 2nd Inhibit for Mating/Demating Electrical Power Connectors (Voltage < 200 Vdc/RMS and Current < 67 Amps)	35
3.8	PAYLOAD BATTERIES	35
M2M-SMA-UTIL-R-2034	Payload Batteries	36
M2M-SMA-UTIL-R-2035	Payload Battery Management System	36
M2M-SMA-UTIL-R-2036	Overcharge Failure/Over-discharge Failure Protection	36
M2M-SMA-UTIL-R-2037	Payload Battery Temperature Extreme Protection	37
M2M-SMA-UTIL-R-2038	Payload Battery External Short Protection	37
M2M-SMA-UTIL-R-2039	Payload Battery Reverse Current Protection	37
M2M-SMA-UTIL-R-2040	Payload Battery Cell Reverse Protection	37
M2M-SMA-UTIL-R-2416	Payload Battery Cell Leakage Protection	37
M2M-SMA-UTIL-R-2042	Payload Battery Overpressurization Protection	38
M2M-SMA-UTIL-R-2043	Payload Battery Cell-to-Cell Separation	38
3.9	ELECTROMAGNETIC COMPATIBILITY	38
3.9.1	Electromagnetic Effects (EME)	38
3.9.2	Protecting Against Hazardous RF Irradiation	38
M2M-SMA-UTIL-R-2044	Payload RF Transmission Protection	38
3.10	PAYLOAD COMMAND AND DATA HANDLING (C&DH)	39
M2M-SMA-UTIL-R-2045	Ground Initiated Hazardous Payload Commanding	40
M2M-UTIL-INFO-0001	Payload Safing	41
M2M-SMA-UTIL-R-2046	Identification of Payload Hazardous Commands	41
M2M-SMA-UTIL-R-2047	Payload Two-Step Hazardous Commands	41
M2M-SMA-UTIL-R-2048	Autonomous Operation	41
3.11	MONITORING.....	42
M2M-SMA-UTIL-R-2049	Payload Monitoring <TBR-30043-001>	42
M2M-SMA-UTIL-R-2050	Payload Monitoring Without Reducing Safety	42
M2M-SMA-UTIL-R-2051	Payload Lost Monitoring Identifiable	43
M2M-SMA-UTIL-R-2052	Utilization Payload Inhibits	43
M2M-SMA-UTIL-R-2053	Payload Timers	43

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 5 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.12	SOFTWARE.....	44
	M2M-SMA-UTIL-R-2054 Payload Safety Critical Software	44
	M2M-SMA-UTIL-R-2055 Flight Software Development	45
	M2M-SMA-UTIL-R-2055-001 Non-CBCS Compliant System Segregation	46
	M2M-SMA-UTIL-R-2055-002 Safe Initialization	46
	M2M-SMA-UTIL-R-2055-003 Safe Termination	46
	M2M-SMA-UTIL-R-2055-004 Off Nominal-Power Conditions	46
	M2M-SMA-UTIL-R-2055-005 Actions for Overrides	47
	M2M-SMA-UTIL-R-2055-006 Commands Out of Sequence	47
	M2M-SMA-UTIL-R-2055-007 Inadvertent Memory Modification	47
	M2M-SMA-UTIL-R-2055-008 Input Validation	47
	M2M-SMA-UTIL-R-2055-009 Integrity Check	48
	M2M-SMA-UTIL-R-2055-010 Prerequisite Checks	48
	M2M-SMA-UTIL-R-2055-011 Disarming an Armed Command	48
	M2M-SMA-UTIL-R-2055-012 Unique Command Messages	48
	M2M-SMA-UTIL-R-2055-013 One Operator Action	48
	M2M-SMA-UTIL-R-2055-014 Redundant Command Path	49
	M2M-SMA-UTIL-R-2055-015 Redundant Command Path Independence	49
	M2M-SMA-UTIL-R-2055-016 Failure Independence	49
	M2M-SMA-UTIL-R-2055-017 Change of State of Inhibits	49
	M2M-SMA-UTIL-R-2055-018 Independent Parameter for FCA	49
	M2M-SMA-UTIL-R-2055-019 Independent Control of an Inhibit	50
	M2M-SMA-UTIL-R-2055-020 Fault Detection and Annunciation	50
	M2M-SMA-UTIL-R-2055-021 Recover from CBCS Anomaly	50
	M2M-SMA-UTIL-R-2055-022 Data for Manual Safing	50
	M2M-SMA-UTIL-R-2055-023 Controlled System Failure Detection	51
	M2M-SMA-UTIL-R-2055-024 Notification of Safing	51
	M2M-SMA-UTIL-R-2055-025 Safing Actions	51
	M2M-SMA-UTIL-R-2055-026 Failure Resolution	51
	M2M-SMA-UTIL-R-2055-027 Unique Detection and Safing	51
	M2M-SMA-UTIL-R-2055-028 Independent Controller Monitor	52
	M2M-SMA-UTIL-R-2055-029 Use of Timers	52
	M2M-SMA-UTIL-R-2055-030 Monitor Capabilities	52
3.13	MATERIALS AND PROCESSES	52
	3.13.1 Materials Selection	53
	M2M-SMA-UTIL-R-2056 Payload Materials	54
	3.13.2 Flammability Hazard Level (FHL) Hazard Rating	54
	3.13.3 Material Offgassing	56
	M2M-SMA-UTIL-R-2057 Non-Metallic Materials Off-gassing	56
	M2M-SMA-UTIL-R-2058 Material Out-gassing	57
	M2M-SMA-UTIL-R-2059 Materials and Fluid Compatibility	57
	3.13.4 Hazardous Materials	57
	3.13.5 Chemicals	59
	M2M-SMA-UTIL-R-2060 Chemical Release	59
	3.13.6 Toxicity Hazard Level (THL) Hazard Rating	60

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 6 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2061	Reduction In Failure Tolerance For Chemicals (Liquids) During Operations	63
M2M-SMA-UTIL-R-2062	Radioactive Payload Material Release	63
3.14	IN-FLIGHT BIOSAFETY LEVEL	64
M2M-SMA-UTIL-R-2063	Biological Material Release	65
3.14.1	Animals	65
3.15	PHYSICAL AGENTS	66
M2M-SMA-UTIL-R-2064	Physical Agents Release	66
M2M-SMA-UTIL-R-2065	Particle Release	67
M2M-SMA-UTIL-R-2066	Containment of Shatterable Materials	68
M2M-SMA-UTIL-R-2067	Fluid Release	68
M2M-SMA-UTIL-R-2068	Contamination Control	69
M2M-SMA-UTIL-R-2069	Payload Pre-Flight Microbial Contamination	69
M2M-SMA-UTIL-R-2070	Visibly Clean Internal Payloads (Habitable)	69
M2M-SMA-UTIL-R-2071	Visibly Clean External Payloads	69
3.15.1	Shatterable Materials	69
M2M-SMA-UTIL-R-2072	Shatterable Materials Release	70
M2M-SMA-UTIL-R-2073	Use of Shatterable Materials	70
M2M-SMA-UTIL-R-2074	Optical Glass Protection	70
3.16	RESERVED	70
3.17	FIRE PROTECTION	70
3.17.1	Fire Prevention	70
3.17.2	Fire Detection and Fire Suppression	71
3.18	HUMAN SYSTEMS SAFETY (IVA)	71
3.18.1	Acoustics	71
M2M-SMA-UTIL-R-2075	Impulse Noise Hazard Limit	72
M2M-SMA-UTIL-R-2076	Intermittent Noise Limits	72
M2M-SMA-UTIL-R-2077	Payload Audible Alarm	73
M2M-SMA-UTIL-R-2078	Audible Alarm Hazard Limit	74
3.18.2	IVA TOUCH TEMPERATURE	74
M2M-SMA-UTIL-R-2079	Touch Temperature Limits	75
M2M-SMA-UTIL-R-2080	Touch Temperature Based on Payload Functionality	75
3.18.3	IVA CREW CONTACT HAZARDS	76
M2M-SMA-UTIL-R-2081	Sharp Edges and Protrusions	76
M2M-SMA-UTIL-R-2082	IVA Levers, Cranks, Hooks, and Controls	77
M2M-SMA-UTIL-R-2083	IVA Use of Safety Wire	77
M2M-SMA-UTIL-R-2084	Clearance for Entrapment Hazard	77
M2M-SMA-UTIL-R-2085	Sharp Item Hazard	78
M2M-SMA-UTIL-R-2086	Burrs	78
M2M-SMA-UTIL-R-2087	Pinch Points	78
M2M-SMA-UTIL-R-2088	Holes	78

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 7 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.18.4	IVA CREW LIFTING AND HANDLING HAZARDS	78
3.18.5	PAYLOAD CONNECTOR AND INSTALLATION HAZARDS	79
M2M-SMA-UTIL-R-2089	Payload Connector Actuation without Tools	79
M2M-SMA-UTIL-R-2090	Incorrect Payload Mating, Demating Prevention	79
M2M-SMA-UTIL-R-2091	Incorrect Payload Installation	79
M2M-SMA-UTIL-R-2092	Crew Hazards Related to Electrical Shock	79
3.18.6	LASERS AND BROADBAND LIGHT	80
M2M-SMA-UTIL-R-2093	Lasers - General	80
M2M-SMA-UTIL-R-2094	Magnification of Lasers	81
M2M-SMA-UTIL-R-2095	Class 3R, 3B, and 4 Lasers	81
M2M-SMA-UTIL-R-2096	Payload Provided Lighting	82
M2M-SMA-UTIL-R-2097	Infrared Radiation (IR) Light Exposure from Payloads	82
M2M-SMA-UTIL-R-2098	Ultraviolet (UV) Radiation Light Exposure from Payloads	82
3.18.7	EMERGENCY RESPONSE	82
M2M-SMA-UTIL-R-2099	Egress from Payload Apparatus	82
M2M-SMA-UTIL-R-2100	Intramodule Emergency Egress	82
M2M-SMA-UTIL-R-2101	Hatch Drag-Throughs	83
3.19	EXTRAVEHICULAR ACTIVITY (EVA)	83
M2M-SMA-UTIL-R-2102	EVA Payload Safety Requirements	84
3.20	GRAPHICAL USER INTERFACE (GUI)	85
M2M-SMA-UTIL-R-2103	Interpretation of Payload Display Information	86
M2M-SMA-UTIL-R-2104	Maximum System Response Time to Crew Input	86
M2M-SMA-UTIL-R-2105	Violation of Operational Limit	86
M2M-SMA-UTIL-R-2106	Stale Data Indication	87
M2M-SMA-UTIL-R-2107	Telemetry Outside Upper or Lower Thresholds	87
M2M-SMA-UTIL-R-2108	Off Scale Indication	87
M2M-SMA-UTIL-R-2109	Sufficient Fixed Placeholder Width	87
M2M-SMA-UTIL-R-2110	Text Data Overflow Indicator	87
M2M-SMA-UTIL-R-2111	Numeric Data Overflow Indicator	88
M2M-SMA-UTIL-R-2112	Critical Data Update Rate	88
M2M-SMA-UTIL-R-2113	Distinguishable Payload Commands	88
M2M-SMA-UTIL-R-2114	Hazardous Payload Commands	88
M2M-SMA-UTIL-R-2115	Payload Display of Status and Error Messages	88
M2M-SMA-UTIL-R-2116	Payload Display Character Height	88
M2M-SMA-UTIL-R-2117	Payload Display Numeric Value	89
M2M-SMA-UTIL-R-2118	Payload Display Off-nominal Values	89
M2M-SMA-UTIL-R-2119	Payload Display Use of Color	89
M2M-SMA-UTIL-R-2120	Payload Graph Display - Off-Nominal Data	89
M2M-SMA-UTIL-R-2121	Termination of Flashing	89
3.21	MICROMETEOROID AND ORBITAL DEBRIS	90
M2M-SMA-UTIL-R-2122	Micrometeoroid and Orbital Debris (MMOD)	90
M2M-SMA-UTIL-R-2123	Payloads Limiting Orbital Debris	90
3.22	PROPULSION.....	91
3.23	PYROTECHNIC SYSTEMS	91

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 8 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2124	Pyrotechnics	91
M2M-SMA-UTIL-R-2125	Pyrotechnic Loss of Function (Must Work)	91
M2M-SMA-UTIL-R-2126	Pyrotechnic Inadvertent Function	91
M2M-SMA-UTIL-R-2127	Electrical Explosive Devices	92
M2M-SMA-UTIL-R-2128	Pyrotechnic Mechanical Containment	92
M2M-SMA-UTIL-R-2129	Transportation of Payloads with Pyrotechnics	93
3.24	PLANETARY PROTECTION	93
M2M-SMA-UTIL-R-2130	Cross-Program Utilization Payload Planetary Protection	93
M2M-SMA-UTIL-R-2131	Cross-Program Utilization Payload Lunar Surface Disposal	93
3.25	SAMPLE RETURN	94
M2M-SMA-UTIL-R-2132	Sample Return Requirements	94
3.26	GROUND SAFETY	94
3.26.1	TRAINING	94
M2M-SMA-UTIL-R-3000	Safety and Health	94
M2M-SMA-UTIL-R-3001	Facility and Operating Site	94
3.26.2	HAZARDOUS OPERATIONS	95
M2M-SMA-UTIL-R-3002	Hazardous Ground Operations	95
3.26.3	SAFETY EQUIPMENT	95
M2M-SMA-UTIL-R-3003	Personnel Protection	95
M2M-SMA-UTIL-R-3004	Industrial Safety Practices	95
3.26.4	PERSONNEL SAFETY	96
M2M-SMA-UTIL-R-3005	Human Factors for Ground Personnel	96
M2M-SMA-UTIL-R-3006	GSE Design	96
M2M-SMA-UTIL-R-3007	Human Interfaces	96
M2M-SMA-UTIL-R-3008	Human Error	96
M2M-SMA-UTIL-R-3009	Physical	96
M2M-SMA-UTIL-R-3010	Temperature	97
M2M-SMA-UTIL-R-3011	Radiation	97
M2M-SMA-UTIL-R-3012	Radiation Program Documents	97
M2M-SMA-UTIL-R-3013	Radiation Sources	97
M2M-SMA-UTIL-R-3014	Radiation Personnel Exposure	97
M2M-SMA-UTIL-R-3015	Radiation Safety - Sources	98
M2M-SMA-UTIL-R-3016	Radiation Safety - Systems	98
M2M-SMA-UTIL-R-3017	General Optical Requirements	98
M2M-SMA-UTIL-R-3018	Optical - Maximum Permissible Exposure	98
M2M-SMA-UTIL-R-3019	Laser Systems	98
M2M-SMA-UTIL-R-3020	Laser System Requirements	99
3.26.5	PAYLOADS AND GROUND SUPPORT EQUIPMENT (GSE)	99
M2M-SMA-UTIL-R-3021	Ground Support Equipment	99
M2M-SMA-UTIL-R-3022	Biomedical Subsystems	99
M2M-SMA-UTIL-R-3023	Electrical Connector - Mismatch	99
M2M-SMA-UTIL-R-3024	Electrical Connector – Scoop Proof	99
M2M-SMA-UTIL-R-3025	Electrical Cabling	99
M2M-SMA-UTIL-R-3026	Electrical Requirements	100
M2M-SMA-UTIL-R-3027	Battery Requirements	100

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 9 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-3028	Grounding, Bonding, And Shielding	100
M2M-SMA-UTIL-R-3029	Ground Potential	100
M2M-SMA-UTIL-R-3030	Electrical Maintenance Operations	100
M2M-SMA-UTIL-R-3031	Electrical Fuses	100
M2M-SMA-UTIL-R-3032	Ordnance Categorization	100
M2M-SMA-UTIL-R-3033	Ordnance – Category A	101
M2M-SMA-UTIL-R-3034	General Ordnance Requirements	101
M2M-SMA-UTIL-R-3035	Ordnance Testing	101
M2M-SMA-UTIL-R-3036	Ordnance Operations	101
M2M-SMA-UTIL-R-3037	Ordnance Operation Location	101
M2M-SMA-UTIL-R-3038	Ordnance Test Equipment – Limited Energy Input	101
M2M-SMA-UTIL-R-3039	Ordnance - In-Calibration Test Equipment	102
M2M-SMA-UTIL-R-3040	Ordnance – Materials Susceptibility	102
M2M-SMA-UTIL-R-3041	Ordnance – Disposal	102
M2M-SMA-UTIL-R-3042	Ordnance – EED Faraday Caps	102
M2M-SMA-UTIL-R-3043	Ordnance – Nonflight Color-Coded	102
M2M-SMA-UTIL-R-3044	Ordnance Test Equipment	102
M2M-SMA-UTIL-R-3045	GSE Materials List	102
M2M-SMA-UTIL-R-3046	GSE - Degradation / Contamination	103
M2M-SMA-UTIL-R-3047	GSE - Mercury Use	103
M2M-SMA-UTIL-R-3048	Mercury Contamination / Personnel Exposure	103
M2M-SMA-UTIL-R-3049	Cleaning Solvents / Adhesives	103
M2M-SMA-UTIL-R-3050	Plastic Films, Foams, and Adhesive Tapes	103
M2M-SMA-UTIL-R-3051	Plastic Films, Foams, and Adhesive Tapes - SDS	103
M2M-SMA-UTIL-R-3052	GSE – Shatterable Materials	104
M2M-SMA-UTIL-R-3053	GSE – Flammability Requirements	104
M2M-SMA-UTIL-R-3054	GSE – Painted Or Coated Materials	104
M2M-SMA-UTIL-R-3055	Contamination - Nutrients for Biological Agents	104
M2M-SMA-UTIL-R-3056	Industrial Hygiene	104
M2M-SMA-UTIL-R-3057	Industrial Hygiene – Hazardous Materials / Physical Agents Exposure	104
3.27	PAYLOAD DISPOSAL.....	105
4.0	VERIFICATION	106
4.1	VERIFICATION METHOD DEFINITIONS	106
APPENDIX A	- ACRONYMS AND ABBREVIATIONS AND GLOSSARY OF TERMS	108
A1.0	ACRONYMS AND ABBREVIATIONS	108
A2.0	GLOSSARY OF TERMS.....	112
APPENDIX B	- OPEN WORK	118
B1.0	TO BE DETERMINED.....	118
B2.0	TO BE RESOLVED	118
B3.0	FORWARD WORK.....	119

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 10 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE

TABLE 2.1-1 APPLICABLE DOCUMENTS	16
TABLE 2.2-1 REFERENCE DOCUMENTS	18
TABLE 3.6-1 PRESSURE SYSTEMS CLASSIFICATIONS	28
TABLE 3.13.2-1 FLAMMABILITY HAZARD LEVEL (FHL) AND HAZARD SEVERITY	56
TABLE 3.13.4-1 LEVELS OF CONTAINMENT/CONTROL AND HAZARD RATINGS	58
TABLE 3.13.6-1 TOXICITY HAZARD LEVEL (THL) AND HAZARD SEVERITY	61
TABLE 3.13.6-2 ECLSS HARDWARE IMPACT RATING (E RATING) AND HAZARD SEVERITY	62
TABLE 3.14-1 NASA IN-FLIGHT BIOSAFETY LEVEL RATING AND HAZARD SEVERITY.....	65
TABLE 3.15-1 PHYSICAL AGENTS AND HAZARD SEVERITY	68
TABLE 3.18.1-1 INTERMITTENT NOISE A-WEIGHTED OVERALL SOUND PRESSURE LEVEL AND CORRESPONDING OPERATIONAL DURATION LIMITS (MEASURED AT 0.6M)	72
TABLE 3.18.3-1 CORNERS AND EDGES I	76
TABLE 3.18.3-2 CORNERS AND EDGES II	77
TABLE 3.18.5-1-3 CREW SAFETY ELECTRICAL CURRENT LIMITS	80
TABLE 3.19-1 EVA PAYLOAD SAFETY REQUIREMENTS	84
TABLE 3.20.1-1 MAXIMUM SYSTEM RESPONSE TIME TO CREW INPUT	86
TABLE 3.20.1-2 PAYLOAD DISPLAY COLORS	89
TABLE B1-1 TO BE DETERMINED ITEMS	118
TABLE B2-1 TO BE RESOLVED ISSUES	118
TABLE B3-1 FORWARD WORK	119

FIGURE

FIGURE 1.3-1 CROSS-PROGRAM UTILIZATION PAYLOADS	12
FIGURE 3.10-1 C&DH TO PAYLOADS CONTEXT DIAGRAM.....	40
FIGURE 3.18.1-1 INTERMITTENT NOISE LIMITS	73
FIGURE 3.18.2-1 SUMMARY OF BARE SKIN EXPOSURE TEMPERATURE RANGES	75

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 11 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

1.0 INTRODUCTION

1.1 PURPOSE

This Moon to Mars (M2M) Cross-Program Utilization Payload Safety Requirements document facilitates Utilization Payload Developers (PDs) access to, and compliance with, Moon to Mars Program Requirements. It collates and captures a set of requirements that satisfy requirements for all M2M Programs. While the individual Programs retain ownership of their technical requirements, this document governs requirements for cross-program utilization payloads that cross Program vehicle hatches or operate externally on multiple Program vehicles during transport or operation.

Tailoring of these requirements is captured in the utilization payload project's requirements documentation and requires approval from the M2M Control Board (M2MCB), applicable joint integration Program control board, or delegate. Thus, verification to the set of requirements in this document is meant to suffice as verification for M2M Programs' safety requirements. This document will be updated as necessary by M2M SMA and represents a common (across Moon to Mars Programs) understanding of applicable safety requirements.

1.2 BACKGROUND

Each program under M2M is governed by NASA HQ level requirements documents. Tailoring of those higher level requirements for the needs of each specific Program has sometimes resulted in different requirement language being adopted by each Program. So even though the Program requirements are meant to satisfy the same governing requirements, the combined M2M SMA team worked to compare language and choose a "common" requirement. In most cases, the requirements language was identical, or very nearly so. In cases of apparent disagreement, the default was to choose the language of the most conservative requirements so as to meet the intent of all other requirements. In select cases, rationale was provided to choose a requirement that was not the most conservative.

1.3 SCOPE

This document is applicable to cross-program utilization payloads. Cross-Program Utilization payloads are payloads that can interface with more than one Lunar exploration vehicle. They include payloads dedicated to utilization, such as science, research, development, test and evaluation, public outreach, education, and commercialization, and does not cover Common Exploration Systems Development (CESD) Primary or Co-Manifested Payloads (CPLs), or secondary payloads with the SLS Program (or other Programs) that fall outside of the Artemis utilization campaign. The Program unique utilization payload requirement documents take precedence for utilization payloads that do not interface with multiple M2M programs. Figure 1.3-1 provides a visual aid to explain cross-program utilization payload. Cross-program payloads are those that are transported or operated in/on more than one Program vehicle/spacecraft or have the possibility of affecting more than one vehicle/spacecraft. Payloads may, either in transport or operation, represent a hazard to the safety of the ground and flight crew or multiple Program vehicles for any given Artemis mission from pre-launch to recovery.

Exploration Ground System (EGS) Payload Safety Review Panel (PSRP) will be

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 12 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

identified as an ad-hoc Stakeholder program for utilization payloads that have pre-launch and/or post-landing and recovery ground processing activities. EGS norm is that payloads that are active while the crew is present on Orion are under control of the launch control system (prime launch team). Given that, it follows that utilization payloads that are active during launch countdown must adhere to the same rules. Payloads are either powered off during launch countdown or are under control of the prime launch team.

Section 3 provides the safety requirements. Cross-Program Utilization Payload interoperable M2M interfaces are addressed in M2M-30035 *Artemis Payload Interface Definition Document (PIDD)*. Section 4 describes the verification process that is used to show that the payload meets the requirements.

This document shall take precedence for cross-program utilization payloads. The Program unique payload requirement documents take precedence for Program unique payloads (i.e., payloads that do not cross Program hatches or interface to different Program).

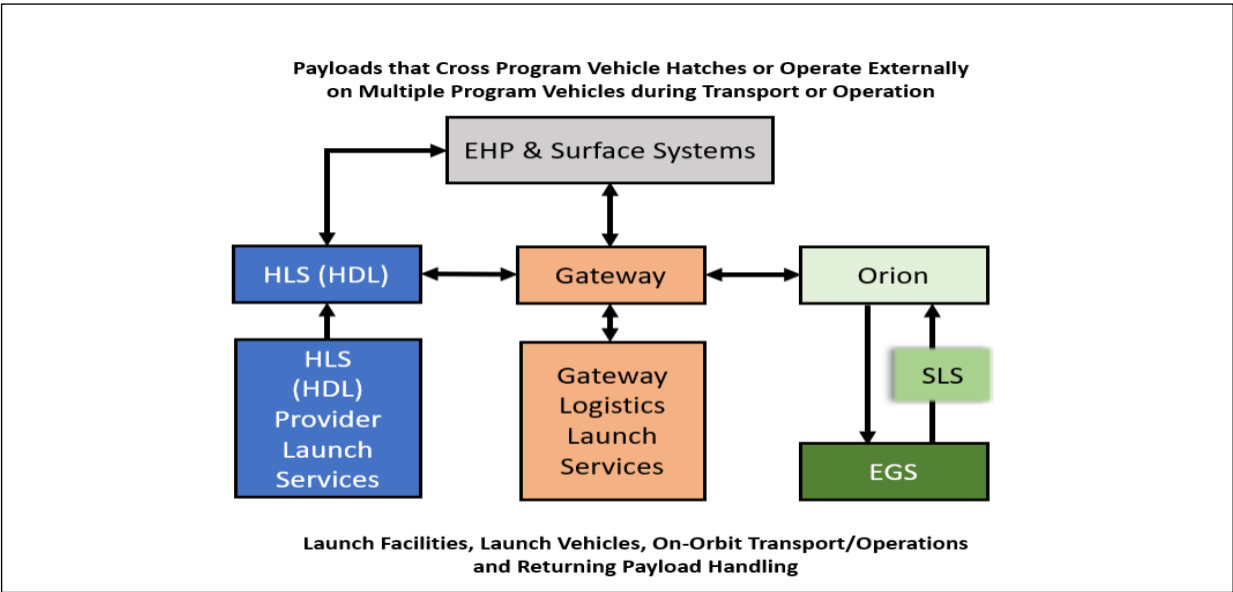


FIGURE 1.3-1 CROSS-PROGRAM UTILIZATION PAYLOADS

The payload developer is responsible for developing and maintaining their payload requirement document, a Requirements Verification Traceability Matrix (RVTM), and verification data. The RVTM includes, at a minimum, the requirement number and text, Safety Criticality designation (Y/N), verification method, success criteria, test objectives, pointer to where the requirement will be verified, pointer to test results, and any other applicable verification information.

NOTE: SLS Secondary Payload requirements that have a cross-program aspect (e.g., trajectories have the potential to intersect with M2M elements) have not been incorporated at this time and are considered forward work. < [FWD-30043-001](#)>

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 13 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

The cross-program safety review process for utilization payloads that will cross program vehicle hatches or operate externally on multiple program vehicles during transport or operation is addressed in M2M 30047, *Moon-To-Mars Cross Program Utilization Payload Safety Process*.

1.4 REQUIREMENT CONVENTION AND NOTATION

All Requirements Keys in this document are assigned using a “five part” nomenclature.

- a. All requirements start with “M2M” for Moon to Mars and “SMA” for Safety and Mission Assurance.

Example: **M2M-SMA-XXX-XXX-XXXX**

- b. The next item in Requirement Key is “UTIL” (for Utilization)

Examples: **M2M-SMA-UTIL-XXX-XXXX**

- c. The next prefix in the Requirement Key indicates the following:

“Shall” – Used to indicate a requirement that is binding, which must be implemented, and its implementation verified in the design. Represented by “-R-” in the requirement key.

Examples: **M2M-SMA-UTIL-R-XXXX**

“Should” – Used to indicate good practice or a goal which is desirable but not mandatory and does not require formal verification. Represented by “-SHOULD-” in the requirement key.

Example: **M2M-SMA-UTIL-SHOULD-XXXX**

“May” – Used to indicate permission. Represented by “-MAY-” in the requirement key.

Example: **M2M-SMA-UTIL-MAY-XXXX**

“Information” – Used to indicate information and is used to communicate that this information is from another source (document or requirement) that should be considered. Represented by “-INFO-” in the requirement key.

Example: **M2M-SMA-UTIL-INFO-XXXX**

Five digit numeric assignment.

Example: **M2M-SMA-UTIL-R-2001**

Single digit numeric assignment for sub-requirements.

Example: **M2M-SMA-UTIL-R-2003-1**

Requirement Rationale Statement

Rationale statements are intended to provide clarification, justification, purpose, and/or the source of a requirement. In the event that there is an inconsistency between a requirement and its rationale, the requirement always takes precedence.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 14 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

1.5 TERMINOLOGY

Each acronym is spelled out in its first use case and a complete list is provided in Appendix A. In addition, Appendix A contains a Glossary defining key terms. This section provides a brief introduction of key safety requirement terms used throughout the document.

1.5.1 Basic Requirement Terminology

Requirement Titles are intended to provide a categorical summary of the requirement scope. In the event that there is an inconsistency between a title and its requirement, the requirement always takes precedence.

- a) Certification: Certification is the process that demonstrates that the payload meets all design and/or performance requirements and applicable standards with the prescribed levels of safety and performance margin.
- b) Do No Harm: is the safety philosophy reflecting that cross-program utilization payloads must demonstrate they fail in a fashion that does no injury to ground or flight crews nor damage to the spacecraft.
- c) Exemption: Exemptions are alternate means for meeting the failure tolerance requirement(s). Exemptions A and B are described in M2M-SMA-UTIL-R-2001. Use of exemptions is documented in the hazard analyses. Exemptions will be evaluated by the lead-program's safety community and elevated to the JICB for awareness/approval.
- d) Fail Safe: Fail safe is the ability to sustain a failure and retain the capability to safely terminate or control the operation.
- e) Safety Critical: Safety critical refers to a condition, event, operation, process, function, or feature with potential to create a critical or catastrophic hazard. A safety critical feature of a design is a feature whose failure or malfunction has the potential to create a critical or catastrophic hazard. This terminology is most often used with structures, circuits, fasteners, software, and mechanisms, but can also apply to propulsion and guidance navigation and control (GNC) systems. A payload with a safety critical feature does not classify the entire payload as safety critical. Safety critical may also be applicable to must-work and must-not-work designs when hazard potential is present. Safety critical features of a payload should be identified early (by Phase I or Phase II Safety Reviews) so that they can be appropriately addressed in the hazard reports and analyses at Safety Reviews.
- f) Verification: The process of proving compliance with requirements—that the product can meet each “shall” statement as proven through performance of various verification methods.

1.6 MEASUREMENT UNITS

Numerical data listed in this document follows the International System of Units (SI) (metric) units with applicable tolerances. When appropriate, the equivalent value in English Units has been added in parenthesis. Conversions between English and SI units are in accordance with NIST SP 811 Guide for the Use of International Systems of Units.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 15 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

1.7 CHANGE AUTHORITY/RESPONSIBILITY

The appropriate NASA Office of Primary Responsibility (OPR) identified for this document is M2M Safety and Mission Assurance (SMA) Office.

Proposed changes to this document shall be submitted via a CR to the M2M Control Board (M2MCB) for consideration and disposition. All such requests will adhere to the M2M Configuration Management Change Process defined in M2M-30005, *M2M Configuration and Data Management Plan (CDMP)*.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 16 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

2.0 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents include specifications, models, standards, guidelines, handbooks, and other special publications. The documents listed in this paragraph are applicable to the extent specified herein. Unless specified the current revisions should be used. Links to the publicly available documents are provided.

In addition, M2M Program payload specific documents are listed below. These documents are available upon request.

TABLE 2.1-1 APPLICABLE DOCUMENTS

Document Number	Document Title
45 SWI 40-201	Radiation Protection Program
EHP-10028	Extravehicular Activity and Human Surface Mobility Program (EHP) Exploration EVA (xEVA) System Compatibility Standards
AFI 91-110	Nuclear Safety Review and Launch Approval for Space or Missile Use of Radioactive Material and Nuclear Systems
AFI 40-201	Managing Radioactive Materials in the USAF
EHP-10046	EHP Safety Technical Requirements
M2M 30005	Moon to Mars (M2M) Configuration and Data Management Plan (CDMP)
M2M 30010	Moon to Mars (M2M) Safety and Mission Assurance Plan <TBD-30043-001>
M2M 30026	Artemis Spectrum Management Plan
M2M 30035	Artemis Payload Interface Definition Document (IDD)
M2M 30038	M2M Utilization Interface Requirements Document
M2M 30040	M2M Graphical User Interface (GUI) Standard
M2M 30047	M2M Cross Program Utilization Payload Safety Process
AIAA-S-113, Rev A 2016	Criteria for Explosive Systems and Devices on Space and Launch Vehicle
ANSI/AIAA-S-080A-218	Space Systems – Metallic Pressure Vessels, Pressurized Structures and Pressure Components
ANSI/AIAA S-081B-2018	Space Systems – Composite Overwrapped Pressure Vessels
ANSI Z-136.1	American National Standard for Safe Use of Lasers
CCSDS 133.0-B-2	Blue Book July 2020, Space Packet Protocol
GP 11035	Gateway Requirements for Thin Walled Flexible Pressure Boundary (TWFPB) Hardware Items
GP 10037, Rev C	Gateway Payload Interface Definition Document
GP 10040	Gateway Loads Data Book
GSDO-RQMT-1080	Cross-Program Contamination Control Requirements
HLS-RQMT-001, Rev D	Human Landing System (HLS) Program System Requirements Document (PSRD)

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 17 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Document Number	Document Title
JSC 20793	Crewed Space Vehicle Battery Safety Requirements with EP-1901, Interpretation Memo for the Battery TR Propagation Requirements in JSC 20793
JSC 27472	Requirements for Submission of Data Needed for Toxicological Assessment of Chemicals to be Flown on Manned Spacecraft
JSC 62809	Human Rated Spacecraft Pyrotechnic Specification
JSC 64825, Rev A	Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials
JSC 67035	Best Practices and Guidelines (BP&G) for Thin Wall Pressure Boundaries (TWPB) for Human Spaceflight Applications
KNPR 1860.1	Kennedy Space Center Ionizing Radiation Protection Program
KNPR 1860.2	Kennedy Space Center Nonionizing Radiation Protection Program
KNPR 8715.3-1, Rev C	KSC Safety Procedural Requirements Volume 1, Safety Procedural Requirements for Civil Servants/NASA Contractors
KSC-STD-E-0022	Bonding, Grounding, Shielding, Electromagnetic Interference, Lighting and Transient Protection, Design Requirements for Ground Systems
MPCV 72615, Rev A	Orion Multi-Purpose Crew Vehicle (MPCV) Program Artemis I Secondary Payload Integrated Requirements and Interface Control Document (IRICD)
NIST SP 811	Guide for the Use of International Systems of Units
NPR 7150.2, Rev D	NASA Software Engineering Requirements
NPR 8715.6, Rev B	NASA Procedural Requirements for Limiting Orbital Debris and Evaluating the Meteoroid and Orbital Debris Environments
NPR 8715.24	Planetary Protection Provisions for Robotic Extraterrestrial Missions
NASA-HNBK-5010	Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware
NASA-STD-3001 Vol 1	NASA Spaceflight Human System Standard: Volume 1: Crew Health
NASA-STD-3001 Vol 2	NASA Spaceflight Human System Standard: Volume 2: Human Factors, Habitability, and Environmental Health
NASA-STD-4003, rev A	Electrical Bonding for NASA Launch Vehicles, Spacecraft, and Flight Equipment.
NASA-STD-5001	Structural Design and Test Factors of Safety for Spaceflight Hardware.
NASA-STD-5017, Rev B	Design and Development Requirements for Mechanisms
NASA-STD-5018	Strength, Design and Verification Criteria for Glass, Ceramics, and Windows in Human Space Flight Applications
NASA-STD-5019, Rev A	Fracture Control Requirements for Spaceflight Hardware
NASA-STD-5020, Rev B	Requirements for Threaded Fastening in Systems in Spaceflight Hardware
NASA-STD-6016, Rev C	Standard Materials and Processes Requirements for Spacecraft
NASA-STD-8719.12	Safety Standard for Explosives, Propellants and Pyrotechnics
NASA-STD-8719.14, Rev C	Process for Limiting Orbital Debris

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 18 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Document Number	Document Title
NASA-STD-8719.27	Implementing Planetary Protection Requirements for Space Flight
NASA-STD-8739.8, Rev A	NASA Software Assurance and Software Safety Standard
NAVSEA S9310-AQ-SAF-010 ⁽²⁾	Technical Manual for Navy Lithium, Battery Safety Program Responsibilities and Procedures
SLS-RQMT-287	Cross-Program Post-Exploration Mission – 1 (EM-1) Payload Safety Requirements
SLS-SPEC-159	Cross-Program Design Specification for Natural Environments (DSNE)
TOX-VR-2023-01 Rev G	Evaluation of Particles/Dusts in Habitable Spacecraft

NOTES:

- (1) In the case of certain cross program utilization payloads that are not transported, stowed, or operated in a vehicle, some of the above documents may not be applicable and is rationale for a tailored set of requirements based on the specific applicable program requirements
- (2) Although not requirements under authority of MPCV Safety and Engineering Review Panel (MERP), the battery safety requirements are applicable to all batteries that will be on Orion when recovered by naval vessel.

2.2 REFERENCE DOCUMENTS

The following documents contain supplemental information to guide the user in the application of this document.

TABLE 2.2-1 REFERENCE DOCUMENTS

Document Number	Document Title
ACD 50044	Lunar Surface Data Book
ACD-CHTR-022	Artemis Payload Integration Working Group Charter
ASTM E8	Standard Test Methods of Tension Testing of Metallic Materials
ASTM E595-15	Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment.
M2M-30040	Moon to Mars (M2M) Graphical User Interface (GUI) Standard
GP 10098	Gateway Extension for Space Packet Protocol
GSDO-RQMT-1243, Rev A	Exploration Ground Systems Program Generic Launch Site Support and Requirements Document
HEOMD-003	Crewed Deep Space Systems Human Rating Certification Requirements and Standards for NASA Missions
HF-STD-001	Human Factor Design Standard
HLS-IRD-007	Human Landing System Mandatory Government Furnished Property IRD – Initial
HLS-IRD-007-01	HLS Program Integrated Lander to Mandatory GFP IRD Sustained Phase
HLS-PLAN-003	Human Landing System (HLS) Program Safety and Mission Assurance (SMA) Plan
HLS-PLAN-013	HLS Planetary Protection Plan
HLS-UG-001	Human Landing System Lunar Thermal Analysis Guidebook

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 19 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Document Number	Document Title
ISO 7731:2003	Ergonomics - Danger signals for public and work areas - Auditory danger signals
JSC 29353	Flammability Configuration Analysis for Spacecraft Applications
KNPR 1820.3	Hearing Loss Prevention
KNPR 1820.4	Respiratory Protection
KNPR 8715.5	Personal Protective Equipment
MPCV 70024, Rev D	Orion Multi-Purpose Crew Vehicle (MPCV) Program: Human-Systems Integration Requirements (HSIR)
NASA-STD-1008	Classifications and Requirements for Testing Systems and Hardware to be Exposed to Dust in Planetary Environments
NASA-STD-6001, Rev B	Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures
NPR 8705.2, Rev C	Human-Rating Requirements for Space Systems
NASA/SP-2010-3407	Human Integration Design Handbook (HIDH).
SP-2016-6015	NASA Systems Engineering Handbook

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 20 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.0 SAFETY REQUIREMENTS FOR CROSS-PROGRAM UTILIZATION PAYLOADS

The safety requirements for Cross-Program Utilization Payloads were developed to ensure crew safety and flight mission success, where crew includes both flight crew and ground crew members. Flight mission success includes the M2M Elements (e.g., spacecraft, launch vehicles, and lunar assets such as rovers and habitats). Payload developers also need to address launch provider ground processing, spacecraft and launch vehicle payload requirements to ensure they meet the full complement of requirements. The safety requirements listed below are aligned with M2M 30035 from the payload's perspective.

The listed requirements were written to protect the NASA ground and flight crews, spacecraft, and assets.

M2M 30047, *M2M Cross Program Utilization Payload Safety Process* establishes the safety process to review and approve the safety analysis for utilization payloads that will be developed for those crossing a program vehicle hatch or operate externally on multiple program vehicles during transport or operation, affecting more than one M2M lunar exploration vehicle. Review of utilization payloads hazard analyses is by the lead program's safety review process which includes a phased safety review process that assures that cross program payload safety requirements and integrated hazards are incorporated into the ongoing design activities and covers all Artemis mission phases.

Payload hazard report risk scoring is based on M2M hazard severity/likelihood definitions found in M2M 30010, *M2M Safety and Mission Assurance Plan*. The payload project team will work with the assigned lead program to determine the scope of the hazard reports.

NOTE: Minor, Moderate, and Severe hazards are typically not document in hazard reports.

A payload categorization assessment will to be completed (e.g., M2M 30047, Appendix C *Payload Category Assessment Form*) to determine the safety category, (Category 1 or Category 2). The assessment of the applicable requirements necessitates an understanding of the payload category. The category determination is approved in support of the System Requirements Review (SRR) at the Phase 0 safety panel review. Payloads that pose no hazard critical or catastrophic to spacecraft or personnel are termed Category 1.

3.1 CORE SMA REQUIREMENTS

The following requirements are applicable to utilization payloads crossing Program hatches or interfacing between different M2M Program vehicles. Core requirements are based on the unique hazards associated with a payload; therefore, specific verification for these requirements vary based on the specific hazard that is identified. Payload hazards, related controls to prevent the hazards, and verification methods will be outlined in the hazard report (HR) and approved by the safety review panel.

Hazard reduction (controls) precedence sequence should be conducted in the following order of precedence: eliminate hazards through design selection, reduce risk through design alteration, and operational controls. Most hazards will require the combination of several of these approaches to adequately control a potential hazard.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 21 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.2 FAILURE TOLERANCE

A safety criticality assessment will be completed in support of the System Requirements Review (SRR) and Phase 0 safety panel review to determine the worst case impact if a cross-program utilization payload fails.

M2M-SMA-UTIL-R-2001 Failure Tolerance to Catastrophic Hazards

The Payload shall be designed such that no combination of two failures, or two operator errors, or one of each can result in a loss of life or permanent disability or loss of M2M element or a major ground facility.

Payload developers should check with the assigned Lead Program for additional clarification on Exemptions A and B (below). The listed text is based on HEOMD-003, *Crewed Deep Space Systems Human Rating Certification Requirements and Standards for NASA Missions* requirement 5.2.2.

Exemption A: Failure of primary structure, structural failure of pressure vessel walls, and structural failure of pressurized lines are exempted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. Each M2M Program has tailored the failure tolerance Exemption requirement and the Payload Developer will follow the Lead integration safety panel's Exemption guidelines that is selected in accordance with M2M 30047, M2M Cross Program Utilization Payload Safety Process.

Exemption B: Other potentially catastrophic hazards that cannot be controlled using failure tolerance are exempted from the failure tolerance requirements with approval from the safety review panel and mandatory concurrence from the Technical Authorities and the Director, JSC (for crew risk acceptance) provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. For selected cases where a reliability-informed approach is used, as agreed by the respective programs Technical Authorities and the Director, JSC, the reliability requirements shall be verified with appropriate confidence intervals using robust reliability approach that is substantially anchored in actual test data verifying margins to environments (natural and induced), life requirements, operational boundaries, and failure modes.

Rationale: Three verifiable controls must be provided to prevent the occurrence of the identified catastrophic hazard for the payload to be considered two failure tolerant.

Compliance with this requirement can be accomplished solely at the payload level, or through a combination of hazard controls between the payload and the payload accommodation [Vehicle Payload System]. The payload accommodation may contribute only one control, if available, to the payload failure tolerance control strategy. Any such shared failure tolerance will be agreed to within the safety review process. Specific hazard controls and implementation must be derived from a design and safety analysis performed by the Payload Developer in accordance M2M 30047, M2M Cross Program Utilization Payload Safety Process. Acceptance of these approaches by the Technical Authorities avoids processing waivers for numerous hazard causes, where failure tolerance is not the appropriate approach. A two failure tolerant system requires three controls.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 22 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Note 1: Analysis of redundant systems, subsystems, or components will consider common-cause failures (e.g., contamination, common power source, etc.), to ensure that the risk of defeating redundancy is sufficiently low.

Note 2: When a safety critical system fails because of improper or unexpected performance due to unanticipated conditions, similar redundancy can be ineffective at preventing the complete loss of the system. Dissimilar redundancy is very effective provided there is sufficient separation among the redundant legs. (For example, dissimilar redundancy where the power for all redundant capability was routed through a common conduit would not survive a failure where the conduit was severed). It is also highly desirable that the spaceflight system performance degrades in a predictable fashion to allow sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures.

Note 3: There are examples of dissimilar redundancy in current systems. For Earth reentry, the Soyuz spacecraft has a dissimilar backup ballistic entry mode to protect for loss of the primary attitude control system and a backup parachute for landing. Other examples include backup batteries for critical systems that protect for loss of the primary electrical system and the use of pressure suits during reentry to protect for loss of cabin pressure.

Note 4: Ultimately, the program and safety review panel evaluate and agree on the failure scenarios/modes and determine the appropriate level of failure tolerance and the practicality of using dissimilar redundancy or backup systems to protect for common cause failures.

Note 5: Where failure tolerance is not the appropriate approach to control hazards, specific measures need to be employed to:

- (1) Recognize the importance of the hazards being controlled.*
- (2) Ensure robustness of the design; and*
- (3) Ensure adequate attention/focus is being applied to the design, manufacture, test, analysis, and inspection of the items.*

M2M-SMA-UTIL-R-2002 Failure Tolerance to Critical Hazards

The Payload shall be designed such that no single failure or single operator error leads to a non-permanently disabling personnel injury, illness, damage to an M2M element, loss of redundancy for in-flight life sustaining function (i.e., with only a single hazard control remaining), and/or loss of use of systems needed for essential mission operations.

Exemptions A and B also apply to Critical Hazards (see above).

Rationale: Two verifiable controls must be provided to prevent the occurrence of the identified critical hazard for the payload to be considered single failure tolerant.

Compliance with this requirement can be accomplished solely at the payload level, or through a combination of hazard controls between the payload and the payload accommodation [Payload System]. The payload accommodation may contribute only one control, if available, to the payload failure tolerance control strategy. Any such shared failure tolerance will be agreed to within the safety review process.

NOTE: *Catastrophic and Critical hazards are fully defined in the M2M SMA Plan (M2M 30010).
<TBD-30043-001>*

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 23 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2003 Redundant Paths

The payload shall protect redundant payload systems (such as assemblies, panels, power supplies, tanks, controls, and associated interconnecting wiring and fluid lines), where payloads implement redundancy to satisfy the failure tolerance requirement, to ensure that an unexpected payload event which damages one payload system will not propagate and damage other payload systems.

Rationale: Propagation of failure has the potential to lead to a catastrophic event.

M2M-SMA-UTIL-R-2003-1 Redundant Paths – Separate Connectors

The payload shall be routed through separate connectors for redundant functions that are required to prevent a catastrophic or critical hazards.

M2M-SMA-UTIL-R-2003-2 Redundant Paths – Separation Distance

Safety-critical redundant subsystems shall be separated or otherwise protected, to ensure that a credible unexpected event that damages one will not prevent the others from performing the safety-critical function.

Rationale: Ultimately, the level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Since redundancy does not, by itself, make a system safe, it is the responsibility of the payload developer, engineering, and safety teams to determine the design that optimizes safety given the mission requirements and constraints. In such a design, both the risk from individual contributors (e.g., hazards or failure modes) and the total risk for the reference mission are below acceptable levels.

M2M-SMA-UTIL-R-2004 Capability without Emergency Equipment and Systems

The payload shall provide the appropriate failure tolerance capability without the use of emergency equipment and systems (i.e., crew survival methods used after hazard has been realized).

Rationale: Emergency equipment is used after the hazard has occurred and does not prevent the failure; thus, it is not a means of hazard control.

M2M-SMA-UTIL-R-2005 Safe Without Services

Payloads shall maintain failure tolerance and not generate any new hazards in the event of sudden loss or temporary interruption of provided services.

Rationale: In the event of a sudden loss or temporary interruption of provided ground or spacecraft services, the payload needs to remain safe state (maintain failure tolerance). Ground and spacecraft services are those provided to the payload interfaces. The payload must remain in a safe state until returned to operation by the ground or flight crew.

M2M-SMA-UTIL-R-2006 Failure Propagation

Payloads design shall preclude propagation of failures from the payload to integrated vehicle or adjacent payloads.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 24 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: The analysis of a component whose failure may propagate across an interface will not end at the interface with other systems/subsystems, but will be analyzed across the interface to determine effects on the interfacing element and ultimately on the spacecraft. To address impacts to the integrated system, spacecraft, launch vehicle, etc., the analysis must be conducted to identify failure effects that could propagate to interfacing flight subsystems or elements. It should also show where isolation can aid in halting the propagation of failure or where removal of hardware contributors can reduce or limit the consequences. For radiation effects potentially propagating to interfaces, including recoverable and non-recoverable single-event effects and total dose effects, analysis must be performed with worst case assumptions demonstrating either that these effects are fully confined on the payload side of the interface, or provide full characterization of their manifestation at the M2M spacecraft side of the interface. Depending on the particular failure mode, this analysis may include radiation analyses performed in compliance with or enveloping accepted Radiation Hardness Assurance (RHA) practices, or Fault Detection, Isolation, and Recovery (FDIR) analysis of anticipated failure modes.

M2M-SMA-UTIL-R-2007 Payload Controls for Human Error

Payload shall implement controls to human error according to the following precedence:

- a. Prevent human error in the maintenance, operation, and control of the system.
- b. Reduce the likelihood of human error and provide the capability for the human to detect and correct or recover from the error.
- c. Design the system to limit the negative effects of errors.

Rationale: Human error is either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence. Controlling Human Error requires identification of human errors through Human Error Analysis (HEA). The HEA is a systematic approach to evaluate human actions, identify potential human error, model human performance, and qualitatively characterize how human error affects a system. HEA provides an evaluation of human actions and error in an effort to generate system improvements that reduce the frequency of error and minimize the negative effects on the payload. The human error analysis considers mission operations while the crew is interacting with the payload – including crew operations, ground control operations (typically covered via hazard reports), and ground processing operations with flight crew interfaces. The analysis also covers response to system failures and abort scenarios. The intent of the human error analysis is to:

- 1) Identify inadvertent operator actions which would cause a catastrophic event and determine the appropriate level of tolerance;*
- 2) Identify other types of human error that would result in a catastrophic event (e.g., operational errors, errors of omission, timing errors); and*
- 3) Apply the appropriate error management as described in this requirement.*

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 25 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.3 ENVIRONMENTAL COMPATIBILITY

M2M-SMA-UTIL-R-2008 Safe in All Natural Environments

The payload shall meet all safety requirements during and after exposure to the applicable natural environments as defined in SLS-SPEC-159 *Cross-Program Design Specification for Natural Environments (DSNE)*.

Rationale: Payload must maintain a Do No Harm posture in all of the natural space environments including ionizing radiation, meteoroids, orbital debris, plasma/spacecraft charging, natural thermal, gravitational, etc., environments. HLS-UG-001, Human Landing System Lunar Thermal Analysis Guidebook may be consulted for guidance on performing thermal analyses using DSNE thermal environments.

3.3.1 PLASMA

Plasma is a quasi-neutral gas of particles (charged and neutral) that exhibits collective behavior distinct from normal gasses allowing the flow of electricity. A space vehicle's interactions with plasma are based on plasma thermal properties and orbital altitudes. Relatively cold, dense plasma of the ionosphere interacts differently than those of tenuous plasma at very high orbits. There are also different plasma interactions in the aurora regions where the currents originating from higher altitudes penetrates to low Earth orbit. Plasma can also be created by the release of ionized gas from payloads.

No unique plasma safety requirements are imposed on Intravehicular Activity (IVA) utilization payloads.

M2M-SMA-UTIL-R-2009 Plasma Environments

Payload safety critical circuits shall be unaffected during and after plasma environments.

Rationale: Safety critical circuits are circuits whose loss of function, malfunction, performance degradation, or inhibit loss can result in critical or catastrophic hazard.

M2M-SMA-UTIL-R-2010 Ionizing Radiation

Payload safety critical circuits shall be unaffected during and after exposure to ionizing radiation environments.

Rationale: Safety critical circuits are circuits whose loss of function, malfunction, performance degradation, or inhibit loss can result in critical or catastrophic hazard. Ionizing radiation can result in hazard control reduction when critical functions are affected by Single Event Effects (SEE) and Total Ionizing Dose (TID).

The ionizing radiation environment consists primarily of high kinetic energy charged particles many of which can induce SEE and TID in electronics. SEE and TID can change electrical state or characteristics of an electronic device thereby creating a hazard. SEE normally occurs randomly but will occur at an increased rate during intense solar flares (Solar Particle Events) that follow release of high energy protons and heavy ions from the Sun. TID effects can slowly degrade payload performance over time as determined by dose rate and payload TID sensitivity. The rate of SEE effects normally occur randomly on the timeline at a rate that depends on the environment severity, solar activity, and payload SEE sensitivity.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 26 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2011 Inadvertent Activation Protection

Payload shall be protected against inadvertent operation that result in a hazard.

Rationale: Payloads must not be susceptible to inadvertent activation when subject to the conducted or radiated emission. Payloads should work with their M2M Payload Integration Manager (PIM) to determine the specific levels.

M2M-SMA-UTIL-R-2012 Induced Environments

The payload shall comply with the applicable safety requirements herein when exposed to the worst-case induced environments.

Rationale: Environments identified by the launch vehicle and spacecraft will be applicable as defined in the mission planning timeline. The payload must retain all safety design features in the appropriate mission-specific and location environment.

3.4 STRUCTURES AND FASTENERS

Structural safety requirements are levied to prevent structural failure of hardware, which could lead to hazards to the crew, M2M Elements, or other payloads.

Payloads designated as “safety critical”, have the potential to create a critical or catastrophic hazard upon failure. The safety panel, with input from the programs’ Structures and Mechanisms groups, help determine if a payload has a safety critical structure. Payloads that meet any of the following conditions are often classified as safety critical (please note this is not a comprehensive list):

- Mounted to unpressurized portion of an M2M Element.
- Launched in the unpressurized section of the vehicle.
- Hard-mounted in the pressurized section of the vehicle.
- Contains a pressurized system
- Contains a hazardous material
- Contains a shatterable material
- Fasteners may be classified as safety critical at the discretion of the safety review panel if payload is hard-mounted in the pressurized section, or include rotating machinery, mechanical stops, or containment devices. As a minimum, fasteners used in the following manner are often classified as safety critical:
 - Used on components that are required to function to prevent a hazard.
 - Used on pressure systems.
 - Used on components used to contain hazardous materials.
 - Used on safety critical mechanisms.
 - Used on safety critical preloaded joints that are required to maintain their preload.
 - Used to restrain external components.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 27 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

- Used to restrain a rotating device that has a kinetic energy greater than 19,310 Joules (J) (14,240 foot-pounds (ft-lbs)) and is not contained.
- Fail safe fasteners (i.e., redundant fasteners permit failure of a certain number of fasteners without overall failure of the device or system) when used for pyrotechnic mechanical containment.). Note: Fail-safe fasteners used in other applications are not necessarily considered safety critical.

M2M-SMA-UTIL-R-2013 Payload Structural Design

Payloads shall meet or exceed NASA-STD-5001, *Structural Design and Test Factors of Safety for Spaceflight Hardware*.

Rationale: Mission safety. Key payload structural support should be adequately analyzed and tested to ensure it will not fail releasing payloads that could injure crew or damage hardware.

M2M-SMA-UTIL-R-2014 Safety Critical Structures

Payload safety critical structures shall be designed to meet the applicable requirements as defined in NASA-STD-5019, *Fracture Control Requirements for Spaceflight Hardware*.

Rationale: Mission safety. Key payload structural support should be adequately analyzed and tested to ensure payloads do not injure crew or damage hardware. NASA-HNBK-5010, Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware provides supplemental information to aid in the application of NASA-STD-5019.

M2M-SMA-UTIL-R-2015 Payload Glass or Ceramic Structures

Payloads shall meet or exceed NASA-STD-5018, *Strength, Design and Verification Criteria for Glass, Ceramics, and Windows in Human Space Flight Applications*, when glass or ceramics are used in the payloads' structural applications.

Rationale: Failure of glass and ceramic structures can lead to serious crew injury.

M2M-SMA-UTIL-R-2016 Payload Fasteners

Payloads shall be in accordance with NASA-STD-5020, *Requirements for Threaded Fastening in Systems in Spaceflight Hardware*, when payload primary structures use safety critical fasteners.

Rationale: In most utilization payload cases the primary structure is the structure that attaches the payload to the spacecraft with emphasis on fasteners sized to accommodate launch and landing loads.

3.5 MECHANISMS

M2M-SMA-UTIL-R-2017 Payload Mechanisms

Payloads shall be designed to meet or exceed NASA-STD-5017, *Design and Development Requirements for Mechanisms*, when payload mechanisms have the potential to result in either a critical or catastrophic hazard.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 28 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: NASA-STD-5017 addresses the functionality (the ability to operate or the ability to retain configuration) of mechanical systems rather than their strength as a structural element or the electrical aspects of an electromechanical system. This NASA Technical Standard is applicable to space flight mechanisms, including valves and ordnance-operated mechanical devices, though it may also serve as a useful guidance document for other systems such as ground support equipment (GSE).

3.6 PRESSURE SYSTEMS/VESSELS

Pressure systems can contain fluids/gases that are considered either hazardous or nonhazardous. Low pressure systems are classified as either low energy fail-safe or sealed containers. A high pressure system has internal pressure >100 pounds per square inch absolute (psia) or stored energy greater than 19,310 J (14,240 ft-lbs). Maximum Design Pressure (MDP) derivations are necessary to understand the capabilities of the pressure systems to preclude rupture hazards. Table 3.6-1 describes pressure systems classifications.

TABLE 3.6-1 PRESSURE SYSTEMS CLASSIFICATIONS

Classification	Sealed Container with no Analysis/ Testing	Sealed Container	Low Energy Fail Safe Pressure Systems	High Pressure Systems	
				Pressure Vessel	Lines, Fittings, Components
Classification Criteria	• ≤ 152 kPa (22 psia) • $\leq 19,310$ J (14,240 ft-lbs) • Toxicity Hazard Level (THL) 0	• > 152 and ≤ 700 kPa (22 and ≤ 100 psia) • $\leq 19,310$ J (14,240 ft-lbs) • THL 0	• ≤ 700 kPa (100 psia) • THL 0 • < 1355.8 J (1000 ft-lbs) • Code of Federal Regulations Title 49 Department of Transportation (DOT) Pressure Vessels for Space Applications, when evaluating DOT pressure vessels.	• > 700 kPa (100 psia) • $> 19,310$ J (14,240 ft-lbs) • Includes metallic, composite, pressure components • THL > 0 with appropriate levels of containment	• > 700 kPa (100 psia) • $> 19,310$ J (14,240 ft-lbs) • Includes metallic, composite, pressure components • THL > 0 with appropriate levels of containment

This section also applies to containers that contain materials that have the potential to increase in pressure due to chemical reaction or change of state (solid to gas).

Not all pressure systems are high energy pressure systems that fail catastrophically. Many pressure systems are small, low energy, fail-safe, pressure systems. Fail Safe is a condition where, after failure of a single individual pressurized component, the remaining components (considered unflawed) can withstand the redistributed pressure, and the failure will not release components or if contents are released, they will not cause an over-pressurization of the system, a hazardous environment, or damage other hardware. If the pressure system is determined to be low energy and fail-safe (per Table 3.6-1), then it can be declared as a low energy pressure

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 29 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

system with a system description in the safety data package (SDP) and a Rupture/Leakage of Pressure System HR is not necessary.

M2M-SMA-UTIL-R-2018 Payload Pressure System

Payload pressure systems and pressure vessels shall meet ANSI/AIAA S-081B-2018, *Space Systems – Composite Overwrapped Pressure Vessels* and ANSI/AIAA-S-080A-2018, *Space Systems – Metallic Pressure Vessels, Pressurized Structures and Pressure Components*.

Rationale: These ANSI standards applies in full.

M2M-SMA-UTIL-R-2019 Payload Thin Walled Flexible Pressure Boundary Hardware

Payload hardware containing Thin-Walled Flexible Pressure Boundary (TWFPB) devices (e.g., bellows, flex hoses, diaphragms, water bags, etc.) with a failure mode that could result in a hazard shall meet the requirements of JSC 67035, *Best Practices and Guidelines (BP&G) for Thin Wall Pressure Boundaries (TWPB) for Human Spaceflight Applications*.

Rationale: Mission safety. A thin-walled flexible pressure boundary (TWFPB) hardware item is classified as fracture critical if a single leakage or rupture/burst event involving the TWFPB could result in a catastrophic hazard (i.e., zero failure tolerant, OFT). Examples of fracture critical TWFPBs include:

- (1) bellows used in fluid components (e.g., valves, regulators, accumulators, etc.)*
- (2) bellows in expansion joints of various types used in fluid lines.*
- (3) diaphragms/membranes used in fluid components (e.g., pressure transducers valves, regulators, burst disks, etc.)*
- (4) flexhoses containing a metal bellows as the inner core element.*

3.6.1 SEALED OR VENTED CONTAINERS

M2M-SMA-UTIL-R-2020 Sealed Payload Containers for Ascent or EVA

Payload sealed containers shall be designed to withstand the maximum pressure differential created by ascent, EVA, or rapid decompression (104.8 kPa (15.2 psia) for items exposed directly to vacuum).

Sealed containers must be compliant with a) and b) (below) in all cases. Additionally, one of the c), d), or e) must be met, depending on the maximum design pressure (MDP) and verification method.

- a) Payload and System are a single, independent container containing a non-hazardous substance.
- b) Payload System contain less than 19,310 Joules (14, 240 foot-pounds) of stored energy due to pressure.
- c) Payload and System have a MDP of 151.7 kPa (1.5 atmospheres (22 psia, 1.5 bars)).
- d) Payload and Systems have an MDP greater than 151.7 kPa (1.5atm (22psia, 1.5bars)), but less than 689.5 kPa (6.81atm (100psia, 6.9bars)) and analysis or test showing minimum safety factor for the design is 2.5 x MDP.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 30 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

- e) Payload and Systems have an MDP greater than 151.7 kPa (1.5atm (22psia, 1.5bars)) but less than 689.5 kPa (6.81atm (100psia, 6.9bars)) and each flight unit pass a proof test of 1.5 x MDP.

Rationale: A sealed container consists of only one pressurized compartment or vessel and has Maximum Design Pressure (MDP) is > 151.7 kPa (22 psia) and ≤ 689.5 kPa (100 psia), Containing non-hazardous materials, and stored energy $\leq 19,310$ Joules (14,240 ft-lbs). When sealed container has an MDP ≤ 151.7 kPa (22 psia), no additional testing or analysis is required. When the MDP is greater than 689.5 kPa (100 psia), it is considered a high pressure component and high pressure system safety requirements are applicable. Science payloads that are comprised of more than one pressurized component are considered a pressure system.

M2M-SMA-UTIL-R-2021 Vented Payload Containers

Vented containers shall size vent flow areas such that structural integrity is maintained with a minimum FoS of 1.4 on metallic structures or 2.0 on composite/bonded structures.

Rationale: Mission safety. Key payload vented containers should be adequately analyzed and tested to ensure they vent properly and have adequate design margin to prevent injury to crew or damage hardware.

M2M-SMA-UTIL-R-2022 Unintentionally Sealed Payload Containers

Vented enclosures that are not intentionally sealed shall not create a hazard in the event of depressurization or repressurization of the surrounding volume as verified by:

- a) Contain less than 4,152 Joules (3,063 foot-pounds) of stored energy due to pressure in the event of vent(s) failure.

Note: Calculation of the stored energy potential can be found in NASA-HDBK-5010, *Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware*, Appendix G.

- b) Vents are sized to maintain a minimum FoS of 1.5 for pressure loads when assessed against the depressurization rates of up to -2068 millibar/min (-30.0 psi/min) and the repressurization rates of up to +931 millibar/min (+13.5 psi/min) (Reference: MPCV 70024 section 3.2.1.6).

Provides an internal volume to the effective vent area ratio that results in a differential pressure loading of no greater than 0.7 millibars differential (0.01psid).

Note: Maximum Effective Vent Ratio (MEVR) for a 0.7 millibar (0.01 psid) pressure differential is defined as:

$$\text{MEVR} = ((\text{Internal volume (cm}^3\text{)})/\text{Effective Vent Area (cm}^2\text{)}) \leq 5080\text{cm}$$

$$\text{MEVR} = ((\text{Internal volume (in}^3\text{)})/\text{Effective Vent Area (in}^2\text{)}) \leq 2000\text{in}$$

Rationale: The rate of change of pressure must be limited to prevent injury to the crew's ears and lungs during depressurization and re-pressurization. Each spacecraft has rate of change of pressure requirement, but they do not consider payload pressure vessel events or impacts.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 31 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.7 ELECTRICAL

Electrical safety requirements are levied to prevent hazards such as electric shock, molten metal, toxic material release, fire, touch temperature hazards, and electronic interference. These requirements include design and operational considerations for the selection of wiring and circuit protection, connector mate/demate, biomedical instrumentation < FWD-30043-002>, batteries, capacitors, Electromagnetic Interference (EMI), Electrostatic Discharge (ESD), corona, and Radio Frequency (RF) signals.

Circuits used in the control of critical and catastrophic hazards are safety critical circuits. It is important to note that a safety critical circuit has certain implications that may not apply in every requirement case.

Safety critical circuits are:

- Circuits whose loss of function could result in a critical or catastrophic hazard, or
- Circuits whose malfunction or degradation of performance could result in a critical or catastrophic hazard, or
- Circuits that control inhibits whose loss could result in critical or catastrophic hazards, or
- Circuits that are inhibited or not operational to prevent operation a critical or catastrophic hazard.

NOTE: Biomedical instrumentation for M2M application in oxygen rich environments are in development. < FWD-30043-002>

M2M-SMA-UTIL-R-2023 Payload Circuit Protection

Payload electrical circuits shall include circuit protection for their internal loads, such that the wire operating temperature limit for the wire insulation will not be exceeded for any possible load or fault condition of the circuit under worst-case environmental conditions.

Rationale: The circuit load protection prevents failures that would lead to fire.

M2M-SMA-UTIL-R-2024 Payload Safe State Indication

Payloads shall provide indication of safe state prior to mating and demating of powered connectors.

Rationale: To prevent inadvertent activation and sparks when mating and demating from a powered connector. (Derived from M2M-30038, M2M-UTIL-R-2015 Local Status of Payload Location 120 Vdc Power a requirement on the M2M Elements).

NOTE: The M2M Element side of the power interface should also be safed. The payload is responsible for calling this out in their operating procedures, (and as a hazard control in their hazard report(s)).

M2M-SMA-UTIL-R-2025 Separation of Redundant Safety Critical Circuits

The Payload electrical power system (EPS) shall physically separate redundant safety critical circuits.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 32 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: As a result of increased emphasis on the routing of redundant safety critical circuits, it is necessary to ensure separation of redundant paths to eliminate common cause failures, (e.g., arching across redundant paths leads to both paths failing).

This ensures that an unexpected event damaging one circuit is not likely to prevent the other circuits from performing the function. All redundant functions required to prevent a catastrophic hazard must not be routed through a single connector. Payload hazard reports must identify damage to electrical circuits as a possible cause of the failure of redundant safety critical circuits. When safety critical circuits cannot be separated from a common wire bundle or connector, additional design feature (e.g., physical barrier that prevents failures in one safety critical circuit from propagating to adjacent safety critical circuits) can be considered on a case-by-case basis.

M2M-SMA-UTIL-R-2026 Protection of Critical Payload Controls

The Payload EPS shall protect against a single inadvertent actuation of safety critical controls using a two-step process of two independent actions (crew or ground).

Rationale: To prevent crew injury due to inadvertent actuation of payloads that have the potential to cause crew injury.

M2M-SMA-UTIL-R-2027 Electrical Connector Scoop Proof Design

The Payload electrical connectors (both IVA and EVA connectors) shall prevent electrical pins from inadvertently contacting the opposing connector half during mating and de-mating of the connector.

Rationale: The use of mechanical design features is necessary to fully enclose or shroud the power connector pins and sockets during mate/demate activities. This minimizes the potential for molten metal caused by FOD or bent pins. Scoop Proof designs provide a longer shell design on the pin half of a connector.

This is the primary design feature that protects against production of molten metal. The longer shell allows the pin contacts to be recessed sufficiently so as not to be damaged if the mating shell is "scooped" into it, thus preventing pins from being bent or contacts from being electrically shorted during mating. The design of AC plugs does not meet this standard because it is not shrouded when partially de-mated. A bent pin analysis is recommended to ensure bent pins will not bypass safety critical circuits, remove more than one inhibit to a hazard, or cause molten metal hazards.

This requirement also applies to EVA connectors. Equivalent to EHP-10028, Exploration EVA (xEVA) System Compatibility Standards requirement [EVASC.0066].

M2M-SMA-UTIL-R-2028 Bonding and Isolation

Electrically powered payloads (both IVA and EVA payloads) shall provide a Class H bond path that complies the bonding requirements in NASA-STD-4003, *Electrical Bonding for NASA Launch Vehicles, Spacecraft, and Flight Equipment*.

Rationale: Electrical shock is considered a catastrophic hazard. Payloads are required to protect the crew from shock hazards when electrical current through the crewmember is > (greater than) 40mA for DC and > (greater than) 8 mA peak for AC. In addition, this bond is often necessary from proper electrical power system function even if a hazard isn't present.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 33 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

This requirement also applies to EVA equipment that requires bonds. Equivalent to EHP-10028, requirement [EVASC.0065].

M2M-SMA-UTIL-R-2029 Electrolytic Capacitors

Payloads that contain liquid electrolyte or unknown capacitors shall be designed to minimize the release of electrolyte at ambient conditions.

Rationale: This is achievable by complying with Table 3.7-1, Capacitor Risk Classification and Verifications. Information in the form of a manufacturer's datasheet, analysis, measurement, etc. must be provided to determine the case size of each capacitor. <FWD-30043-003>

M2M-SMA-UTIL-R-2030 IVA/EVA/EVR Connector Mate/Demate Inhibit and Design

When exceeding catastrophic current limits for crew electrical shock defined in Table 3.18.5-1-3, Crew Safety Electrical Current Limits OR when exceeding 3 Amps at the connector interface, crew or robotic mating/demating of power connectors shall employ at least one upstream verifiable inhibit with bonding and isolation per M2M-SMA-UTIL-R-2028 and be designed with the following connector design features:

- a. Electrical Connector Long Shell Design: Electrical connectors that prevent electrical pins from inadvertently contacting the opposing connector half during mating and demating of the connector.
- b. Electrical Connector Contact Type: Connector attached to the powered (hot end) side of wires, cables, wire bundles and wire harnesses for one-way power interfaces that has socket contacts.
- c. Protection of Open IVA/EVA Connectors – Electrical Power Conductors and Terminations: Protection is needed to prevent crew contact with exposed power conductors and terminations.
- d. Bond path to ground for conductive surfaces are maintained while mating/demating the powered pin/sockets on recessed connectors (e.g., connectors attached to equipment remote from the crew such as back-of-the-rack connections).

Rationale: Power connectors (including blind mate connectors) can present shock or molten metal hazards to the crew and/or equipment during power connector mate/demate. A verifiable upstream inhibit provides one level of control to prevent shock and/or molten metal hazards to the crew and equipment. The design must provide for verification of the upstream inhibit at the time that it is inserted. Adequate bonding and chassis isolation as well as utilizing the following connector design features, provide the equivalent of a second level of control for IVA unless exceeding the threshold in requirement M2M-SMA-UTIL-R-2031. EVA connectors require a second inhibit as described in M2M-SMA-UTIL-R-2032.

- a. Connectors with a long shell on the receptacle (i.e., scoop proof) that adequately encloses the pins and sockets prevents damage to the exposed contact pins during mating.
- b. Connectors with socket contacts on the powered (hot end) side of wires to prevent foreign objects from shorting contacts in the connector. This design feature does not apply for harnesses connected to equipment in which bi-directional power is present.
- c. For IVA/EVA connections, connector caps can be utilized to provide protection against connector damage and prevent shock hazards due to crew direct or inadvertent contact

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 34 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

to exposed power conductors and terminations. Open EVA connectors with established keep-out-zones would also meet the intent of this requirement.

- d. *M2M-SMA-UTIL-R-2028 provides the appropriate bonding and isolation requirements per NASA-STD-4003.*

M2M-SMA-UTIL-R-2031 IVA 2nd Verifiable Upstream Inhibit for Mating/Demating Electrical Power Connectors

Prior to and during mate/demate of an intravehicular electrical power connector, each powered circuit shall have a second verifiable upstream inhibit when the Open Circuit Voltage is greater than 200 Vdc/RMS or when the short-circuit power/current is greater than 67 amps.

Rationale: Power connectors can present electrical shock or molten metal hazards to the crew and/or equipment during power connector mate/demate. A second verifiable inhibit is required for IVA operations when the Open Circuit Voltage is greater than 200 Vdc/RMS or when the short-circuit power/current is greater than 67 amps because the controls listed in requirement L2-GW-0403 no longer provide sufficient electrical arcing and molten metal risk protection at those thresholds. ISS experience used 8.2Kw limit (65 amperes at 126 volts) based on the capabilities of the ISS Direct Current-to-Direct Current Converter Unit. Connector testing has shown that 67 amperes at 33 volts is the threshold for significant damage to sockets, per MA2-99-170 Crew Mating/Demating of Powered Connectors. The design must provide for verification of at least one of the upstream inhibits at the time that it is inserted.

The use of Ground Fault Circuit Interrupts (GFCIs) is not allowed as a substitute for an upstream inhibit because GFCI current limits do not protect for concerns associated with molten metal hazards. However, the use of GFCI's is prudent and encouraged because it provides additional shock hazard protection.

M2M-SMA-UTIL-R-2032 Extravehicular 2nd Inhibit for Mating/Demating Electrical Power Connectors (Voltage >= 200 Vdc/RMS or Current >= 67 Amps)

The Payload shall have a second upstream inhibit that is verifiable prior to and during mate/demate of an extravehicular (EVA/EVR) electrical power connector when the open circuit voltage is greater than or equal to 200 Vdc/rms or when the short-circuit power/current is greater than or equal to 67 Amps.

Rationale: First inhibit requirement details are found in M2M-SMA-UTIL-R-2030. The second inhibit is required for extravehicular activities because arcing and molten metal can cause a hole in the xEVA suit, potentially ignite the suit materials due to the high oxygen environments in the xEVA Suit, or damage safety critical ExtraVehicular Robotics (EVR) systems. This voltage threshold is not based on M2M Program electrical system design but is based on historical ISS testing and is meant to provide the upper limit to inform future design. See MA2-99-170 and SSP 51721, Crew Mating/Demating of Powered Connectors. The second upstream inhibit needs to be a "verifiable" inhibit since this is a catastrophic hazard. This is covered by requirements in Section 3.11, Monitoring requirements. The monitoring is covered by the Computer Based Control Systems (CBCS) that monitors inadvertent operation, or failure, can result in a critical or catastrophic hazard. The monitoring will show that the inhibit is on or off and if there are any indicated changes. The CBCS will "verify" that power across the connector is off for the crew to mate or demate powered connectors.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 35 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2033 Extravehicular 2nd Inhibit for Mating/Demating Electrical Power Connectors (Voltage < 200 Vdc/RMS and Current < 67 Amps)

The Payload shall be designed such that the load downstream of the extravehicular (EVA/EVR) electrical power connector is the lesser of 3 amperes or 180 W per powered pin/conductive path prior to and during mate/demate if the powered circuit is greater than the values in Table 3.18.4-3 but less than 200 Vdc/RMS and less than 67 amperes.

Note: This is in addition to power inhibits upstream of the extravehicular (EVA/EVR) electrical power connector (reference M2M-SMA-UTIL-R-2030).

Rationale: First prioritization is for the hardware load design to be able to reduce power to the lesser of 3 amperes (at 28 VDC) or 180W (1.5 amperes at 120 VDC) per powered pin. For cases where hardware cannot be designed to reduce power below the defined thresholds, every effort should be made for the hardware load design to be below the spawling current threshold (current at which molten metal is ejected during mate/demate). Spawling current varies depending on the end item design. If that also can't be met, a second upstream inhibit will be needed or an Exemption B will have to be written (reference M2M-SMA-UTIL-R-2001 "Failure Tolerance to Catastrophic Hazards"). If an upstream electrical inhibit failure (as required in M2M-SMA-UTIL-R-2030) is experienced, a replacement upstream inhibit will be utilized prior to any mate/demate operations. The reduction of downstream draw is required for extravehicular activities because arcing and molten metal can cause a hole in the Exploration EVA Suit (xEVA Suit), potentially ignite the suit materials due to the high oxygen environments in the xEVA Suit, or damage safety critical ExtraVehicular Robotics (EVR) systems. This voltage threshold is not based on M2M Program electrical system design. See MA2-99-170, Crew Mating/Demating of Powered Connectors. The testing was performed with specific voltage across the connector and 200 V was determined to be the maximum. Amperage of 67 amps is provided as an additional, separate threshold requirement. 200 Vdc/RMS and amperage of 67 amps is the maximum which is from the requirement of M2M-SMA-UTIL-R-2032 where Extravehicular 2nd Inhibit for Mating/Demating Electrical Power Connectors is required at those thresholds. First inhibit requirement details are found in M2M-SMA-UTIL-R-2030. Current and Power limit is based on test performed in a vacuum/plasma environment. See EP5-5T1-015, Summary of the Electrical Connector Contact Arcing Test, and MA2-99-170, Crew Mating/Demating of Powered Connectors. This requirement applies to Crew EVA Mate/Demate of connectors or for connectors that are not easily replaced and must maintain long life certification (i.e., source or load side SORI or LPGF connectors). In cases of non-crew, yet potentially catastrophic mate/demate, reducing downstream current draw below the spawling current threshold of the contacts can be used in place of reducing the downstream load to the lesser of 3 Amperes or 180 W with Exemption B approval from the appropriate safety review panel. The "end user" is operation specific and refers to the component that is at the end of the electrical chain being mated/demated.

3.8 PAYLOAD BATTERIES

Battery is defined as one cell or a packaged or unpackaged assembly of two or more cells that provide stored electrical energy. Specific design and verification requirements for a battery are dependent upon the battery chemistry, capacity, complexity, charging, environment, and application. The variety of battery chemistries available, combined with the variety of battery-powered applications, results in each battery application having specific, unique requirements pertinent to the specific battery application.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 36 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Battery hazards are caused by buildup or venting of flammable, corrosive or toxic gasses and reaction products; the expulsion of electrolyte; and by failure modes of over-temperature, internal and external shorts, reverse current, cell reversal, leakage, recharging of over discharged batteries, and overpressure. Electrical, mechanical, or environmental abuse could cause internal cell pressure build-up that leads to rupture of battery, leakage of electrolyte, venting, fire or explosion with potential injury to the crew, or damage to equipment, M2M Crewed Element or other crewed space environment application having specific, unique requirements pertinent to the specific battery application.

At the battery, level similar hazard controls and hazard propagation when multiple batteries in series or parallel have to be addressed.

Detailed design information for all batteries on crewed spacecraft, including vehicle, payload, and crew equipment batteries are contained in JSC 20793, *Crewed Space Vehicle Battery Safety Requirements*.

Some potentially critical or catastrophic hazards, such as leakage and internal shorts, cannot practically be controlled using failure tolerance. Batteries may be exempted from the failure tolerance approach, at the discretion of the safety review panel, provided the risk they pose is mitigated using Exemption B to the maximum practical extent through a defined process in which approved standards and margins are implemented. (Refer to JSC 20793, Section 4.1.2.)

M2M-SMA-UTIL-R-2034 Payload Batteries

All batteries used on payloads shall be designed, selected, analyzed, and tested in accordance with JSC 20793, *Crewed Space Vehicle Battery Safety Requirements* and EP-1901, *Interpretation Memo for the Battery TR Propagation Requirements in JSC 20793*.

Rationale: JSC 20793 is the specification for use of batteries on crewed vehicles. Any payload that interfaces with an M2M Element must comply with that specification.

M2M-SMA-UTIL-R-2035 Payload Battery Management System

The use of a battery management system shall be physically isolated and incapable of powering on any payload system functions.

Rationale: The intent of this requirement is to preclude the possibility of the battery management system being an ignition source, either through electrical or thermal energy means. Powered off after battery charging operations refers to no current draw on the battery outside of the leakage current and parasitic loads associated with the battery packaging and assembly. The use of battery management systems is desirable for cell balancing concerning over voltage, under voltage, and over current during charge.

M2M-SMA-UTIL-R-2036 Overcharge Failure/Over-discharge Failure Protection

The battery/charger design shall maintain required failure tolerance against overcharge / over-discharge failure and prevent charging of an over discharged battery.

Rationale: For batteries with cells or cell strings that should not be charged (as in primary/nonchargeable batteries), redundant serial blocking diodes should be installed in each parallel leg of a battery consisting of primary cells to prevent circulating currents between parallel cells or cell stacks, unless tests show these currents cannot present catastrophic failure modes.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 37 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Small Schottky diodes have been used for this purpose to minimize voltage drop. (Derived from JSC-20793D, Crewed Space Vehicle Battery Safety Requirements, section 5.1.2.)

M2M-SMA-UTIL-R-2037 Payload Battery Temperature Extreme Protection

Batteries shall be designed to mitigate the failure mode of over/under-temperature.

Rationale: Controlling applicable, credible hazards is critical in ensuring a safe, reliable battery system. These controls can be at the cell or battery level. The effects of this condition result in the buildup or venting of flammable, corrosive, or toxic gasses; reaction products; and the expulsion of electrolyte.

M2M-SMA-UTIL-R-2038 Payload Battery External Short Protection

Batteries, battery circuitry, and packaging shall be designed to mitigate the failure mode of external shorts.

Rationale: Controlling applicable, credible hazards is critical in ensuring a safe, reliable battery system. These controls can be at the cell or battery level. The effects of this condition result in the buildup or venting of flammable, corrosive, or toxic gasses; reaction products; and the expulsion of electrolyte.

M2M-SMA-UTIL-R-2039 Payload Battery Reverse Current Protection

Batteries shall be designed to mitigate the failure mode of reverse current.

Rationale: Best practice is to use a diode in the positive leg of the battery. Controlling applicable, credible hazards is critical in ensuring a safe, reliable battery system. These controls can be at the cell or battery level. The effects of this condition result in the buildup or venting of: flammable, corrosive, or toxic gasses; reaction products; and the expulsion of electrolyte.

M2M-SMA-UTIL-R-2040 Payload Battery Cell Reverse Protection

Batteries shall be designed to mitigate the failure mode of cell reversal.

Rationale: Best practice for a series-parallel configuration is to use a fuse in the negative leg of each series cell string. Best practice for a parallel-series configuration is to use a fuse in the negative leg of each parallel cell string. Controlling applicable, credible hazards is critical in ensuring a safe, reliable battery system. These controls can be at the cell or battery level. The effects of this condition result in the buildup or venting of flammable, corrosive, or toxic gasses; reaction products; and the expulsion of electrolyte.

M2M-SMA-UTIL-R-2416 Payload Battery Cell Leakage Protection

Batteries shall be designed to mitigate the failure mode of cell leakage.

Rationale: Controlling applicable, credible hazards is critical in ensuring a safe, reliable battery system. These controls can be at the cell or battery level. The effects of this condition result in the buildup or venting of: flammable, corrosive, or toxic gasses; reaction products; and the expulsion of electrolyte.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 38 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2042 Payload Battery Overpressurization Protection

Batteries shall be designed to mitigate the failure mode of overpressurization (cell and pack level).

Rationale: Controlling applicable, credible hazards is critical in ensuring a safe, reliable battery system. These controls can be at the cell or battery level. The effects of this condition result in the buildup or venting of flammable, corrosive, or toxic gasses; reaction products; and the expulsion of electrolyte.

M2M-SMA-UTIL-R-2043 Payload Battery Cell-to-Cell Separation

Payload battery packs with greater than 80 Wh/kg specific energy cells shall provide a physical cell-to-cell separation of 1 mm, at a minimum, and include nonflammable material around each cell in case of a cell side wall rupture.

Rationale: Having structural support between cells will protect against side wall ruptures of the cell in the event of a cell thermal runaway. A nonflammable barrier between the cells will provide electrical isolation from the support structure, as well as additional protection against the effects from a thermal runaway within the pack. Payload battery over 80Wh are tested to be passively propagation resistance or if failed be redesigned to meet the propagation requirements of JSC 20793 section 5.1.5.1. and the EP-19-001 Interpretation Memo for the Battery TR Propagation Requirements in JSC 20793 Rev D. (See JSC 20793).

3.9 ELECTROMAGNETIC COMPATIBILITY

3.9.1 Electromagnetic Effects (EME)

EME includes such areas as EMI, ESD, corona, electrical grounding, electrical bonding, and RF compatibility. RF emitter safety requirements are defined in Section 3.9.2 – RF Transmitter Compatibility. EME compliance relies on verification activities defined in the Program Utilization Payload-Unique IRD to protect the vehicle and crew. Evaluation of the payload for determination of EME safety critical circuits is the purview of the safety review panel or its designee (e.g., Electromagnetic Effects Panel (EMEP), M2M Frequency Spectrum Management).

3.9.2 Protecting Against Hazardous RF Irradiation

RF transmissions hazards include intentional RF transmissions during in-space operations and/or unintentional RF transmissions. The Artemis and supporting Program Spectrum Managers will coordinate to ensure compatibility of payload spectrum utilization with M2M elements. (See M2M-30026, Artemis Spectrum Management and Control Plan and M2M-30035, Artemis Payload Interface Definition Document (IDD)).

M2M-SMA-UTIL-R-2044 Payload RF Transmission Protection

Payload Intentional RF transmitters shall provide protection against hazardous irradiation.

Rationale: Intentional RF transmissions can result in circuit degradation, damage, malfunction, inadvertent operations of M2M safety critical systems, crew contact hazards, including hazards

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 39 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

to M2M spacesuits. Intentional RF levels are to be defined for worst case RF output without attenuation or firmware/software controls that limit transmitter power to a level lower.

Examples include:

- *Interference with M2M Element safety critical functions,*
- *Interference with M2M Crewed Systems Safety Critical functions*
- *Malfunction/inadvertent operations of safety critical systems,*
- *Intravehicular Activity (IVA) crew health*

Lunar Surface Deployable payloads that contain intentional RF radiating devices are subject to additional requirements that can be found in the M2M Element requirements. <TBD-30043-002>

Payload developers should reference M2M-30026, Artemis Spectrum Management and Control Plan for additional responsibilities and requirements for obtaining regulatory approval for use of RF transmitters and planned use of frequencies through the supporting Program's Spectrum Manager. Spectrum analysis deliverables are required from the payload developer in order to determine their RF compatibility with M2M elements.

3.10 PAYLOAD COMMAND AND DATA HANDLING (C&DH)

The Lunar exploration systems (Artemis spacecraft and vehicles) C&DH system will provide services to payloads described in M2M-30038, M2M Utilization Interface Requirements Document (IRD). Key C&DH functions at the interface level are identified in Figure 3.10-1 C&DH to Payloads Context Diagram. The requirements in this section are general and apply whether the communication between C&DH system and the payload is wired, wireless, internal to the vehicle, or external to the vehicle. Payload to C&DH system communication onboard the vehicle will be via wired or wireless connectivity to support effective command and data handling.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 40 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

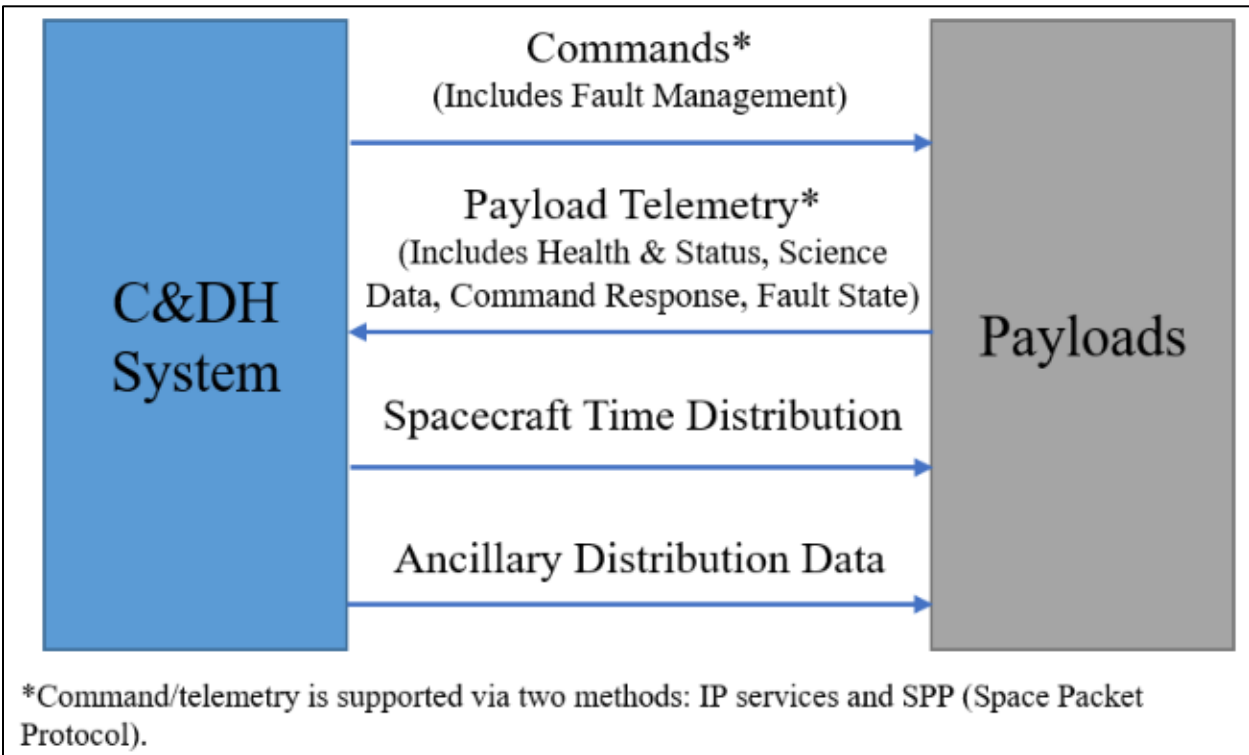


FIGURE 3.10-1 C&DH TO PAYLOADS CONTEXT DIAGRAM

M2M-SMA-UTIL-R-2045 Ground Initiated Hazardous Payload Commanding

Ground operations control centers which can issue hazardous commands shall be considered “certified” for hazardous commanding ensuring all the following:

- A. Command System Availability
- B. Hardware Failure/Software Error Detection
- C. Command System Initialization/Termination
- D. Command Hardware/Software Validation and Configuration Control
- E. Data Transfer Error Detection
- F. Data Integrity
- G. Safing Capability
- H. Command Access Restrictions
- I. Operational Fault Tolerance

Rationale: This requirement applies to ground operation centers which are initiating hazardous commands. Payloads with the potential for hazardous command uplink can choose to utilize a NASA approved control center (e.g., Payload Operations Integration Center (POIC)), when they are not a NASA approved control center. This requires the initiation of the hazardous command to be at the NASA approved control center and is integrated into the existing capabilities of that control center. If providers are utilizing a NASA approved control center, this requirement is already met by that NASA approved control center.

In the event remote control centers are not “certified” to provide the protections to prevent inadvertent commands, isolation of the remote ground operations center via a certified control

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 41 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

center isolation capability is permissible to ensure inadvertent commands are not uplinked from the uncertified remote ground operations center. If a remote center is utilizing the isolation method, the certified control will verify any needed inhibits are in place via telemetry sent to the certified control center prior to a potential hazardous event. If hazardous commands are unable to be removed from the remote center's database, then the isolation method will be used.

M2M-UTIL-INFO-0001 Payload Safing

Lunar exploration systems will remove power to the payload location within time-to-effect of receiving a payload fault message indicating the payload needs power removed, or the payload heartbeat recovery is unsuccessful.

Rationale: Payloads may detect an internal condition, such as a fire, and will notify the module it is powering down and needs power removed. The payload safing requirement (M2M-UTIL-R-1043) is listed in M2M 30038, Moon to Mars Utilization Interface Requirements Document. Its function is to remove power to the payload location within time-to-effect of receiving a payload fault message indicating the payload needs power removed, or the payload heartbeat recovery is unsuccessful.

M2M-SMA-UTIL-R-2046 Identification of Payload Hazardous Commands

Payload hazardous commands shall be identified.

Rationale: Hazardous commands (either external or internal to the payload) are those that can remove an inhibit to a hazardous function or activate an unpowered hazardous payload system, reduce safety critical redundancy, or reduce failure tolerance, create a hazardous condition, or control actively safed systems (such as robotics) during the timeframe the system is safed (or not in use). Lunar exploration systems (source of external commands) need to understand the impact of commands they send so that they can incorporate additional controls for their hazardous commands to control the hazards.

M2M-SMA-UTIL-R-2047 Payload Two-Step Hazardous Commands

The payload shall implement two-step commanding for hazardous commands.

Rationale: Two-step commanding ensures no single inadvertent external command results in execution of a hazardous command.

M2M-SMA-UTIL-R-2048 Autonomous Operation

If communication loss with a payload could result in a catastrophic or mission critical event, the payload shall provide the capability for autonomous operation of payload functions.

Rationale: This capability means that the payload does not depend on communication with Earth (e.g., mission control) to perform functions that are required to control the catastrophic and mission critical hazard. While the Crew is present, the payload should automate catastrophic and mission critical hazard controls to minimize the need for Crew actions; using Crew action only as a last resort, where automation is not practical.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 42 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.11 MONITORING

Monitors are indicators used to obtain status of functions, devices, inhibits and parameters. Incorporating monitors into circuits requires design considerations and risk trades. The problems identified below should not occur when monitors are working properly. In some cases, monitors can:

- Defeat inhibits or controls
- Provide false status indications (loss of input without providing an indicator change), or
- Prohibit response time to recover from payload failures.

M2M-SMA-UTIL-R-2049 Payload Monitoring <TBR-30043-001>

Monitors shall be available at all times and not affect the inhibits. Monitoring of two of three electrical inhibits is required when inadvertent operation could result in a catastrophic hazard and/or for electrical inhibits that can be removed by the crew, ground, or computer control commanding.

Monitoring is applied to Must Not Work Functions (MNWF), Must Work Functions (MWF), and Actively Safed systems.

- MNWF – A function, if performed inadvertently or at an in-opportune time, results in a hazard.
- MWF – A redundant function, if not performed, can result in a catastrophic hazard if the function is not performed.
- Actively Safed Systems – Only hazardous when system exceeds pre-defined limits.

Payload designs should be such that real-time monitoring is not required to maintain control of catastrophic functions.

Rationale: Monitoring includes status of inhibits, state of operations, and execution of safing functions. Monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible. When monitors are in circuits with inhibits and controls, monitors provide current-limiter functions to prevent load current from enabling, damaging, or disabling the inhibit. Current limiter functions can protect circuits from harmful effects due to a short-circuit or similar problems in the load.

Monitoring may not always be appropriate and status of inhibits may not be required. With the safety review panels, approval, monitoring and hazard detection, and safing may be utilized to support control of hazardous functions provided there is adequate crew response time available (time-to-effect (TTE) of the hazard) and safing procedures are developed. The TTE of the hazard is the time between the loss of an inhibit and the occurrence of the hazard.

Requirements for monitoring critical hazards are not normally imposed, but may be required by the safety review panel on a case-by-case basis. Monitoring of one of the two inhibits is prudent and the capability to restore inhibits to a safe condition should be available. When inhibits are not directly monitored, safety review panel's review to discern whether monitoring of the control of that inhibit may be considered on a case-by-case basis.

M2M-SMA-UTIL-R-2050 Payload Monitoring Without Reducing Safety

Monitoring circuits shall not add additional hazards.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 43 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: Monitoring circuits shall be designed such that the information obtained is as directly related to the status of the monitored device as possible without compromising or reducing safety of that monitored device.

M2M-SMA-UTIL-R-2051 Payload Lost Monitoring Identifiable

Failure of a safety critical monitor shall be identifiable.

Rationale: Examples of potential safety critical monitoring items are: valve position indicators, and thermal or pressure sensors. Examples of failure indication include: stale data telemetry, telemetry drop off, or telemetry noise signal. Personnel safety often depends on understanding the state of the system and providing a status that the monitoring function is no longer valid increased personnel awareness that something is wrong.

M2M-SMA-UTIL-R-2052 Utilization Payload Inhibits

A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits.

Rationale: Compliance with this requirement may be accomplished at the payload level or through a combination of hazard controls at the Segment/System levels. Requirements for monitoring of these inhibits and for the capability to restore inhibits to a safe condition are normally not imposed but may be imposed on a case-by-case basis.

Monitoring includes status of inhibits, state of operations, and execution of safing functions. Monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible.

When monitors are in circuits with inhibits and controls, monitors provide current-limiter functions to prevent load current from enabling, damaging, or disabling the inhibit. Current limiter functions can protect circuits from harmful effects due to a short-circuit or similar problems in the load.

M2M-SMA-UTIL-R-2053 Payload Timers

Payloads that use timers shall provide three independent timer inhibits or three independent timer safing capabilities.

Rationale: Timers are considered only one control to a hazard since there are many credible failure modes that can allow the timer to start prior to the desired time. Monitoring of timers is typically not available. Failure of a timer, or a computer causing bypass of a timer or any other credible failure to satisfy one inhibit is still just one failure.

A single timer that allows transfer of more than one inhibit without other controls renders the inhibits dependent. In this case, all inhibits transferred by a single timer are effectively only 1 inhibit enabled by a single timer.

The use of a timer can be used as one level of control of an inhibit when:

- *Timers cannot be bypassed by computers, ground commanding, or crew,*
- *Timers show no credible failure modes that result in loss of an inhibit.*

When credible failure modes exist that could allow the timer to start prior to a desired time, a safing capability will be provided. If this safing is via a RF command, then the command capability will be provided to the flight crew.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 44 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.12 SOFTWARE

Computer Based Control Systems (CBCS) use computer hardware and software as an integral part of the payload design. A computer-based or complex electronic-based control system includes any hardware, software or firmware used to prevent a catastrophic or critical hazardous event, regardless of the media the software or firmware resides on. This includes any Commercial Off-The-Shelf (COTS) software integrated into the CBCS design.

CBCS safety is the application of engineering and management principle, criteria, and techniques to provide hardware failure and software error tolerance to minimize risks associated with the use of computers to control hazards. The following CBCS and CBCS-related requirements will be applied to a payload's computer-based or complex electronic-based control systems, whose inadvertent operation, or failure, can result in a critical or catastrophic hazard. CBCS requirements are applied at the Payload-level. CBCS requirements do not need to be applied to lower-level components, such as sensors or actuators, if Payload-level compliance can be established.

CBCS requirements cover general computer-based design controls for must work (MW) functions (MWF) and/ or must not work (MNW) functions (MNWF). Some requirements apply to both MWF and MNWF, while controls that are only used for MWFs may not be possible to comply with requirements designed to protect for MNWFs and vice versa. In addition, if a situation arises where a particular requirement cannot be applied to the design and there is no viable work around it, an exception or deviation may be required. These types of situations should be brought to the safety review panel for review.

Software is classified as safety critical if the software is determined by and traceable to a hazard analysis. Software is classified as safety-critical if it meets at least one of the following criteria:

- a. Causes or contributes to a system hazardous condition/event,
- b. Controls functions identified in a system hazard,
- c. Provides mitigation for a system hazardous condition/event,
- d. Mitigates damage if a hazardous condition/event occurs,
- e. Detects, reports, and takes corrective action if the system reaches a potentially hazardous state.

M2M-SMA-UTIL-R-2054 Payload Safety Critical Software

Safety-critical software and requirements shall be developed in accordance with NPR 7150.2D *NASA Software Engineering Requirements*, SWE-134 (see below) which describes and defines the technical requirements for safety-critical software.

For safety-critical software or mission-critical software, the project manager shall implement the following items in the software: [SWE-134]

- a. The software is initialized, at first start and restarts, to a known safe state.
- b. The software safely transitions between all predefined known states.
- c. Termination performed by software functions is performed to a known safe state.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 45 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

- d. Operator overrides of software functions require at least two independent actions by an operator.
- e. Software rejects commands received out of sequence when execution of those commands out of sequence can cause a hazard.
- f. The software detects inadvertent memory modification and recovers to a known safe state.
- g. The software performs integrity checks on inputs and outputs to/from the software system.
- h. The software performs prerequisite checks prior to the execution of safety-critical software commands.
- i. No single software event or action is allowed to initiate an identified hazard.
- j. The software responds to an off-nominal condition within the time needed to prevent a hazardous event.
- k. The software provides error handling.
- l. The software can place the system into a safe state.

NOTE: These requirements apply to components that reside in a mission-critical or safety-critical system, and the components control, mitigate, or contribute to a hazard as well as software used to command hazardous operations/activities.

Rationale: The intent of this requirement is for determining if the software used in the payload is safety critical. In most situations, software is considered safety-critical when it can cause a hazard, is used to control a hazard, or is used to monitor a hazard.

M2M-SMA-UTIL-R-2055 Flight Software Development

The CBCS safety-critical flight software shall be developed in accordance with a formal software development process.

Rationale: The intent of this requirement is to ensure the provider follows a formal software development process when creating safety-critical software. Software is safety critical if it meets at least one of the following criteria in NASA-STD 8739.8A, NASA Software Assurance and Software Safety Standard:

- a. Causes or contributes to a system hazardous condition/event,
- b. Controls functions identified in a system hazard,
- c. Provides mitigation for a system hazardous condition/event,
- d. Mitigates damage if a hazardous condition/event occurs,
- e. Detects, reports, and takes corrective action if the system reaches a potentially hazardous state.

The software development process should include software requirements definition, design, implementation, verification, maintenance, and retirement phases, and incorporate software quality assurance, configuration management, problem reporting and corrective action, reliability, maintainability, safety, verification and validation, certification, and operational use of the software. Reference NPR 7150.2, NASA Software Engineering Requirements.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 46 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Payload CBCS Requirements:

M2M-SMA-UTIL-R-2055-001 Non-CBCS Compliant System Segregation

The Payload CBCS shall segregate (isolate) hazard control, hazardous commands, and safety critical data from non-safety critical functions.

Rationale: Computers that control hazards or hazardous commands must be isolated from systems that are not compliant to protect from corruption or interference of safety-critical functions. Physical separation is not mandated but preferred. Payloads with noncompliant CBCS systems must not have hazardous command interfaces.

M2M-SMA-UTIL-R-2055-002 Safe Initialization

The Payload CBCS shall safely initialize and safely transition between modes to a known, safe state without generating unplanned/spurious signals.

Rationale: The intent is to make sure that when initialized, the system cannot initialize to a state that will be unsafe. In this case, a safe state is defined as having no identified hazards present and no active system processes which could lead to an identified hazard. Additionally, this requirement applies when transitioning between states. For example, the initialization or state transition of a vehicle flight control system would be different while docked versus while in free flight. In the context of a propulsion system, one would not want a system to come up with a valve open if it should not be open. As another example, if memory has been initialized to a null state, then the input and output queues should likewise be empty. Unplanned or spurious signals could be interpreted by the effectors as a command and resulting in an unsafe condition and are therefore specifically verified not to be present during initialization.

M2M-SMA-UTIL-R-2055-003 Safe Termination

The Payload CBCS shall perform an orderly shut-down of a function to a known safe state upon receipt of a termination command or detection of a termination condition.

Rationale: The objective of this requirement is to reduce the potential for a shutdown to cause problems in other parts of the system. The system should place hazardous effectors in a safe state for the particular scenario. For most work functions, safe termination implementation should address safe termination of the last remaining leg of the function.

M2M-SMA-UTIL-R-2055-004 Off Nominal-Power Conditions

The Payload CBCS shall continue to operate safely (generate no spurious signals) during off-nominal power conditions or contain design features which safe the CBCS during off-nominal power conditions.

Rationale: The system should be able to operate safely not only during nominal conditions, but also during off-nominal conditions. For example, some power supplies have power conditioning to compensate for over-voltage and under voltage, and, with such conditioning, one would want to protect from brown outs. One would require energy storage in the power supply to enable the avionics to shut down safely. A safe state may mean a state with reduced functionality until the system can either resume normal operations or a safe power down can be achieved.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 47 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Note: For must work functions, the system will need to include protection for off nominal power conditions as opposed to safing the CBCS.

M2M-SMA-UTIL-R-2055-005 Actions for Overrides

Payload CBCS overrides shall require at least two independent actions by the operator.

Rationale: Independent actions by the operator help to reduce potential operator mistakes. For example, the second action provides situational awareness and confirmation that the action is, in fact, the desired action. When one executes an override, this typically bypasses the safety checks and balances, so one would want to ensure the operators are fully aware of what they are doing in a potentially high-risk situation. If the operational time to criticality time to effect does not allow for two operator actions, an equivalent design solution may be necessary, e.g., based on single operator action and a mode condition.

M2M-SMA-UTIL-R-2055-006 Commands Out of Sequence

The Payload CBCS shall reject commands received out of sequence if executing the commands out of sequence will cause a hazard.

Rationale: Rejecting commands received out of sequence is intended to mitigate potential hazards associated with commands issued spuriously or otherwise sequenced improperly. For command sequencing that is part of the hazard control strategy, the computing system may need to implement a strategy in a certain order, and without that order the system may remain in or enter a hazardous condition.

Note: Commands out of sequence requirement is a specific case of prerequisite checks.

M2M-SMA-UTIL-R-2055-007 Inadvertent Memory Modification

The Payload CBCS shall detect and recover from inadvertent memory (includes both temporary and long-term memory) modification during all modes of operation.

Rationale: As a result of inadvertent memory modifications, which may occur, as a result of, but not limited to, radiation-induced errors, uplink errors, and configuration errors, the computing system must be able to detect the problem and recover to a safe state. While memory modification protection may be used as a part of the overall design strategy, prevention does not satisfy this requirement.

M2M-SMA-UTIL-R-2055-008 Input Validation

The Payload CBCS shall discriminate between valid and invalid inputs from sources external to the CBCS and remain or recover to a known safe state in the event of an invalid external input.

Rationale: This requirement ensures that only valid input from external sources is incorporated into the control system state. External input includes commands and data (including new software images) as well as measurements from sensors attached directly to the CBCS. The equipment controllers receiving input (such as commands) from external sources, must validate whether the command is a known command, and parameter limit checking.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 48 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2055-009 Integrity Check

The Payload CBCS shall perform integrity checks when data or commands are exchanged across transmission or reception lines and devices.

Rationale: This requirement ensures that the data or command messages are not corrupted in transmission and that the data or command that was sent is the same as the data or command that was received. An integrity check ensures the message is well-formed and not corrupted.

M2M-SMA-UTIL-R-2055-010 Prerequisite Checks

The Payload CBCS shall reject hazardous commands which do not meet prerequisite checks for execution.

Rationale: This requirement is intended to ensure the safe execution of hazardous commands by checking that conditions are appropriate to the execution of the command.

Note: Where a prerequisite check can prevent the execution of a hazardous command, the status of that parameter should be made available to crew and ground operators of the certified control center via telemetry sent to and readable by the certified control center.

M2M-SMA-UTIL-R-2055-011 Disarming an Armed Command

Where two step commanding is required, a Payload mechanism for disabling the armed command shall be provided.

Rationale: The purpose of this requirement is to ensure that an accidentally or inadvertently armed command does not remain armed indefinitely. Typical examples would include time-out, a disarm command, or a disarm if the command following the arm is not the fire command.

M2M-SMA-UTIL-R-2055-012 Unique Command Messages

Where loss of a function could result in a catastrophic hazard, the Payload CBCS shall provide at least one independent and unique command message to disable each leg of control.

Rationale: For any catastrophic hazard, there will be at least two controls (legs) to prevent the hazard. This requirement ensures that at least two commands are required to disable the must work function. Developer will need to provide a list of the redundant functions within the fault tolerant capability and identify commands which can disable each of the legs of redundancy. The typical circumstances where a command would be issued to disable a leg of control to a must work function will be due to a failure or maintenance activities. Otherwise, it is assumed that all legs are active.).

M2M-SMA-UTIL-R-2055-013 One Operator Action

At least one independent operator action shall be required for each operator-initiated command message used in the shutdown of a capability or function that could lead to a hazard, or the removal of an inhibit that controls a hazard.

Rationale: This requirement protects against disabling legs of control by protecting against the scripting or combining of the "unique and independent" command messages together such that multiple commands, including inhibit removals, can be issued by a single operator action.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 49 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Note: this requirement does not apply to onboard system initiated FDIR responses. This requirement also prevents an inadvertent accidental removal of multiple controls to a hazard.

M2M-SMA-UTIL-R-2055-014 Redundant Command Path

Where the must work function protects for a short time to effect hazard and the software provides the sole control for safety critical must work functions, another non-identical method for commanding the function shall be provided.

Rationale: This requirement is intended to assure that time critical and safety critical commanding can be completed in the presence of a failure of the nominal command path. This requirement is applied if the time to effect of the hazard precludes the ability to perform a remove and replace or similar operational workaround.

M2M-SMA-UTIL-R-2055-015 Redundant Command Path Independence

Alternate or redundant functional paths shall be separate or protected such that any single credible event which causes the loss of one functional path will not result in the loss of the redundant functional path.

Rationale: This requirement assures that the redundant command paths established under M2M-SMA-UTIL-R-2050-014 are not subject to a single event which can result in the failure of multiple paths.

M2M-SMA-UTIL-R-2055-016 Failure Independence

A failure occurring within a computer, or its interfaces shall not prevent other computers from performing their intended safety function.

Rationale: The intent of this requirement is to ensure that a single computer, that is operating erroneously, cannot impair the ability of other computers from performing the necessary detection and safing.

M2M-SMA-UTIL-R-2055-017 Change of State of Inhibits

Command messages to change the state of inhibits shall be unique for each state and each inhibit.

Rationale: This requirement prohibits a use of a single command to toggle an inhibit between enabled and disabled. This assures that a command cannot cause an inhibit to be removed unintentionally. Thus, one command cannot simply toggle (change) the inhibit but must explicitly state "enable inhibit x" or "disable inhibit x". A command to change the state of an inhibit regardless of its current state would be prohibited under this requirement.

M2M-SMA-UTIL-R-2055-018 Independent Parameter for FCA

Where hazardous commands can be initiated by a hard-coded, automated, failure recovery sequence, the CBCS shall ensure a separate, functionally independent parameter shall be checked before issuance or execution of each hazardous command.

Rationale: As an exception to the prohibition against combining inhibit removals into scripted sequences, it is sometimes necessary to combine these commands in order to provide time

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 50 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

critical automated recovery capability. When this is done, those commands are required to provide this independent parameter check. The separate, functionally independent parameter check is needed to ensure that, before the hazardous command is executed or issued, conditions are appropriate for the safe and necessary execution of the hazardous command. It is a way of reducing the risk of an incorrect execution and to verify that the automated sequence will not create additional hazards.

Note: Where a prerequisite check can prevent the execution of a hazardous command, the status of that parameter should be made available to crew and ground operators.

M2M-SMA-UTIL-R-2055-019 Independent Control of an Inhibit

A processor shall not independently control multiple inhibits to a hazard.

Rationale: The intent is not to have a single or the same processor, due to a malfunction, lose control of multiple inhibits to a hazard. A single processor can control a single inhibit for several hazards but not control multiple inhibits for a single hazard.

This requirement allows computers with multiple processors to be used if they can establish true independence between processors and inhibit controls.

M2M-SMA-UTIL-R-2055-020 Fault Detection and Annunciation

The Payload CBCS shall detect and annunciate faults to the crew, at any location, that affect safety critical systems, subsystems, and/or crew health.

Rationale: It is necessary to alert the crew to faults (not just failures) that affect critical functions. A fault is defined as a defect that when executed under the appropriate conditions may cause a failure. A failure is the inability of a system or component to perform its required functions within specified performance requirements.

M2M-SMA-UTIL-R-2055-021 Recover from CBCS Anomaly

The Payload CBCS shall detect, isolate, and recover to a known safe state in the event of an anomaly within the CBCS.

Rationale: The intent of this requirement is to establish a safe state following detection of incorrect or incomplete processing as determined by the Hazard Analysis. A typical error may include events such as: single event upset (SEU), computer/processor miscompare or voted out computer/processor, unhandled arithmetic exception, Built in Test, or other mechanisms for determining incorrect or incomplete processing. A typical response to an error of this type would include a reset of the effected computer/processor to a predetermined, known, initial configuration (safe state).

M2M-SMA-UTIL-R-2055-022 Data for Manual Safing

Where the performance of manual safing is required, the Payload CBCS shall notify the crew or ground operators of the need to perform manual safing and provide the data necessary for the performance of manual system safing for the identified hazard, and safe within the Time to Effect of the hazard.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 51 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: In order for crew or ground operators to perform manual safing, the crew need to be notified (for example, caution and warning alarms) of need to perform the safing and have the data necessary to enable them to perform the safing.

M2M-SMA-UTIL-R-2055-023 Controlled System Failure Detection

The Payload CBCS shall provide real-time detection of failures in the controlled system, where independence exists between sensors used for nominal closed loop system control and those used for failure detection.

Rationale: This requirement addresses the need for a closed loop control system to be monitored independent of the system that is controlling the hazardous effectors. This assures that compromise of the control loop does not prevent the safing from taking place.

M2M-SMA-UTIL-R-2055-024 Notification of Safing

Payload processors detecting a failure shall notify other systems providing safing actions.

Rationale: The intent of this requirement is to ensure that all safing functions are notified of the condition and can begin the appropriate actions.

M2M-SMA-UTIL-R-2055-025 Safing Actions

The Payload systems, providing safing actions necessary to control a critical or catastrophic hazard shall immediately perform safing.

Rationale: For the purposes of this requirement, immediate is considered to be within either the next major cycle or within the time to effect of the hazard, whichever is shorter. The intent of this requirement is to ensure safing is immediate, not compromised, and degradation of the system does not prevent safing from occurring. This requirement establishes the expectation that the time to effect for each hazard is quantified and the system has been verified to have the necessary safing capability.

M2M-SMA-UTIL-R-2055-026 Failure Resolution

After a failure of an inhibit to a Must Not Work Function (MNWF), Payload system operations shall be automatically suspended to ensure loss of a second inhibit will not result in activation of the MNWF.

Rationale: The premise of the fail-safe approach is reliant on a fully fault-tolerant capability to detect anomalous behavior and safe in such a situation. Continued operation of the system in a degraded mode should not be considered.

M2M-SMA-UTIL-R-2055-027 Unique Detection and Safing

The Payload CBCS shall use different functionality for each detection and safing function used to control the hazard.

Rationale: This requirement is intended to ensure that there are no common mode failures in the logic of the individual detection and safing functions. For example, copy and paste errors are protected because the functionality for each detection and safing function must be unique. Consideration of Time to Effect (TTE) and severity of the hazard should be considered when

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 52 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

determining the necessary degree of differentiation between different detection and safing methods.

M2M-SMA-UTIL-R-2055-028 Independent Controller Monitor

The Payload shall ensure a computer (or feature) independent of the computer directly controlling the hazardous function provides detection and safing for hardware or software failures of the controlling computer.

Rationale: The premise behind this requirement is that a failing/failed computer-controlled system cannot be relied on to provide detection and safing of its own failure.

M2M-SMA-UTIL-R-2055-029 Use of Timers

The Payload timing functions that provide control of inhibits to protect from a catastrophic hazard shall provide safing capabilities if the timer fails.

Rationale: Timers are considered only one control of an inhibit to a hazard. Monitoring of timers is typically not available. When credible failure modes exist that could allow the timer to start prior to a desired time, a safing capability must be provided. If this safing is via a RF command, then the command capability must be provided to the flight crew.

M2M-SMA-UTIL-R-2055-030 Monitor Capabilities

Where inadvertent activation or failure to activate a function may result in a catastrophic hazard, the Payload shall monitor the status of those functions, inhibits, and controls, including changes to the state of the indicator upon loss of input or failure of the monitors, and provide safety critical status to the crew and ground operators of the certified control center via telemetry sent to and readable by the certified control center.

Rationale: Controls are hardware and software features provided to mitigate (reduce the likelihood of) the cause of a catastrophic hazard. Inhibits are a special implementation of hazard controls for safety-critical functions, which disable the functions. Monitoring controls and inhibits ensures they are always functional and effective. In addition, monitoring provides situational awareness of the state of the payload and the risks presented by a change in the status of these controls. This knowledge can support actions to move to a less hazardous state or inform decisions while operation in this state.

3.13 MATERIALS AND PROCESSES

In establishing safety requirements for materials used in and/or for spaceflight or for materials being studied in the space environment, special considerations are required. Precautions are taken to keep the crewmembers, environment, vehicle's systems hardware, and vehicle safe. Capability and limitations are considered for the clean-up of potential leakage and/or exposure of the crew and system hardware, the compact living environment, and the limited ability to provide assistance and supplies. Altered material properties and physical responses due to the decreased gravitational environment and increased oxygen environment are also be taken into consideration when evaluating and planning for the use of materials.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 53 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

The following material requirements are established to prevent and control hazards. Materials selection requirements address hazards from material flammability, offgassing and compatibility. Hazardous materials requirements address hazards from external and internal release in the following subsections:

- 3.13.1 Materials Selection
- 3.13.2 Flammability Hazard Level (FHL) Hazard Rating
- 3.13.3 Material Offgassing
- 3.13.4 Hazardous Materials
- 3.13.5 Chemicals
- 3.13.6 Toxicity Hazard Level (THL) Hazard Rating

NOTE: See section 3.14 Biosafety Level (BSL) for biological materials.

The Program assigned to lead the safety review will require additional data to assess the payload materials. To help the payload project the lead Program will assign a payload engineer to help identify this data (e.g., data needed for toxicological assessment of chemicals to be flown on manned spacecraft).

3.13.1 Materials Selection

These requirements are intended to ensure proper material selection. Flammable materials could cause initiation or propagation of a fire in the presence of an ignition source. Offgassing of toxic products in the M2M Elements' environment could lead to illness or long term health effects for the crew. Materials compatibility issues could cause unacceptable degradation of the materials and result in hazardous conditions within the payload or within the spacecraft environment.

Materials used in the fabrication of payloads should be selected by considering the operational requirements for the particular application and the design engineering properties of the candidate materials. The operational requirements include, but are not limited to, operational temperature limits, loads, life expectancy, and vehicle related induced and natural space environments. The worst-case anticipated use environment (i.e., most hazardous pressure, temperature, material thickness, and fluid exposure conditions) is used in the evaluation of material suitability.

The design engineering properties to be considered in material selection include mechanical properties, fracture toughness, stress corrosion, thermal and mechanical fatigue properties, fluids compatibility, etc. These are covered with structural design and pressure system requirements within this document. Conditions which could contribute to deterioration of hardware will receive special consideration.

NASA Marshall Space Flight Center (MSFC) Materials and Processes Technical Information System (MAPTIS) contains a listing of materials (both metallic and nonmetallic) with a rating indicating acceptability for each material's characteristic. Although primarily designed for experienced users, it can be used to help select materials that have already been shown to meet the applicable acceptance criteria. MAPTIS is accessible via the Internet at <http://maptis.nasa.gov> (registration is required) and the appropriate safety panel can provide assistance on its use. For materials which create potentially hazardous situations as described in the paragraphs below and for which no prior NASA test data or rating exists, other test results should be provided for a safety review or the payload provider can request assistance from the appropriate safety review panel in conducting further evaluation or applicable tests.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 54 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

The use of materials that do not strictly comply with the requirements in this document might still be acceptable in the specific hardware application and will be assessed on a case-by-case basis. Rationale to demonstrate that a materials application is acceptable will be documented in a Material Usage Agreement (MUA) and/or HR for all materials that are technically acceptable but do not meet the requirements in this document.

M2M-SMA-UTIL-R-2056 Payload Materials

Materials selection and process control shall meet NASA-STD-6016, *Standard Materials and Processes Requirements for Spacecraft* or its equivalent.

Rationale: A listing of materials (both metals and nonmetals) with a "rating" indicating acceptability for each materials characteristic is available electronically in the NASA MSFC MAPTIS. Properties to be considered in material selection include, but are not limited to, the following:

- (1) Mechanical properties.
- (2) Fracture toughness.
- (3) Flammability and offgassing characteristics.
- (4) Corrosion.
- (5) Stress corrosion.
- (6) Thermal and mechanical fatigue properties.
- (7) Glass-transition temperature.
- (8) Coefficient of thermal expansion mismatch.
- (9) Vacuum outgassing.
- (10) Fluids compatibility.
- (11) Microbial resistance.
- (12) Moisture resistance.
- (13) Fretting.
- (14) Galling.
- (15) Susceptibility to electrostatic discharge (ESD).
- (16) Susceptibility to lunar dust contamination (see NASA-STD-1008, *Classifications and Requirements for Testing Systems and Hardware to be Exposed to Dust in Planetary Environments*)

3.13.2 Flammability Hazard Level (FHL) Hazard Rating

The NASA/JSC Materials and Processes Branch, the NASA SME, assess flammability hazards for all chemicals and test materials. All payload chemicals to which the crew might be exposed are assigned an FHL rating. FHL ratings were developed by NASA Subject Matter Experts (SMEs) and are unique to the spaceflight and spacecraft environments. The FHL takes into consideration the physical state and flash point of the chemical. For liquids and powders, the FHL is the flammability hazard that would result if the chemical was released into the vehicle; without regard to the controls that prevent release of the chemical. For gases, the FHL is the flammability hazard that would result based on leakage of the chemical. The assessment takes into consideration that pressurized gases can leak from a container until the internal pressure is cabin ambient pressure, resulting in the potential for formation of a localized flammable gas cloud. The flash point is the lowest temperature at which a chemical can form vapors or an ignitable mixture in the air that will ignite given an ignition source. A lower flash point is an

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 55 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

indication that the chemical is easier to ignite. The allowable quantity of flammable chemicals that could be released depends on the chemical's flash point.

Chemical and material processing and related reactions are assessed for flammability. The FHL of a mixture of chemicals is determined from the flammability of the entire mixture or the most flammable component in that mixture depending on the chemical components. Descriptions of the five FHLs are provided in the Table 3.13.2-1.

Most flammable fluids are toxic at lower concentrations than their lower flammability limit resulting in the response to leaks of flammable fluids being driven by the response to the Toxicological Hazard Level (THL). Nontoxic flammable gases such as hydrogen and methane would have a higher FHL than THL hazard rating. The preferred method to prevent release of chemicals that are flammable is through Levels of Containment (LoC). Refer to JSC 64825A, *Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials*, for additional details.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 56 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE 3.13.2-1 FLAMMABILITY HAZARD LEVEL (FHL) AND HAZARD SEVERITY

Hazard Severity	FHL	Description	Flash Point*	
Acceptable (Not a hazard)	0	Any liquid, powder or gas considered to be a nonflammable material and limited quantities of flammable liquids and powders based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of < 20 liters	Temperature °C (°F)	Volume (ml)
			< 49 (120)	< 5
			49 (120) – 93 (200)	< 25
			93 (200) – 148 (300)	< 50
			> 148 (300)	<250
Critical	1	Flammable liquid, powder and gas; quantity limits for liquid and power are based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of 20-100 liters	< 49 (120)	5 – 25
			49 (120) – 93 (200)	25 – 100
			93 (200) – 148 (300)	50 – 250
			> 148 (300)	250 – 1000
Catastrophic	2	Flammable liquids and powders; quantity limits are based on the flammable material's flash point	< 49 (120)	25 – 100
			49 (120) – 93 (200)	100 – 250
			93 (200) – 148 (300)	250 – 500
			> 148 (300)	> 1000
	3	Flammable liquids and powders; quantity limits are based on the flammable material's flash point	< 49 (120)	100 – 250
			49 (120) – 93 (200)	250 – 500
			93 (200) – 148 (300)	500 – 1000
			> 148 (300)	
	4	Flammable liquid, powder and gas; quantity limits for liquid and powder are based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of ≥ 100 liters	< 49 (120)	> 250
			49 (120) – 93 (200)	> 500
			93 (200) – 148 (300)	> 1000
			> 148 (300)	
Description details developed in coordination with NASA/JSC Materials and Processes Branch based on JSC 64825A, Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials.				
The final FHL will be provided with the NASA SME evaluation on the HMST.				
* The flash point is the lowest temperature at which a chemical can form vapors or an ignitable mixture in the air that will ignite given an ignition source. A lower flash point is an indication that the chemical is easier to ignite.				

3.13.3 Material Offgassing

M2M-SMA-UTIL-R-2057 Non-Metallic Materials Off-gassing

Non-metallic materials shall be selected to avoid producing toxic levels of off-gassed products in order to protect ground and flight crews.

Rationale: This requirement only applies to payloads in the M2M Element pressurized environment. Offgassing is the release of chemicals from materials – the new car smell is an example of material offgassing. Offgassing can result in a toxic atmosphere if chemical compounds accumulate in a spacecraft closed environment and reach concentrations above their Spacecraft Maximum Allowable Concentrations (SMAC). Payloads are assessed to ensure they do not generate toxic levels of offgassing products into the crewed environment. MAPTIS contains a listing of materials and payloads that have been subjected to offgassing tests. The

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 57 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

material offgas rating in MAPTIS is based upon the amount of the material that is allowed. If not all major use materials are listed in the MAPTIS database, toxic offgassing testing is normally required. Offgassing tests of payloads should be in accordance with NASA-STD-6001, Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures.

M2M-SMA-UTIL-R-2058 Material Out-gassing

Materials shall be selected to minimize contamination of adjacent payloads and vehicle hardware which may be sensitive to outgassing.

Rationale: Contamination of other payloads or spacecraft hardware could impact these items and lead to failures. Nonmetallic payload materials exposed to space vacuum should be tested in accordance with ASTM E595-15 Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment.

M2M-SMA-UTIL-R-2059 Materials and Fluid Compatibility

Payload materials and fluids shall be compatible.

Rationale: Material compatibility refers to chemical reaction between a fluid and materials in contact with that fluid, resulting in unacceptable degradation of the materials or the fluid. In some cases, chemical reaction can lead to ignition of the materials or the fluid. Ignition of a material may occur in contact with oxidizer fluids like oxygen and ignition of a fluid may occur by a material catalyzing exothermic decomposition of hypergolic fuels like hydrazine. Material compatibility can be a concern with fluids used in cleaning, test, and operation in all system environments and service life. NASA-STD-6001, Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures, in addition to NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft, addresses hazardous fluids such as gaseous oxygen, liquid oxygen, fuels, oxidizers, and other fluids that could chemically or physically degrade the system or cause a potentially hazardous exothermic reaction.

Special attention should be paid to payload materials used for or with an enriched oxygen environment. An Oxygen Compatibility Assessment (OCA), as required by NASA-STD-6001, is necessary for pressurized oxygen system hardware. The assessment may identify areas where testing is required before the hardware can be approved. An OCA may also be necessary for compressed air systems and pressurized systems containing enriched oxygen (greater than 21 percent oxygen by volume). The need to conduct an OCA for these systems will be determined during the initial safety review. It is recommended that the White Sands Test Facility be consulted when performing an OCA. Per NASA-STD-6016, any system containing nitrogen tetroxide (NTO) may require an analogous NTO compatibility assessment (NTOCA) due to flammability risks of the exposed materials.

Note that the compatibility of service fluids with individual materials is not considered a valid substitute for an adequate functional qualification of a component that contains moving parts and has a specified cycle-life when exposed to the fluid of interest.

3.13.4 Hazardous Materials

A hazardous material is any item, substance, or agent (such as physical, chemical, biological, and/or radioactive), which has the potential to cause harm to the crew, the M2M Element environment, and/or equipment either by itself or through interaction with other materials and/or

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 58 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

factors. The use of hazardous materials cannot always be avoided in spaceflight, so requirements are established for hazard prevention through controlling the release of hazardous materials. Flammability requirements associated with hazardous materials are addressed in section 3.13.2 *Flammability Hazard Level (FHL) Hazard Rating*.

Using Failure Tolerance to Prevent Release of Hazardous Materials

The failure tolerant design approach applies levels of hazard controls to prevent hazards. The required number of levels of hazard controls are based on the hazard severity. Marginal hazards are required to have one level of hazard control. Critical hazards (single failure tolerant) are required to have two levels of hazard control. Catastrophic hazards (two failure tolerant) are required to have three levels of hazard control. The appropriate number of levels of control should exist for all phases of use of the end item hardware. Phases of use include, but are not limited to, launch, stowage, operations (including sample manipulations and maintenance), return, and/or disposal (including trash/waste). The preferred application of levels of hazard control to prevent the release of hazardous materials (including volatile lunar samples) is through Levels of Containment (LoC).

LoC requires concentric independent layers (physical barriers) in the payload design where each individual layer is of a design integrity able to contain the hazardous material. The required number of independent levels of physical barriers is based on the hazard severity and is maintained throughout the flight. If any of the levels of containment are opened during the mission and then, resealed for continued containment or exchanged for a different level of containment, reestablishing the containment is verified by leak test, approved procedure, or design certification. Manipulations or changes in the levels of containment may require the addition of another level of containment prior to removal or exchange in order to maintain the required number of levels of containment. Table 3.13.4-1 is provided as a guideline for the relationship between LoC/C and hazardous material hazard ratings.

TABLE 3.13.4-1 LEVELS OF CONTAINMENT/CONTROL AND HAZARD RATINGS

	0 LoC/C Not a Hazard	1 LoC/C Marginal Hazard	2 LoC/C Critical Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard
Hazard Response Level (HRL) (Color of Label)	0 (GREEN)		1 (BLUE)	2 (YELLOW)	3 (ORANGE)	4 (RED)
Toxicity Hazard Level (THL)		0	1	2	3	4
Biosafety Level (BSL)		1	2 (Mod)	2 (High)		
Flammability Hazard Level (FHL)	0		1	2, 3, 4		

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 59 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Environmental Control and Life Support System (ECLSS) Hardware Impact Rating (E-Rating)	E0-E1	E2-E3	E4-E6			
	0 LoC/C Not a Hazard	1 LoC/C Marginal Hazard	2 LoC/C Critical Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard

Notes:

- [1] HRL (color indicated in table) is an indication for the integrated on-orbit response for THL, BSL and FHL; HRL reflects the minimum for post-spill safety clean-up and does not necessarily reflect the level of containment/control required for the end item design.
- [2] LoC/C are assessed by the M2M Program SRPs as part of the safety review process.
- [3] Controls for Marginal Hazards are documented in the SDP and/or may be verified through the applicable IRD.
- [4] THL 2-4 and BSL-2H all require 3 LoC/C.
- [5] THL 4 requires Program Manager approval for use on M2M Program Vehicles
- [6] Varying LoC/C for FHLs are based on hazardous material properties/quantities in the end item.
- [7] E-Ratings are included to show the relationship to LoC/C and are not part of the HRL.
- [8] LoC/C for physical agents are also based on the hazard severity.
- [9] The flammability hazard level of a liquid is determined by a combination of the flash point and volume of that liquid and is based upon the assumption that the entire volume of liquid is spilled. For gases, the flammability hazard level determined on a case-by-case basis.
- [10] Substances that have a FHL of 3 or 4 are given a Flammability Label (Flame) along with a Hazard Label based on the worst-case hazard.
- [11] While the FHL of a substance does not drive a need for PPE, FHL 2-4 require at least 2 levels of containment for clean-up, and therefore are designated HRL 1.

3.13.5 Chemicals

Requirements for the use of payload chemicals are established to prevent hazards associated with chemicals such as impacts to crew health and environmental contamination. Chemicals are addressed here based on the prevention of payload chemical release and based on the reduction in hazard controls during operations with THL-1 and FHL-1 liquids.

M2M-SMA-UTIL-R-2060 Chemical Release

Chemicals within a payload shall be controlled to prevent release with levels of failure tolerance based on the on hazard response level.

Rationale: This requirement does not apply to crew food, drinking water from the galley, crew personal preference items, or items considered to be structural components. If any of these items are used in a manner different than what is intended here (such as for experimental purposes), an evaluation may be requested by the appropriate safety review during the safety review process.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 60 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

This requirement applies to all chemicals that are located in or may be introduced into the pressurized habitable environment (including payloads returning from or routinely used in the unpressurized environment). It is established to protect the crew from chemically-induced toxicity hazards and/or to protect the environment and Lunar Exploration System or Vehicle equipment from contamination hazards. Toxicity hazards are chemicals that may be harmful to crews (including physiological effects such as irritation to skin or eyes).

3.13.6 Toxicity Hazard Level (THL) Hazard Rating

The THL ratings were developed by the NASA SMEs, in the JSC Toxicology and Environmental Chemistry Group, and are unique to the spaceflight, spacecraft, and space exploration environments (Reference: Memorandum Number TOX-VR-2023-01 Rev G *Evaluation of Particles/Dusts in Habitable Spacecraft*). The THL depends on the intrinsic toxicity and physical properties of the chemical without regard to physical containment (i.e., full release of material).. The THL and other hazard ratings (biosafety, flammability, and ECLSS) will be collectively documented on the payload's Hazard Materials Summary Tables (HMST). If the chemical is considered to not be one of the hazards identified here, the associated hazard rating would be marked as "N/A" for Not Applicable on the HMST. Toxicity hazards are chemicals (toxicants) that may be harmful to crewmembers with physiological effects such as irritation to skin or eyes. Flammability hazards are chemicals that may ignite, burn, combust, and/or catch fire resulting in harmful byproducts, decrease in breathable air, and/or equipment damage. ECLSS impact hazards are chemicals that may adversely impact Lunar Exploration System or Vehicle ECLSS hardware resulting in a degraded/compromised pressurized environment (crew living environment) and/or spacecraft ECLSS hardware damage. Since chemicals have multiple hazard ratings, the hazard severity for release of the chemical is determined by the highest hazard rating.

Controls to prevent release of chemicals are provided through failure tolerance or exemption based on the hazard severity. All chemicals should maintain a minimum of one control to prevent release (containment or other appropriate controls) at all times. Documentation of chemical usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the appropriate safety review panel.

Payloads Returning From or Routinely Used in the Unpressurized Environment:
Controls, such as placing the item in a sealed container or allowing for bake off time, are implemented prior to bringing external payloads into the pressurized environment.

The following is collectively taken into consideration when assessing payload chemicals and assigning THLs: the chemical's physicochemical properties (physical state and chemical properties of chemical), total quantity, human physiological effects (e.g., irritancy, carcinogenicity, systemic toxicity), and, when appropriate, the rate at which the chemical is removed from the environment/vehicle. The ECLSS Cabin Environmental Impact Rating (additional details below) is also considered when assessing chemicals as it aids in understanding length of time and dose of crewmember exposure. In such cases, an integrated assessment is coordinated between two NASA SME groups. When the assessment is complete, the THL is documented on the payload's HMST.

The THL of a mixture of chemicals is determined from the toxicity of the entire mixture or, if not known, the most toxic component in that mixture. The hazards before, during, and after chemicals are processed and related products are assessed. If there is little or missing

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 61 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

information for a chemical (for example: COTS items), the THL rating will be conservative to ensure safe conditions on Lunar Exploration System or Vehicle.

NOTE: Material offgassing, sometimes referred to as toxic offgassing, is generally not assessed under THL hazard ratings. For details on the THL data submittal and the HMST verification process, reference JSC 27472, *Requirements for Submission of Data Needed for Toxicological Assessment of Chemicals to be Flown on Manned Spacecraft*.

Descriptions of the five THLs are defined in JSC 27472 and provided in Table 3.13.1.6-1. Utilization of potentially catastrophic uncontainable chemicals, rated as THL-4 chemicals are prohibited from entering crewed compartments.

TABLE 3.13.6-1 TOXICITY HAZARD LEVEL (THL) AND HAZARD SEVERITY

Hazard Severity	THL	Description
Marginal	0	any gas, gel, solid, or liquid that has the potential for, at worst, short-term, slight chemical (i.e., not mechanical) irritation that will not require therapy
Critical	1	any gas, gel, solid, or liquid that has the potential for slight to moderate irritation that will not resolve quickly (in <30 minutes) without intervention
Catastrophic	2	a containable solid, gel, or non-volatile liquid that has the potential for moderate to severe irritation and/or ocular damage that may have a long-term performance impact
Catastrophic	3	a containable solid or low-volatility liquid that has the potential for appreciable systemic effects, long-term serious injury (e.g. cancer), or internal tissue damage
Catastrophic	4*	an uncontainable gas, volatile liquid, or fine particles/fume that has the potential for moderate to severe irritation, and/or appreciable systemic effects, and/or a long-term performance impact
Description developed by the JSC Toxicology and Environmental Chemistry Group based on JSC 26895, Guidelines for Assessing the Toxic Hazard of Spacecraft Chemicals and Test Materials. The final THL will be provided with the NASA SME evaluation on the HMST * THL-4 chemicals require safety review panel approval for use in the Lunar Exploration System or Vehicle habitable pressurized environment		

NOTE: The NASA SMACs and the American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Values (TLVs) indicate maximum concentrations of exposure to airborne contaminants (i.e., vapors). The SMACs, TLVs, and THLs are based on different criteria and are meant to be used in very different circumstances so there is no direct quantitative relationship between them.

The ECLSS Hardware Impact Rating (E-Rating) is used to understand ECLSS performance or hardware impacts such as functional degradation, operational constraints and/or life cycle impacts relative to planning for resupply and/or refurbishment. Descriptions of the seven E-Ratings are provided in the Table 3.13.6-2.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 62 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE 3.13.6-2 ECLSS HARDWARE IMPACT RATING (E RATING) AND HAZARD SEVERITY

Hazard Severity	ECLSS Hardware Impact Rating (E Rating)	Description
Acceptable (Not a hazard)	E0	No ECLSS performance degradation. No change in scheduled maintenance. (Operational capacity* consumption is <2%, with 100% of the capacity margin** retained.)
	E1	No ECLSS performance degradation. No change in scheduled maintenance. (Operational capacity consumption is >2% and <10%, with > 10% of the capacity margin consumed.)
Marginal	E2	ECLSS functional performance is degraded by <10%. Early replacement of consumable components may be necessary within nine months. (Operational capacity consumption is >10% and <25%, with > 25% of the capacity margin consumed.)
	E3	ECLSS functional performance is degraded by >10% and <25%. Early replacement of consumable components may be necessary within six months. (Operational capacity consumption is >25% and <50%, with > 50% of the capacity margin consumed.)
Critical	E4	ECLSS functional performance is degraded by >25% and <50%. Early replacement of consumable components may be necessary within one month. (Operational capacity consumption is >50% and <75%, with > 75% of the capacity margin consumed.)
	E5	ECLSS functional performance is degraded by >50% and <75%. System maintenance is required to restore functional performance within one week. (Operational capacity consumption is >75% and <90%, with 100% of the capacity margin consumed.)
	E6	ECLSS functional performance is degraded by >75%. System maintenance is required to restore functional performance within one day. (Operational capacity consumption is >90%, with >100% of the capacity margin consumed.)
Description details developed in coordination with NASA ECLSS Engineering Group based on JSC 66869, Guidelines for the Assessment of Chemicals and Materials for Impacts to Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft. The final E Rating will be provided with the NASA SME evaluation on the HMST. * Operational capacity: capability of the system performance ** Capacity margin: allowance provided for system performance (hardware is nominally operated at less than 100% to allow for margin)		

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 63 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2061 Reduction In Failure Tolerance For Chemicals (Liquids) During Operations

Payloads shall provide a minimum of one level of control to prevent release of THL-1 and FHL-1 liquids.

Rationale: This requirement applies exclusively to THL-1 and FHL-1 liquids during the payload's operational phase where these liquids are necessarily handled, (i.e., setup, data collection, fluid manipulations, and tear down). This requirement does not apply to THL-1 or FHL-1 liquid that would have a hazard severity higher than critical due to another hazard rating. This requirement also does not apply to any other hazardous material that would be rated under THL or FHL ratings or other hazard ratings (for example: non-liquid THL-1 materials, non-liquid FHL-1 materials, biological materials, radioactive material, etc.). This requirement does not impact the on in-flight operational response that would occur in response to an inadvertent spill of hazardous materials.

Controls to prevent release of chemicals are provided through failure tolerance based on the hazard severity. This requirement is assuming application of the failure tolerance control method, reference Section 3.2 Failure Tolerance for details. The release of THL-1 or FHL-1 liquid is considered to be a critical hazard severity, which nominally requires two levels of control. When utilizing a failure tolerance approach, the control to prevent release of hazardous materials has traditionally been through the implementation of levels of containment. All chemicals should maintain a minimum of one control to prevent release (containment or other appropriate controls equivalent to containment) at all times.

The single level of control addressed in this requirement should be successfully demonstrated and verified to remain valid during all expected, worst-case environmental conditions and prevent the release of the THL-1 or FHL-1 liquid. Upon completion of operations, the second level of control will be re-established at the earliest opportunity. Two levels of control are still required during launch, stowage/trash, and return.

M2M-SMA-UTIL-R-2062 Radioactive Payload Material Release

Payloads containing radioactive material shall prevent the release of the radioactive source material and energetic particles emitted by the source material.

Rationale: This requirement applies to all radioactive materials that are located in or may be introduced into the pressurized habitable environment and are not considered exempt or under exemption per the U.S. Nuclear Regulatory Commission (NRC) Regulations Title 10, Code of Federal Regulations (CFR). It is established to protect the crew from physiological impacts and the environment and vehicle from contamination due to exposure to radiation source material and secondary emissions.

NOTE: *It is recommended that if the payload does need radioactive materials. the payload development team include a radiation expert that understands the complexity of working with radioactive materials. For pre-/post-flight ground processing, the payload provider should comply with appropriate license requirements. This may include obtaining special license(s).*

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 64 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.14 IN-FLIGHT BIOSAFETY LEVEL

The In-Flight Biosafety Level (BSL) ratings provided by the NASA SMEs, NASA/ JSC Biosafety Review Board (BRB), are unique to spaceflight. The rating structure was derived from the four BSL categories established for biohazardous materials in ground-based laboratories by the U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH) with additional considerations made for the unique environment and conditions of spaceflight. For example, due to microgravity conditions in space, aerosols from microorganisms can be more of a risk factor than on Earth as larger particles and droplets can be suspended as aerosols for longer timeframes. In consideration of microgravity, the BSL-2 category is divided into BSL-2M (Moderate) and BSL-2H (High). Descriptions of the five In-Flight BSLs are provided in Table 3.14-1.

Biological material is documented on the HMST. Biological material considered to be biohazardous material will be assigned an In-Flight BSL rating, also referred to as BSL. Biological material that is determined to be non-infectious and outside the biohazard category will not be assigned a BSL rating.

Factors that affect the BSL rating include the origin and volume of the biological material, physical state of the sample growth medium (solid or liquid), infectivity dose, medical or spacecraft integrity consequences, and proposed operations/usage. If there is limited information available on a biological material or the operation and use, the BSL rating may be elevated to ensure safe conditions on Lunar Exploration System or Vehicle. When two or more biohazardous materials or agents are present in a payload, the hazard severity will be driven by the highest BSL rating.

Samples and cell lines purchased from suppliers will typically be identified with a BSL rating. The NASA BRB In-Flight BSL rating evaluation may differ from supplier BSL information. The NASA BRB rating will serve as the rating by which the payload hardware will be evaluated for flight.

Prohibited Biological Material: Biological materials rated BSL 3 and 4 are prohibited from the M2M Crewed Element as the M2M Crewed Element (both the internal and external environments) is not equipped to provide the necessary protection from these biological materials. Prions (an infectious protein particle similar to a virus but lacking nucleic acid; thought to be the agent responsible for scrapie and other degenerative diseases of the nervous system) are considered BSL-3 and are not allowed on M2M Crewed Elements.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 65 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE 3.14-1 NASA IN-FLIGHT BIOSAFETY LEVEL RATING AND HAZARD SEVERITY

Hazard Severity	NASA Biosafety Level (BSL) Rating	Description
Marginal	1	Well-characterized agents not known to consistently cause diseases in healthy adults, minimal hazard to environment
Critical	2M (Moderate)	Moderate risk agents associated with human disease. Primary exposure routes include: skin (percutaneous) exposure, ingestion, and mucous membrane exposure.
Catastrophic	2H (High)	Higher risk agents associated with human disease. Risk is increased by lower infectious dose, likelihood of aerosolization, larger amounts of agent presents and other factors
Not Allowed*	3	Agents with potential for airborne transmission. May cause life-threatening diseases.
	4	Agents with high potential for life threatening disease. High potential for aerosol transmission of agent with no disease prevention (prophylactic) or specific therapy
<i>Description developed in coordination with NASA/JSC Biosafety Review Board based on JSC Procedural Requirements (JPR) 1800.5, Biosafety Review Board Operations and Requirements.</i> NOTE: The In-Flight BSL is commonly referred to as BSL instead of In-Flight BSL		

M2M-SMA-UTIL-R-2063 Biological Material Release

Payload biological materials shall be controlled to prevent release with failure tolerance based on the hazard severity shown in Table 3.14-1.

Rationale: This requirement applies to all biological materials that are located in or may be introduced into the pressurized habitable environment. It is established to protect the crew and environment from immediate or latent biohazards, including contamination of food and water supplies. Biohazards are biological materials or biological agents that may be harmful to the crew and/or to the environment. This requirement encompasses live and cultured biological materials used in payloads and/or collected as samples from Lunar Exploration System or Vehicle. This requirement also applies to vectors of biological materials such as animals and plants, non-biological materials such as soil or dust, and environmental conditions such as warm, moist air that may harbor or promote the growth of biological materials.

Controls to prevent release of biological materials are provided through failure tolerance or exemption based on the hazard severity. The preferred method to prevent release of biological materials is through LoC. Documentation of biological materials usage, along with the controls containment methods for all phases and conditions of use, is supplied for review and approval by the appropriate safety review panel.

Due to the typically nonvolatile nature, biological materials do not impact the ECLSS impact hazard ratings.

3.14.1 Animals

The NASA SMEs that review animal use are the JSC BRB, the NASA/Flight Institutional Animal Care and Use Committee (IACUC), and the NASA Chief Veterinarian. Invertebrates are typically

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 66 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

reviewed by the BRB and vertebrates are jointly reviewed. An integrated assessment is coordinated between the SME groups with the assigned In-Flight BSL and any special notes documented on the payload's HMST.

Payloads involving animals and related operations are reviewed on a case-by-case basis. Cross-Program utilization safety requirements for animals will be developed at a later time. <FWD-30043-004>

Special consideration is given to operations that involve the crew handling animals or coming into contact with animal experiment products such as waste. The primary concern with animals is the prevention of zoonotic disease, a disease that can spread from animals to humans, and contamination of the environment. The use of feral or non-colony born animals is discouraged due to the potential for a greater variety of pathogens.

Animals and samples taken from animals are appropriately controlled at all times. Animal housing units and glove boxes or workstations designs include particulate matter filters and keep it from exhausting into the crewed environment. Procedures involving renewing animal food supplies or removing animal waste should not expose the crew to the animals. Refer to requirements in JPR 1800.5, *Biosafety Review Board Operations and Requirements*, for additional details on animal experiments.

Rodents: NASA has developed a listing of mouse pathogens based on potential zoonotic diseases. Specific Pathogen Free (SPF) certified rodents are required to be utilized for crew flight activities. For a listing of the NASA approved vendors and detailed testing protocols pre-flight to certify mice as SPF mice, refer to JPR 1800.5.

3.15 PHYSICAL AGENTS

The term "physical agents" is used here to specify the response of materials in microgravity and their use in spaceflight and spacecraft. Physical agents are materials or substances that become hazardous or more hazardous based on how they act and respond in microgravity. The differences in the way particles and fluids respond in environments where the gravitational force is different than on the Earth's surface (for example lower force (microgravity) on Lunar Exploration System or Vehicle or increased force during launch and landing) may create hazards. Some physical agents (for examples some particles and THL-0 fluid) are nominally considered non- or marginally hazardous and become more hazardous when released in appreciable concentrations or large mass due to how they act and respond in microgravity. Requirements for payload physical agents are addressed based on the prevention of release of physical agents and based on the prevention of release of shatterable materials, a unique set of physical agents.

NOTE: Hazard controls related to lunar dust that would be brought into the crew compartment with returning payloads is assessed by each M2M element. < FWD-30043-005>

M2M-SMA-UTIL-R-2064 Physical Agents Release

Payload physical agents whose release would create hazards shall be controlled to prevent release.

Rationale: This requirement encompasses particles and fluids that are located in or may be introduced into the pressurized habitable environment and act as physical agents when released.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 67 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

It is established to protect the crew from physiological hazards and/or to protect the environment and Lunar Exploration System or Vehicle equipment from hazards resulting from contamination.

Documentation of physical agent usage, along with the controls for all phases and conditions of use, is supplied for review and approval to the safety review panel.

M2M-SMA-UTIL-R-2065 Particle Release

Payload particles whose release would create hazards shall be controlled commensurate with the hazard severity to prevent release.

Rationale: Particles that are determined to be chemically inert and/or insoluble in water are a nuisance at low concentrations and a physical hazard at high concentrations. The concentrations identified in the Table 3.15-1 apply to short duration events driven by failures that would release particles rapidly. It does not apply to a routine or intermittent source of particles or over long periods of time. For these particles and use, hazard control measures to limit exposures should be implemented. For example, nanoparticle generation by routine three dimensional (3D) printing should be controlled to prevent release or limit release to acceptable levels. Consideration should also be given to implementing the Occupational Safety and Health Administration (OSHA) recommendations that work with nanomaterials occur in ventilated enclosures (e.g. glove box, laboratory hood, or process chamber) equipped with High Efficiency Particulate Air (HEPA) filters.

Table 3.15-1 is provided as a reference based on specific particle density, lung deposition, and minute volume; the concentration limit will differ for different minute volumes or particle densities. The routine or purposeful release of particles should be identified when the payload data is provided for review as indicated in the verifications. As particles addressed here are considered physiological hazards instead of chemically induced toxicity hazards, a THL rating is not assigned; instead, the details will be captured in the payload's HMST as a note in the comments section.

Physiological Hazards: The unique attributes of the decreased gravitational environment cause particles to remain suspended in the air for extended timeframes. The main physiological hazards caused by particle release for the crew are suffocation and asphyxiation. Particles > 10 μm in diameter released in large amounts cannot be inhaled deeply into the lower respiratory tract (lungs) but could cause acute asphyxia (suffocation within a few minutes) due to mechanical blockage of the upper respiratory tract, especially the larynx. Particles $\leq 10 \mu\text{m}$ diameter can be inhaled deeply into the lungs and cause a slow asphyxiation (suffocation within many minutes to hours) by obstructing the deep lung and interfering with oxygen exchange.

Acceptable Level: Concentrations below occupational limits are considered acceptable as they are not expected to cause any significant hazard or permanent health issue. Control to prevent release is not required but remains recommended when feasible. The release of particles in this size and concentration are considered to be a nuisance and will be indicated as such on the HMST.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 68 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE 3.15-1 PHYSICAL AGENTS AND HAZARD SEVERITY

Type of Particle	Target Organ	Acceptable Nuisance Level	Critical Hazard	Catastrophic Hazard
Reactive, toxic, soluble	Eyes, URT, Lungs, Skin	Case-by-case	Case-by-case	Case-by-case
Inert, insoluble > 10 µm; < 500 µm	URT	$C \leq 10 \text{ mg/m}^3$	$10 \text{ mg/m}^3 < C < 50 \text{ g/m}^3$	$C \geq 50 \text{ g/m}^3$
Inert, insoluble $\leq 10 \text{ µm}$	Lungs	$C \leq 3 \text{ mg/m}^3$	$3 \text{ mg/m}^3 < C < 13 \text{ g/m}^3$	$C \geq 13 \text{ g/m}^3$ *
Inert, insoluble sharps	Eyes	$PS \leq 50 \text{ µm}^\dagger$	N/A	$PS > 50 \text{ µm}$
Inert, insoluble non-sharps	Eyes, URT	$PS \geq 500 \text{ µm}^\dagger$	$PS < 500 \text{ µm}^\dagger$	$C \geq 50 \text{ g/m}^3$

URT = upper respiratory tract; C = concentration; PS = particle size
 *Concentration limit will vary based on minute volumes and particle density. This value assumes a particle density of 1.5 g/cc, 50% deposition in the lungs, and a minute volume of 10 liters/min during an exposure duration of about 360 minutes, divided by a safety factor of 2.
 †Particles of this size may present a potentially catastrophic hazard if released at high velocity

M2M-SMA-UTIL-R-2066 Containment of Shatterable Materials

Payloads that contain shatterable materials where containment is to be removed, shall include procedures requiring the crew shall inspect for damage prior to opening and when applicable restore containment after operations.

Rationale: Shatterable materials are sometimes used in the open cabin, and inspection prior to removing containment to ensure materials are not released into the cabin, Likewise, for safety reasons the shatterable materials need to be returned to containment after use.

M2M-SMA-UTIL-R-2067 Fluid Release

Payloads shall prevent the release of fluid into the habitable volume with containment commensurate with Hazard Severity.

Rationale: The hazard severity for release of fluid is categorized based on potential leakage volume Physical Agent Assessments and the Hazardous Materials Summary Table and the toxicity level, Table 3.13.6-1 Toxicity Hazard Level (THL) and Hazard Severity.

All payload physical agents should be included in the assessment review request. Specific examples of items to include in the assessment request are payload materials that produce particles such as dust, constituents of thermal insulation panels such as vacuum insulation panels and filters such as activated carbon and particle mesh filters. These items can degrade and release particles while in-flight. All payload fluids should also be included in a Payload Physical Agent Assessments and the Hazardous Materials Summary submitted with the hazard report(s).

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 69 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2068 Contamination Control

Payloads shall include controls on contamination-sensitive manufacturing processes, such as adhesive bonding, controls on packaging for shipment and storage, and a Foreign Object Damage/Debris (FOD) Prevention Program.

Rationale: Maintain clean environment in all M2M Ground Facilities and Elements. Additional guidance can be found in NASA-STD-6016C, Standard Materials and Processes Requirements for Spacecraft, section 4.2.6.7 Contamination Control.

M2M-SMA-UTIL-R-2069 Payload Pre-Flight Microbial Contamination

Payloads shall ensure that bacterial and fungal concentrations on the surfaces do not exceed the following acceptability limits, and no microorganisms that pose a risk to crew health or environment are present.

- 1) 10,000 Colony Forming Units (CFUs) / 100 cm² bacteria
- 2) 100 Colony Forming Units (CFUs) / 100 cm² fungi

Rationale: Preflight payload integration microbial limits are intended to limit the presence of medically significant bacteria and fungi and ensure that bacterial and fungal contamination on spacecraft internal surfaces can be controlled during spaceflight missions. The verification should include analyses of the test data show microbial levels are within the specified bacterial and fungal parameters, and no medically significant organisms have been identified.

M2M-SMA-UTIL-R-2070 Visibly Clean Internal Payloads (Habitable)

Payloads shall conform to Visibly Clean–Sensitive (VC–S) cleanliness level as specified in GSDO-RQMT-1080, *Cross-Program Contamination Control Requirements*, paragraph 3.4.1 Visual Cleanliness Level Requirements using portable hand-held incident lighting, unless specific hardware items require a more stringent cleanliness level.

Rationale: Preflight clean surfaces are intended to limit the presence of medically significant materials and ensure that contamination on spacecraft internal surfaces can be controlled during spaceflight missions.

M2M-SMA-UTIL-R-2071 Visibly Clean External Payloads

External payloads shall conform to GSDO-RQMT-1080 Visibly Clean–Sensitive (VC–S) cleanliness level before close-out, including areas that are inaccessible in the final assembly, and that may act as contamination sources while in flight.

3.15.1 Shatterable Materials

Shatterable materials are unique physical agents. A shatterable material is any material that can fracture under a load or impact and produce fragments that are potentially hazardous to the crew and/or vehicle. Common shatterable materials include glass, ceramics, LCD monitors, certain metallic alloys, optical equipment, and any other frangible materials that can fracture and produce fragments. Shatterable material requirements are addressed based on preventing release of fragments and based on protecting optical glass from fracture.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 70 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2072 Shatterable Materials Release

Payloads with shatterable materials shall prevent the release of fragments larger than 50 micrometers (μm) into the habitable volume.

Rationale: This requirement encompasses shatterable materials that are located in or may be introduced into the pressurized habitable environment. It is established to protect the crew from physiological hazards and/or to protect the environment and M2M equipment from hazards resulting from contamination.

M2M-SMA-UTIL-R-2073 Use of Shatterable Materials

Payloads containing shatterable materials shall comply with the requirements in NASA-STD-5018, Strength, Design and Verification Criteria for Glass, Ceramics and Windows in Human Space Flight Applications.

Rationale: Mission safety. Brittle or shatterable materials may fail completely and create FOD injuring crew or damaging hardware.

M2M-SMA-UTIL-R-2074 Optical Glass Protection

Camera lenses, filters, and any other optical glass shall be non-stressed (no delta pressure), and protected.

Rationale: Optical glass is typically thicker than regular glass (e.g., Digital Single-Lens Reflex (DSLR) camera lenses), and less susceptible to damage from contact loads. Optical glass should not protrude beyond the plane of the outer rim of the lens casing (i.e., it should be recessed to provide protection when in use). Protection of the optical glass can be provided via lens caps when not in use.

Use of optical glass typically involves the crew when the protective cap or covering is removed from the glass to prevent contact loading. When not in use, the payload should be stowed or the shatterable components protected. The intent of this is to prevent inadvertent impacts from the crew or other equipment that might result in glass fragments.

3.16 RESERVED

3.17 FIRE PROTECTION

Fire protection includes three factors: fire prevention, fire detection and fire suppression. Safety relies on fire prevention to mitigate a fire event. Fire detection and suppression are considered responses to a fire event rather than controls to preventing a fire.

3.17.1 Fire Prevention

Fire prevention is accomplished primarily by controlling flammable materials and ignition sources. Flammable materials are controlled per Section 3.13 and ignition sources are minimized via adherence to electrical design requirements such as proper bonding, grounding, wire and

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 71 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

fuse sizing, and circuit protection per section 3.7. An ignition source is a source of heat sufficiently intense and localized to induce combustion.

3.17.2 Fire Detection and Fire Suppression

Any payload with a potential fire source should consider fire detection and suppression as part of the integrated environment with the vehicle. Detection and suppression design requirements are levied and verified via each M2M Elements ECLSS documentation. <FWD-30043-006> The assigned Payload Integration Manager (PIM) will work with the payload project to determine the applicable requirements and associated verification(s).

3.18 HUMAN SYSTEMS SAFETY (IVA)

This section covers topics with a direct effect on the crew. The topics include acoustics, touch temperature, contact hazards, lasers and broadband light (radiation), emergency lighting and emergency response. NASA-STD-3001, Volume 2 NASA Space Flight Human-System Standard: Volume 2: Human Factors, Habitability, and Environmental Health provides information concerning crew anthropometric data, range of motion, etc. that is not repeated below. The requirements below focus on IVA crew safety.

3.18.1 Acoustics

Acoustics requirements are intended to protect crew hearing and allow them to hear audible alarms and perform critical communication. A source that emits noise for a cumulative total of more than eight hours in any 24-hour period is considered a continuous noise source. A source that emits noise for a cumulative total of eight hours or less in any 24-hour period is considered an intermittent noise source. A source that emits noise with a sound level of 37 dBA or less, measured 60 cm (2 feet) from its loudest point is considered an insignificant noise source.

Noise levels are measured either as an A-weighted sound level as a single decibel (dBA), overall sound pressure level (dB), value or using a family of Noise Criterion (NC) curves, which describe the relative loudness of an area or noise source. Each NC curve defines the values at each sound pressure level values at each octave band frequency from 60 to 16,000 Hz that must not be exceeded. The NC level (e.g., NC-52) is a single value which represents a complete sound spectrum. For more information on NC curves, refer to ANSI/ASA S12.2-2008.

Intermittent noise sources must meet the intermittent noise requirements. These intermittent sources are managed to ensure the sound level and time limits are not exceeded.

Payloads must identify to the Safety Review Panel (SRP) those noise sources that do not meet the limits established. If the SRP determines the exception creates a critical or catastrophic hazard, the payload provider will be required to define controls and verifications to mitigate the hazard. Noise sources above 80 dBA are not allowed and must be discussed during the phased safety review process if the potential exists for exceeding the limit.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 72 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2075 Impulse Noise Hazard Limit

Payload impulse noise shall be less than 140 dB peak overall sound pressure level at the crewmember's head location.

Rationale: A limit of 140-dB peak SPL for impulse noise prevents acoustic trauma (OSHA 29 CFR 1910.95, Para 1910.95(b)(2) and WHO Environmental Health Criteria 12 – NOISE, Para 3.1.3).. Impulse noise is defined as a change in Sound Pressure Level (SPL) of more than 10 dB in one second or less.

Hearing protection cannot be used to satisfy this requirement.

This requirement is applicable during the worst-case operational scenario and closest nominal distance to the crewmember's head. This includes the equipment operating in the loudest mode of operation that can occur in flight under nominal crew or hardware operation circumstances, during setup, and/or when doors/panels are opened or removed.

M2M-SMA-UTIL-R-2076 Intermittent Noise Limits

Payload operating in crewed compartments shall be equal to or less than the A-weighted Overall SPL Limits during the Maximum Noise Duration as specified in Table 3.18.1-1 and as shown in Figure 3.18.1-1.

Note 1: These acoustic requirements do not apply during failure or maintenance operations.

Rationale: SPL Limits for Intermittent Noise, the intermittent noise requirement protects for effective communication, habitability, and noise exposure. The cumulative duration of the intermittent operation will be determined by the maximum noise level produced by the payload 0.6 m from its loudest surface during its loudest intermittent operation. This requirement is not applicable to impulse noise.

TABLE 3.18.1-1 INTERMITTENT NOISE A-WEIGHTED OVERALL SOUND PRESSURE LEVEL AND CORRESPONDING OPERATIONAL DURATION LIMITS (MEASURED AT 0.6M)

Maximum Noise Duration Per 24-Hour Period	L _{Amax} (dBA re 20 µPa)
8 Hours	≤ 49
7 Hours	≤ 50
6 Hours	≤ 51
5 Hours	≤ 52
4.5 Hours	≤ 53
4 Hours	≤ 54
3.5 Hours	≤ 55
3 Hours	≤ 57
2.5 Hours	≤ 58
2 Hours	≤ 60
1.5 Hours	≤ 62
1 Hour	≤ 65
30 Minutes	≤ 69
15 Minutes	≤ 72
5 Minutes	≤ 76
2 Minutes	≤ 78

1 Minute	≤ 79
Not Allowed	≥ 80

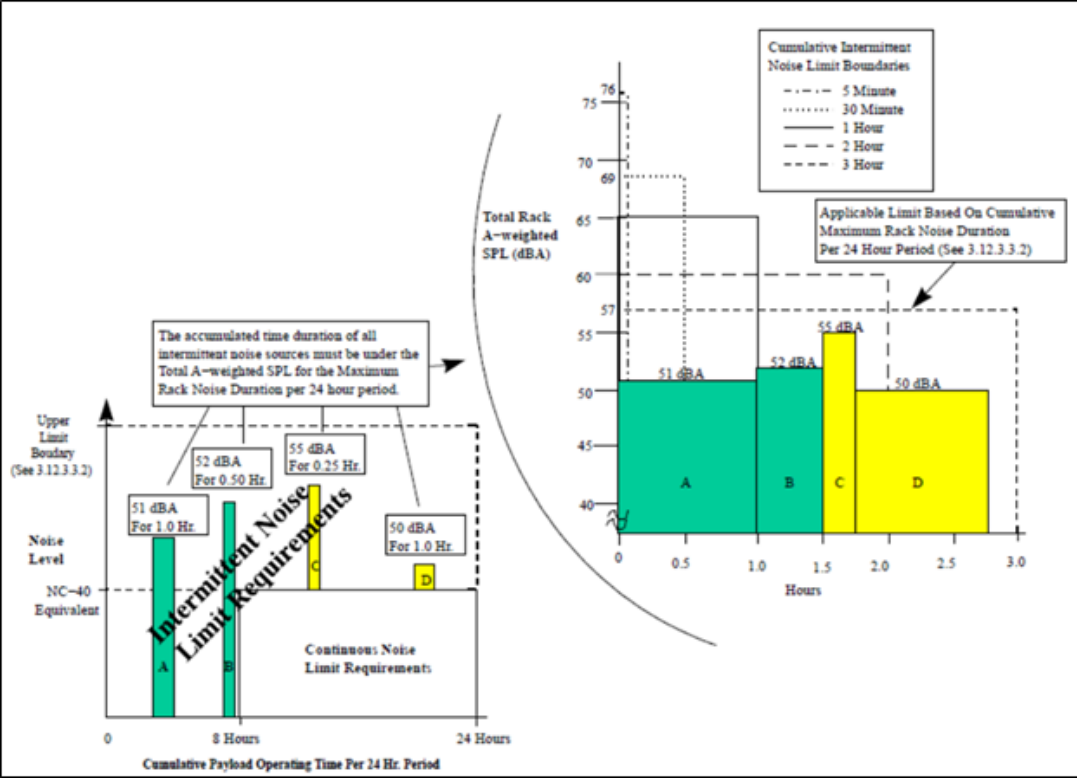


FIGURE 3.18.1-1 INTERMITTENT NOISE LIMITS

M2M-SMA-UTIL-R-2077 Payload Audible Alarm

To ensure alarm audibility, the SPL of Class I and II alarms at the operating position of the intended receiver shall meet at least one of the following criteria:

- Using measurements of A-weighted sound levels [ISO 7731:2003(E), method a) in Section 5.2.2.1], the difference between the two A-weighted SPLs of the signal and the ambient noise is greater than 15 dBA ($LS_{A} - LN_{A} > 15$ dBA).
- Using measurements of octave-band SPL [according to ISO 7731:2003(E), method b) in Section 5.2.3.1], the SPL of the signal in one or more octave-bands exceeds the effective masked threshold by at least 10 dB in the frequency range from 250 Hz - 4000 Hz ($LS_{i,oct} - L_{Ti,oct} > 10$ dB).
- Using measurements of 1/3 octave-band SPL [according to ISO 7731:2003(E), method c) in Section 5.2.3.2], the SPL of the signal in one or more 1/3 octave-bands exceeds the effective masked threshold by 13 dB in the frequency range from 250 Hz - 4000 Hz ($LS_{i,1/3oct} - L_{Ti,1/3oct} > 13$ dB).

Rationale: This requirement is applicable to emergency and warning tones and ensures they are audible over the continuous noise in the habitable areas. Acoustic measurements are periodically taken in-flight and are used as a basis to quantify the ambient noise.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 74 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

If the alarm signal is intended to arouse sleeping occupants, option 1 above must be utilized. When using options 2 or 3, the alarm must meet the requirement in at least one octave or 1/3 octave band, respectively.

M2M-SMA-UTIL-R-2078 Audible Alarm Hazard Limit

Alarm signal's A-weighted Sound Level shall be 95 dBA or less at the location of the intended receiver.

Rationale: Alarms are allowed to produce sound levels up to 95 dBA in order to provide adequate design space for audibility. This is considered safe since alarms can be silenced.

Continuous Noise Limits

Cross-program utilization payloads that operate continuously must comply with the continuous noise limits provided in program-specific requirement documents (e.g., GP 10037 PIDD). In cases in which a continuously operating payload has competing continuous noise limits (NC-37 vs. provider specified NC level), then the most stringent requirement must be satisfied. The intermittent noise requirement specifies the permitted operational duration for intermittently operating noise sources based on their maximum measured sound level (dBA).

3.18.2 IVA TOUCH TEMPERATURE

Touch temperature requirements for payload exposed surfaces are established to protect crew from skin damage. Touch temperature is addressed here based on the acceptable touch temperature limits for bare skin contact and based on payload functional design. Hazard controls to consider include waiting until payload surface reaches acceptable temperatures or use of personal protective equipment (PPE) like gloves. Pain/Non-Disabling Injury Skin Temperature Limits, are summarized in Figure 3.18.2-1 —Summary of Bare Skin Exposure Temperature Ranges below. {Reference NASA-STD-3001V2 Rev D)

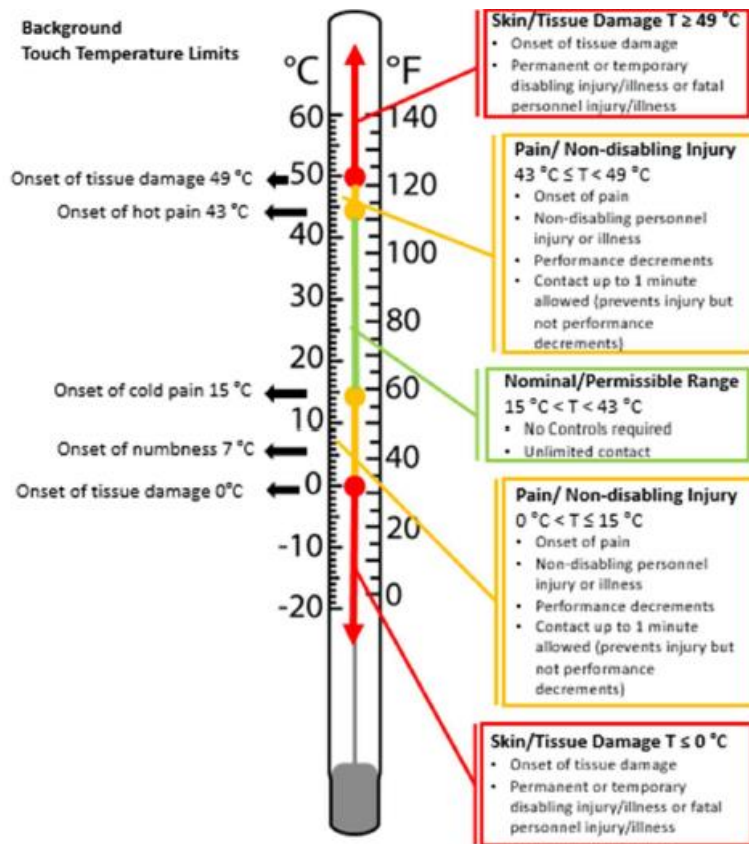


FIGURE 3.18.2-1 SUMMARY OF BARE SKIN EXPOSURE TEMPERATURE RANGES

M2M-SMA-UTIL-R-2079 Touch Temperature Limits

For payload exposed surface temperature (T_{ES}) greater than 49° Celsius (C) (120.2° Fahrenheit (F)) or less than 0°C (32°F), bare skin contact shall be controlled based on permissible material temperature (T_{PM}) and skin contact time (incidental and intentional contact).

Rationale: This requirement applies to payloads inside and/or connected to the M2M internal pressurized environment. Additional information on the derivation of hot and cold temperature limits can be found in NASA-STD-3001. Volume 2, 39.3.2.1.

M2M-SMA-UTIL-R-2080 Touch Temperature Based on Payload Functionality

For payloads with exposed surface temperature (T_{ES}) that is outside the acceptable permissible material temperature (T_{PM}) due to payload functionality, bare skin contact shall be prevented through the use of controls.

Rationale: This requirement applies to payloads that are intentionally designed to be outside of the acceptable, non-hazardous temperature range of 0°C (32°F) to 45°C (113°F) due to the purpose of the payload. This includes payloads that are specifically designed to function as freezers or heaters.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 76 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.18.3 IVA CREW CONTACT HAZARDS

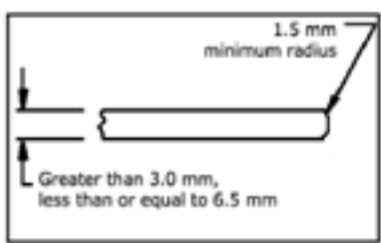
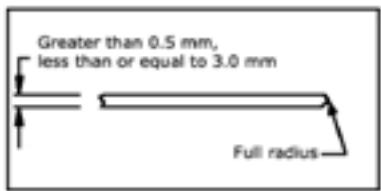
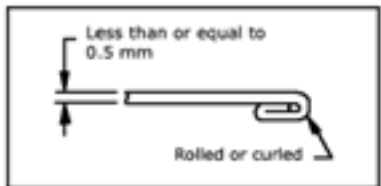
Crew exposure to hazards associated with sharp edges, latches, levers, cranks, hooks, controls, and holes located within the payload, must not pinch, snag, cut, entrap, or abrade the crew. Resulting injuries can range from a minor nuisance to potentially catastrophic.

M2M-SMA-UTIL-R-2081 Sharp Edges and Protrusions

Payload edges and protrusions to which the bare skin of the crew could be exposed shall be rounded as specified in Tables 3.18.3-1 *Corners and Edges I* and 3.18.3-2 *Corners and Edges II*.

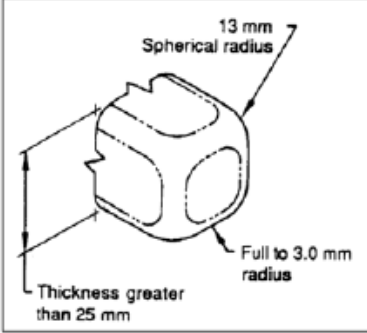
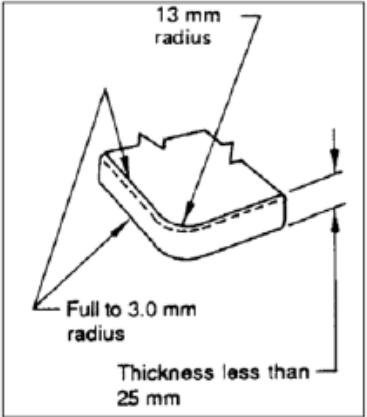
Rationale: Payloads in IVA accessible areas must be designed to preclude sharp edges and protrusions or must be covered in such a manner as to protect the crew and critical support equipment.

TABLE 3.18.3-1 CORNERS AND EDGES I

Material Thickness (t)	Minimum Corner Radius	Minimum Edge Radius	Figure
3.0 mm < t ≤ 6.5 mm (0.125 in < t ≤ 0.25 in)	6.5 mm (0.26 in)	1.5 mm (0.06 in)	
0.5 mm < t ≤ 3.0 mm (0.02 in < t ≤ 0.125 in)	6.5 mm (0.26 in)	Full radius	
t < 0.5 mm (t < 0.02 in)	6.5 mm (0.26 in)	Rolled, curled, or covered to 3.0 mm (0.120 in)	

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 77 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE 3.18.3-2 CORNERS AND EDGES II

Material Thickness (t)	Minimum Corner Radius	Minimum Edge Radius	Figure
$t > 25 \text{ mm}$ ($t > 1 \text{ in}$)	13 mm (0.5 in (spherical))	3.0 mm (0.120 in)	
$6.5 \text{ mm} < t \leq 25 \text{ mm}$ ($0.25 \text{ in} < t \leq 1 \text{ in}$)	13 mm (0.5 in)	3.0 mm (0.125 in)	

M2M-SMA-UTIL-R-2082 IVA Levers, Cranks, Hooks, and Controls

The payload shall locate levers, cranks, hooks, and controls where they cannot pinch, snag, cut, abrade, or provide kickback to the crewmember appendages or equipment such as tethers.

Rationale: Levers, cranks, hooks, and controls can generate snag/safety hazards that may pose a threat to IVA crewmembers.

M2M-SMA-UTIL-R-2083 IVA Use of Safety Wire

For payloads utilizing safety wire (lock wire) the IVA crew shall be protected from the cut end.

Rationale: The use of safety wire is prohibited, for fasteners that could be manipulated on orbit including maintenance and contingency operations.

M2M-SMA-UTIL-R-2084 Clearance for Entrapment Hazard

Payloads shall be designed to protect the crew from entrapment (tangles, snags, catches, etc.).

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 78 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: This applies to items with which the crew will come into direct contact. Entrapment can occur in places where loose cables or equipment items block passageways. Entrapment can also occur from protrusions or openings that snag body parts or personal equipment.

For example, if holes are small, then fingers may be entrapped. Larger holes, on the other hand, allow free movement. Crewmembers are likely to be under time-critical conditions when they need to evacuate or return to safety.

M2M-SMA-UTIL-R-2085 Sharp Item Hazard

Payload functionally sharp items shall be prevented from causing injury to the crew or damage to equipment when not in use.

Rationale: "Functionally sharp" payload items are those that, by their function, do not meet the requirement for exposed corners and edges (i.e., syringe, scissors, knife). These items must be prevented from causing harm when not in nominal use. Capping sharp items is one way of doing this.

M2M-SMA-UTIL-R-2086 Burrs

Exposed payload surfaces shall be free of burrs.

Rationale: Removal of burrs can help to prevent personnel injury and damage to protective equipment from sharp edges during normal operations.

M2M-SMA-UTIL-R-2087 Pinch Points

Payload shall prevent pinch points from injuring the crew.

Rationale: Pinch points can cause injury to the crew but may exist for the nominal function of equipment (i.e., equipment panels). This may be avoided by locating pinch points out of the reach of the crew or providing guards to eliminate the potential to cause injury.

M2M-SMA-UTIL-R-2088 Holes

Payload with round or slotted holes that are uncovered shall be less than 1.02 cm (0.4 in) or greater than 3.56 cm (1.4 in) in minimum dimension for equipment located inside habitable volumes.

Rationale: This requirement addresses entrapment hazards associated with IVA crewmembers who are required to work with IVA payloads.

3.18.4 IVA CREW LIFTING AND HANDLING HAZARDS

IVA handling is based on the EVA constraints and lunar gravity that set the upper limits. This limits the need for extra safety controls associated with multiple environments and physical constraints.

A payload handled in the IVA environment (shirt sleeve environment) is assumed to be brought outside during an EVA. Handling of these payloads is addressed in Section 3.19 *Extravehicular Activity (EVA)*.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 79 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.18.5 PAYLOAD CONNECTOR AND INSTALLATION HAZARDS

M2M-SMA-UTIL-R-2089 Payload Connector Actuation without Tools

Payload connectors shall be operable without tools for mating and demating while wearing the most encumbering equipment and clothing anticipated.

Rationale: Connector actuation includes mating/connecting and demating/disconnecting of a connection. Lost or damaged tools prevent connectors from being connected or disconnected, which may result in Loss of Crew (LOC) or Loss of Mission (LOM).

M2M-SMA-UTIL-R-2090 Incorrect Payload Mating, Demating Prevention

Payload cable, gas and fluid lines, and electrical umbilical connectors shall prevent potential mismating and damage associated with mating or demating tasks.

Rationale: The preferred method of preventing improper installation and mating is a design that prevents it such as misaligned mounting holes, pins, or keys. The designs to prevent installation and mating errors are to be rugged enough to withstand persistent attempts. Cues (such as color or labeling) can be provided to remind crewmembers, so they save the time of trying to make improper installations. However, these cues are not to be the sole countermeasure to improper installation and mating.

M2M-SMA-UTIL-R-2091 Incorrect Payload Installation

The payload shall be designed so that it cannot be mounted or installed improperly.

Rationale: Payload tasks including installation/removal of equipment are not likely to be familiar. The preferred method of preventing improper installation and mating is a design that prevents it, such as misaligned mounting holes, pins, or keys. They can make payload tasks easier and lessen the likelihood of human error thereby help avoid associated hazards, decrease the risk of LOC, LOM and/or damage to hardware.

Consideration should be made to allow keys to be removed or items to be interchangeable if this would increase operational flexibility or contingency response options without causing hazards. The designs to prevent installation and mating errors are to be rugged enough to withstand persistent attempts. Cues (such as color or labeling) can be provided to remind crewmembers, so they save the time of trying to make improper installations. However, these cues are not to be the sole countermeasure to improper installation and mating.

M2M-SMA-UTIL-R-2092 Crew Hazards Related to Electrical Shock

Payload designs shall comply with the requirements in Table 3.18.5-1-3 to control electrical hazards to the crew.

Rationale: Protection of Crew. Reference NASA-STD-3001V2, 9.3.3.3 and 9.3.3.4.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 80 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

TABLE 3.18.5-1-3 CREW SAFETY ELECTRICAL CURRENT LIMITS

Activity	Current Limit	NASA-STD-3001 Reference
Nominal Situations, (routine human contacts to conductive housing)	Electrical current through the crewmember to $\leq$ (less than or equal to) 0.4 mA for Direct Current (DC) and $\leq$ (less than or equal to) 0.2 mA peak for Alternating Current (AC)	9.3.3.3 Nominal Physiological Electrical Current Limits
To avoid catastrophic physiological effects to the crewmember	Limit the electrical current through the crewmember to $\leq$ (less than or equal to) 40mA for DC and $\leq$ (less than or equal to) 8 mA peak for AC	9.3.3.4.1 Catastrophic Physiological Electrical Current Limits for all Circumstances
During critical operations where a startle reaction is possible	Limit electrical current through the crewmember to $\leq$ (less than or equal to) 2 mA for DC and $\leq$ (less than or equal to) 0.5 mA for AC to avoid potentially catastrophic conditions.	9.3.3.4.2 Catastrophic Physiological Electrical Current Limits for Startle Reaction

NOTE: Biomedical instrumentation for M2M application in oxygen rich environments are in development.

< FWD-30043-002>

3.18.6 LASERS AND BROADBAND LIGHT

Crew exposure to high-intensity laser and/or broadband light emissions could result in biological damage to the eye or skin. Sustained damage to the eye could lead to crew incapacitation or blindness. Skin tissue destruction can also occur. Hazards from crew exposure to high-intensity laser and/or broadband light emissions are controlled by making the source inaccessible to the crew (e.g., containment of the source) or by providing the appropriate number of controls to prevent exposure (e.g., power inhibits) based on hazard severity.

M2M-SMA-UTIL-R-2093 Lasers - General

Payload lasers shall be designed and controlled in accordance with ANSI Z-136.1, American National Standard for Safe Use of Lasers.

Rationale: This requirement is applicable for all payloads with lasers.

The ANSI standard provides for the safe use of lasers and laser systems by providing classifications according to their relative hazards and then specifying appropriate controls. The basis of the hazard classification is the ability of the laser beam to cause biological damage to the eye or skin during use. This standard is used to protect the crew as well as ground-based general public with and without optical aid consideration. The ANSI standard also provides the Maximum Permissible Exposure (MPE) for each classification. Use of ANSI Z-136.1 2007 or newer is acceptable and should be specified when providing data to the NASA SME, the JSC/Non-Ionizing Radiation (NIR) Group.

Payload laser classification should be done based on vendor-provider data or through testing of the laser at the source. Any modifications made to a COTS laser (i.e., change in use or power input/output, etc.) should be assessed to confirm there is no change in the laser output at the source as this may change the laser classification. Testing of the maximum output (based on max power or energy to the laser with no inhibits) may be needed to confirm there is no change in the laser classification.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 81 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Fully contained lasers are acceptable with no additional controls under the general laser requirement. If access to a contained laser is possible, safety interlocks or other controls should be provided.

Class 1 and 2 lasers are considered to be safe without containment or eye protection. Class 1 lasers are considered to be incapable of producing damaging radiation levels during operation. Class 2 lasers emit in the visible portion of the spectrum and eye protection is afforded by the eye aversion response.

Class 1M, 2M and higher lasers are not safe when magnified; therefore, they require an ocular hazard assessment to address the potential for viewing with optical equipment (cameras, binoculars, etc.).

Class 3R, 3B and 4 are considered catastrophic and require full containment and two failure tolerant controls against crew exposure.

For lasers operating in free-space, additional guidance can be obtained from ANSI Z-136.2 (2012), Safe Use of Optical Fiber Communication Systems Utilizing Laser Diode and LED Sources, and ANSI Z-136.6 (2015), Safe Use of Lasers Outdoors, as referenced in ANSI Z-136.1. These references are not specific to spaceflight so additional information and guidance would be needed from the NASA SME to apply these to spaceflight.

M2M-SMA-UTIL-R-2094 Magnification of Lasers

For exposed payload lasers of Class 1M, 2M and above, exposure resulting from magnification by optical equipment shall be below the MPE.

Rationale: Class 1M and 2M and higher lasers are potentially hazardous if viewed with certain optical aids. An ocular hazard assessment ensures optical magnification by equipment on board M2M Elements (cameras, binoculars, etc.) that could be used to view a laser source, or its specular reflection does not result in exposure above the MPE. Information on worst case Gateway optical equipment can be obtained from the JSC/NIR Group. Additional controls, such as operational controls, are required to prevent viewing a laser with optical magnification equipment if the analysis shows exposure would be above the MPE. (e.g., a flight rule preventing use of certain optical equipment during certain operational times, such as docking).

M2M-SMA-UTIL-R-2095 Class 3R, 3B, and 4 Lasers

Class 3R, 3B or 4 payload lasers shall be inaccessible to the crew or provided with three controls to prevent exposure and damage to external systems.

Rationale: Class 3R, 3B, or 4 lasers can be hazardous to the eye or skin from direct beam or specular reflection viewing conditions. Class 4 lasers could also pose a diffuse reflection or fire hazard. Crew exposure to Class 3R, 3B, or 4 lasers is considered a catastrophic hazard, so the design is required to provide two failure tolerance to prevent exposure.

Payloads with Class 4 lasers that are relying on containment need to assess and ensure it can't cause structural damage. If access to a contained laser is possible, safety interlocks or other controls should be provided. Other controls could include filters, laser only points away from Lunar Exploration System or Vehicle, laser turned off during EVA, etc.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 82 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2096 Payload Provided Lighting

The lighting illumination level provided by the payload shall permit planned crew activities without injury.

Rationale: In most cases the habitable environment should provide the illumination levels necessary for safe crew to payload operations, but payloads should verify this is the case for all M2M Element where crew to payload interaction is planned.

M2M-SMA-UTIL-R-2097 Infrared Radiation (IR) Light Exposure from Payloads

Payload infrared light sources shall be controlled to prevent crew exposure that exceeds the Threshold Limit Values (TLV) as calculated per American Conference of Governmental Industrial Hygienists (ACGIH) *Documentation of the Threshold Limit values for Chemical Substances and Physical Agents & Biological Exposure Indices* (2023 or newer).

Rationale: This requirement is intended to prevent ocular injury and skin damage caused by overexposure to infrared radiation (IR) from artificial sources. The payload should prevent exposure through controls or containment. Infrared radiation (IR) sources are not necessarily required to be contained at the source but should be obstructed by applicable means (e.g., shields, filters) before reaching the crew.

M2M-SMA-UTIL-R-2098 Ultraviolet (UV) Radiation Light Exposure from Payloads

Payload ultraviolet light sources shall be contained.

Rationale: This requirement is intended to prevent ocular injury and skin damage caused by overexposure to UV radiation from artificial sources.

3.18.7 EMERGENCY RESPONSE

In an emergency situation, the crew must be able to remove themselves from any payload apparatus, migrate via the translation paths and isolate volumes, if required, in a timely manner.

M2M-SMA-UTIL-R-2099 Egress from Payload Apparatus

The design shall enable crew egress from payload apparatus in less than 30 seconds.

Rationale: The crew must be able to free themselves from any apparatus such that they can evacuate/relocate if necessary. Thirty seconds is based on engineering judgment and is meant to represent expedited egress in the event of emergencies. This 30 second timeframe is a subcomponent of the overall three minute time to isolate a volume by closing a hatch. Margin is already accounted for in the overall egress scenario, so no safety factor needs to be added to account for microgravity conditions.

If the crew can evacuate by detaching themselves rather than complete removal of the apparatus (e.g., exercise equipment harness), that is acceptable as long as it does not impede their ability to don emergency breathing apparatus and/or emergency entry suits.

M2M-SMA-UTIL-R-2100 Intramodule Emergency Egress

The payload design shall not impede emergency IVA egress to contiguous pressurized volumes.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 83 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: A minimum emergency translation corridor is maintained within M2M modules. The minimum emergency corridor allows for a crewmember to reverse direction at any point along the corridor during emergency situations. Temporary intrusions or items that can be quickly relocated or reconfigured will be assessed by the appropriate safety review panel on a case by case basis. Payload rotation due to maintenance and payload rack translation are acceptable protrusions into the emergency translation corridor. Cables, hoses, and wires in the translation corridor must be restrained to prevent entanglement during emergency egress. Desktop analysis/engineering judgment is typically adequate to satisfy this requirement for individual payload items. If the safety panel determines the hardware has potential to impact the translation path, the payload will be included in the integrated assessment performed by the Program internal volume configuration teams.

M2M-SMA-UTIL-R-2101 Hatch Drag-Throughs

Utilization payload design and installation shall preclude the presence of drag-throughs in hatchways.

Rationale: Cables, lines, hoses, and ducts, in addition to anything which could pose interference with hatch closure, are considered drag-throughs. Any proposed drag through, including portable equipment, must be approved by the applicable Program(s).

3.19 EXTRAVEHICULAR ACTIVITY (EVA)

Regardless of whether EVAs are planned, contingency, or not required by a payload, all hardware in EVA accessible areas must be compliant with these EVA safety requirements. Only the appropriate safety review panel supported by EHP Requirements, Interfaces, Verification Analysis (RIVA) Panel can determine if a payload is outside EVA accessible areas. If that determination is made, no assessment for EVA is required. Any agreed to EVA task used to satisfy the failure tolerance criteria can be used only as a third level of control to safe a payload if the appropriate safety review panel approves. The EVA task must also be negotiated by the operations team.

Generic EVA hazards are those introduced by being exposed to the EVA environment i.e., hazards independent of what is to be performed while EVA. Operational hazards (e.g., fatigue, tether management, distance from airlock) are those relating to the specific EVA operation to be performed. The requirements listed here address the generic hazards. Hazards related to EVA should be captured on the UHR. The EVA operations community ensures the operational hazards are addressed during the planning phase for each specific EVA. However, if failure to meet these loads creates a hazard to the EVA crew or to spacecraft, the failed load requirement(s) are dealt with as safety requirements and address in Hazard Reports and/or waivers.

The authority document on EVA Compatibility Standards is EHP-10028, *Exploration EVA System Compatibility Standards*. This document contains all requirements and associated rationale for EVA suit compatibility with any hardware. The EVA compatibility requirements that are applicable to payload safety are listed in Table 3.19-1 with explanatory information and a pointer reference to the associated EHP-10028 requirements numbers.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 84 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2102 EVA Payload Safety Requirements

The Payload shall be designed and comply with the requirements in Table 3.19-1, containing applicable EVA safety requirements from EHP-10028, *Exploration EVA System Compatibility Standards*. <FWD-30043-012>

Rationale: To reduce potential errors associated with duplication of requirements a pointer is provided to the applicable EVA requirements document. The assigned Payload Integration Manager (PIM) will aid the payload project to ensure the latest requirements are communicated to the project.

TABLE 3.19-1 EVA PAYLOAD SAFETY REQUIREMENTS

EVA Safety Topic	Description	EHP 10028 Requirement	Title
EVA Temperature Extremes	The spacesuit is protected from damage caused by high and low temperature extremes based on the following requirements. A burn through of spacesuit material can result in a loss of breathable atmosphere and potential loss of crew. All external hardware in an EVA accessible area must meet the incidental contact requirement. Incidental contact is considered brush and bump contact of up to 30 seconds at 0.1 psi or 3 seconds at 1 psi.	EVASC.0104	Incidental Contact
		EVASC.0104	Unlimited Contact
External Corner and Edge	The spacesuit must be protected from cuts, tears and snags by adhering to the following requirements. These requirements apply to any protrusion, burr, or exposed sharp edge that has the potential to cut an EVA glove or puncture the spacesuit. All hardware in EVA accessible areas must meet these requirements	EVASC.0105	Sharp Edges and Protrusions
		EVASC.0105	EVA Burrs
Equipment Clearance for Entrapment Hazard	Clearance for equipment removal and replacement are necessary to prevent the creation of a crew entrapment hazard. Entrapment hazards are caused by insufficient clearance, either statically or during movement or rotation of a	EVASC.0109	EVA Holes or Slots
		EVASC.0107	Levers, Cranks, Hooks, and Controls
		EVASC.0069	Use of Safety Wire

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 85 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

EVA Safety Topic	Description	EHP 10028 Requirement	Title
	hardware payload, that results in not meeting any or all of the following requirement: A. EVA Holes (entrapment of crew fingers) B. Gloved Operation (entrapment of crew hand) C. Translation Paths (entrapment of crew body)	EVASC.0003	Gloved Operation
		EVASC.0008	Translation Paths
		EVASC.0110	Pinch Points
		EVASC.0112	Crew Protection from Moving or Rotating Equipment
		EVASC.0132	Uncontrolled Motion of Flex Hoses
		EVASC.0137	Entanglement
		EVASC.0100	Component Hazardous Energy – Stored Energy
		EVASC.0121	Magnetic Field Limits for EVA Payloads
		EVASC.0092	EVA Hazardous Material Control
		EVASC.0096	Payload Laser Safety for EVA Applications
		EVASC.0047	EVA Payload Visual Contrast
Payload EVA Handling	Payload handling needs to consider ground, IVA, and EVA handling. This section addresses the EVA handling and associated spacesuit considerations	EVASC.0160	Lunar Gravity EVA Handling Capability

3.20 GRAPHICAL USER INTERFACE (GUI)

To ensure crew safety for payloads with simple displays a list of the minimum Graphical User Interface (GUI) requirements is provided below. M2M 30040, *M2M Graphical User Interface (GUI) Standard* <FWD-30043-007> contains the detailed GUI requirements and is to be used for payloads that have more detailed crew displays. The list below reproduces the requirements in M2M 30040 based on M2M 30040 Appendix D, *Payload Mapping Matrix* and denoted as:

- Applicable as “Shall” (Safety Critical)
- Applicable as “Shall” for Hazardous Controls

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 86 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2103 Interpretation of Payload Display Information

Payload display information shall be presented in a directly usable form that does not require mental transposition or computation by the operator. [M2M 30040, 3.1.e]

Rationale: Because human cognitive capabilities are limited, overtaxing operators in extreme environments can lead to errors. Information should be presented in the most easily digestible form possible. It should be pre-processed, pre-calculated, and correctly formatted so that perception and understanding can be achieved as quickly as possible. This leaves more cognitive resources available for critical tasks such as monitoring and problem solving.

M2M-SMA-UTIL-R-2104 Maximum System Response Time to Crew Input

The system shall provide feedback to the crew input in accordance with the system response times in Table 3.20.1-1: Maximum System Response Time to Crew Input. [M2M 30040, 3.1.j]

TABLE 3.20.1-1 MAXIMUM SYSTEM RESPONSE TIME TO CREW INPUT

System Response	Example	Maximum Time (s)
Continuous input: cursor and onscreen dynamic elements	Cursor and symbol motion	0.07 (15 Hz)**
Discrete input: Indication of a visual, auditory, or tactile discrete input	Onscreen keystroke echo; click or beep; detent/physical feedback	0.1
Update to local element	Display of popup menu	0.5
Display of a requested GUI	Calling up a new display or display component	1.0
Display of updated data on crew command of a state change	Status of "on" when commanded on; status of "open" when commanded open	1.0
Feedback for commands that cannot be completed within 1 second: 1. Indication that a command or process is in progress 2. Status of the command/process after request completed	1. A progress bar showing time remaining or a progress message.	1.0
	2. After request is completed - status message of success/fail/unknown	1.0

**Note: Data update rates are not currently addressed and are usually reflected in each programs higher level System Requirements Document (SRD). However, <FWD-50040-010> addresses the need to address this concern since there is not currently an M2M level SRD.

M2M-SMA-UTIL-R-2105 Violation of Operational Limit

The capability to show the violation of any operational limit or telemetry threshold of a GUI element shall be provided. [M2M 30040, 3.3.1.b]

Rationale: Operators need to know when an operational limit or telemetry threshold has been exceeded so that they can understand the system state and know where to begin troubleshooting. Data quality indicators (e.g., yellow/red up or down arrows to indicate an alert threshold has been reached) or fields that contain status text (e.g., "High" or "Low" to indicate a temperature threshold has been reached) provide information about potential sources of problems in the system.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 87 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2106 Stale Data Indication

There shall be an indication when data are stale. [M2M 30040, 3.3.1.c]

Rationale: Feedback that data are stale or missing is important for the crew's accurate assessment of data during troubleshooting and decision-making periods. Typically, "m"s are used across the Artemis displays to indicate a missing data element.

M2M-SMA-UTIL-R-2107 Telemetry Outside Upper or Lower Thresholds

A yellow or red up or down arrow following a telemetry value shall be used to indicate that telemetry is outside of upper or lower thresholds that trigger a Caution or Warning alarm. [M2M 30040, 3.3.1.e]

Rationale: The ability to view the pattern of out-of-threshold telemetry values in a system summary display provides more troubleshooting information than an alert message alone. If necessary, a black arrow on a yellow background or a white arrow on a red background may be substituted to achieve contrast or draw extra attention.

M2M-SMA-UTIL-R-2108 Off Scale Indication

The system shall provide indication that a telemetry value is offscale high or low when that information is necessary to address a malfunction. [M2M 30040, 3.3.1.f]

Rationale: Off-scale high or low values in telemetry can indicate a sensor problem and can signal an issue that may or may not be serious. When an offscale value is needed to address a malfunction, the system is to provide an indicator next to the value (e.g., "H" for high and "L" for low.).

M2M-SMA-UTIL-R-2109 Sufficient Fixed Placeholder Width

Telemetry fields shall have sufficient fixed placeholder width to show the longest possible value, including the size of any data quality indicators. [M2M 30040, 3.3.1.g]

Rationale: Telemetry values can vary in length, and can have associated data quality indicators (e.g., yellow/red up or down arrows to indicate a caution/warning threshold has been reached). The ability to view complete, non-truncated information is important for context, and for making informed decisions.

M2M-SMA-UTIL-R-2110 Text Data Overflow Indicator

When text data overflow occurs, each character of the entire field shall be replaced by yellow asterisks. [M2M 30040, 3.3.1.h]

Rationale: Providing a visual indication that a text data field overflow has occurred helps operators understand the value is larger than the system can display. This prevents them from using the values when making decisions, which can reduce errors. Yellow asterisks are typically used across the Artemis displays to indicate an overflow has occurred.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 88 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2111 Numeric Data Overflow Indicator

When numeric data overflow occurs, each character of the entire field shall be replaced by yellow asterisks, except for the signed field and the decimal point. [M2M 30040, 3.3.1.i]

Rationale: Providing a visual indication that a numeric data field overflow has occurred helps operators understand the value is larger than the system can display. This prevents them from using the values when making decisions, which can reduce errors. Yellow asterisks are typically used across the Artemis displays to indicate an overflow has occurred.

M2M-SMA-UTIL-R-2112 Critical Data Update Rate

Data values that the user must reliably and accurately read shall be updated no more often than 1 Hertz. [M2M 30040, 3.3.1.j]

Rationale: To ensure crew safety and to prevent incorrect response actions.

M2M-SMA-UTIL-R-2113 Distinguishable Payload Commands

Payload display command names for different commands shall be distinguishable from one another. [M2M 30040, 3.3.2.g]

Rationale: When command names are similar, there is a higher risk of selecting the wrong command, which could result in unsafe operations. Using distinct command names can help operators distinguish between and send intended commands.

M2M-SMA-UTIL-R-2114 Hazardous Payload Commands

Commands that are irreversible or hazardous should include a black and yellow diagonally striped border (i.e., hazard tape). [M2M 30040, 3.3.2.i]

Rationale: Striped borders around hazardous controls have been used in aircraft and other safety-critical machinery for decades. The crosshatch pattern catches the eye, causes a visual pause, and reminds operators that this control is to be approached with caution. Sparingly used striped borders around hazardous commands serve the same purpose in vehicle/habitat displays.

M2M-SMA-UTIL-R-2115 Payload Display of Status and Error Messages

Payload display status and error messages shall be displayed in a consistent, designated location. [M2M 30040, 3.3.3.a]

Rationale: A consistent, designated location for status and error messages makes the location predictable and reduces the need to visually scan and search for the message.

M2M-SMA-UTIL-R-2116 Payload Display Character Height

Character height shall be a minimum of 0.25 deg, with 0.4 deg or greater preferred. (Note that Font height in degrees refers to the angle subtended at the eye by the height of an upper-case letter in the font. For example: 0.25 deg is 10-point type at 32 in). [M2M 30040, 3.4.1.g]

Rationale: Text size needs to be large enough for operators to accurately read under expected spaceflight conditions. Font height in degrees refers to the angle subtended at the eye by the

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 89 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

height of an uppercase letter in the font. For example: 0.25 deg is 10-point type at 32 inches viewing distance. The font may need to be larger when taking into account flight and crew conditions. For more information about calculating/selecting font size, refer to the Human Integration Design Handbook (NASA/SP-2010-3407).

M2M-SMA-UTIL-R-2117 Payload Display Numeric Value

Units of measure shall be displayed for each numeric value or for each group of numeric values where the units are the same. [M2M 30040, 3.4.6.b]

Rationale: To ensure crew safety and to prevent incorrect response actions.

M2M-SMA-UTIL-R-2118 Payload Display Off-nominal Values

When it is important to identify out-of-range or off-nominal values, they shall be highlighted (e.g., via color and a numeric/text indicator, or limit line). [M2M 30040, 3.4.8.f]

Rationale: When a graph is provided to monitor data values, a threshold indicator (e.g., color, line, symbol) provides a way to quickly and easily identify data values that are out-of-range or off-nominal.

M2M-SMA-UTIL-R-2119 Payload Display Use of Color

The meanings in Table 3.20.1-2 shall be represented with the colors shown. [M2M 30040, 3.4.10.b]

TABLE 3.20.1-2 PAYLOAD DISPLAY COLORS

Meaning	Color
Highest alert level, emergency, warning, failed	Red
Second highest level, caution, off-nominal, trip, manual override, or attention required	Yellow
Advisory	Blue
Unavailable, unselectable	Gray
Missing or stale data	Cyan

M2M-SMA-UTIL-R-2120 Payload Graph Display - Off-Nominal Data

For critical information and critical tasks when color is used to convey meaning, the system shall provide an additional cue. [M2M 30040, 3.4.10.e]

Rationale: To ensure crew safety and to prevent incorrect response actions

M2M-SMA-UTIL-R-2121 Termination of Flashing

The GUI shall allow termination of flashing that persists more than 10 seconds. [M2M 30040, 3.4.11.e]

Rationale: To ensure crew safety and to prevent incorrect response actions.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 90 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.21 MICROMETEOROID AND ORBITAL DEBRIS

Meteoroids occur naturally in space and usually originate from comets or asteroids. Orbital debris is manmade materials that remain in orbit around the earth. Both types of objects travel at extremely high velocities and pose a risk to all externally mounted spacecraft. Hardware items, such as pressure vessels, cryogenic carriers, and other stored energy devices require Micrometeoroid and Orbital Debris (MMOD) protection since they could create a catastrophic hazard if impacted or penetrated by a meteoroid or orbital debris particle. Other resulting hazards of MMOD strikes can include fluid leakage, glass fragments, or other debris.

M2M-SMA-UTIL-R-2122 Micrometeoroid and Orbital Debris (MMOD)

Payloads with the potential to create a catastrophic hazard if impacted or punctured by MMOD shall be designed in accordance with NPR 8715.6, *NASA Procedural Requirements for Limiting Orbital Debris and Evaluating the Meteoroid and Orbital Debris Environments* with an assessed Probability of No Penetration (PNP) to be $\geq$ required minimum PNP (the lesser of 0.9999 or $0.99999(A*Y)$).

Where A = Total hazardous impact surface area of the payload or cargo/crew vehicle in square meters (surface area should not include elements of the payload that do not represent catastrophic hazard to crew or station survivability if failed due to impact such as radiators and solar arrays), while Y = Exposure time in years.

Rationale: MMOD strikes to externally mounted payloads with catastrophic hazard potential can result in loss of an M2M Element or endanger the flight crew.

*Shielding is one method of reducing the risk. The Assessed PNP of the shielding must be equal or greater than the required minimum PNP that is determined from the lesser value of 0.9999 or $0.99999(A*Y)$. The assessed PNP must be calculated for the cumulative on-orbit exposure time of the payload beginning with the initial launch date. The required minimum PNP parameter $A =$ Total hazardous impact surface area in square meters while $Y =$ Exposure time in years.*

For the purposes of MMOD, a penetration is defined as damage/failure to stored energy devices that causes a hazard to crew or vehicle survivability. Typically, penetration is defined as a partial or complete perforation of the pressure vessel or casing, detached spall from the pressure vessel wall, damage to the pressure vessel that would allow unstable crack growth, or deformation of a casing of rotating machinery such that the deformation could intrude into the dynamic envelope of the rotating device.

M2M-SMA-UTIL-R-2123 Payloads Limiting Orbital Debris

Payloads that have the potential to create orbital debris (e.g., external payloads) shall comply with NASA-STD-8719.14, *Process for Limiting Orbital Debris*.

Rationale: Payloads that have the potential to create orbital debris, a safety hazard to M2M spacecraft adhere to the processes and requirements in NASA-STD-8719.14 to limit orbital debris.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 91 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.22 PROPULSION

Cross-program utilization payloads requirements for payloads with propulsion systems is forward work. <FWD-30043-008> The launch vehicle providers are a good starting point until this section is updated as payloads with propulsion systems will have to also meet requirements imposed by the launch vehicle.

3.23 PYROTECHNIC SYSTEMS

Pyrotechnic systems (explosive-loaded and explosively-actuated, non-loaded devices) can create a hazard due to failure to fire and/or inadvertent firing, including explosion debris and collision of released materials with M2M systems. Hazard causes associated with ground processing, natural and induced environments, hardware/software failure modes, and operator error must be considered.

Malfunction and inadvertent operation of control circuits caused by extremes of ground and flight environments must be avoided by protective design features.

All pyrotechnic device safety requirements for must work applications, inadvertent actuation, electrical, and containment are stated in the following paragraphs.

M2M-SMA-UTIL-R-2124 Pyrotechnics

Electro explosive payload systems and payload firing circuits associated with pyrotechnic functions shall comply with the requirements in JSC 62809, *Human Rated Spacecraft Pyrotechnic Specification*."

Rationale: Vehicle and crew protection from the sudden release of energy from a pyrotechnic device.

M2M-SMA-UTIL-R-2125 Pyrotechnic Loss of Function (Must Work)

If failure to function is catastrophic, the design of the pyrotechnic subsystem shall be in accordance with JSC 62809, *Human Rated Spacecraft Pyrotechnic Specification*.

Rationale: Where failure to operate causes a catastrophic hazard, pyrotechnic operated devices are designed, controlled, inspected, and certified to criteria equivalent to those specified in JSC 62809. Payload hardware provider should consult the NASA JSC Pyrotechnics Office for guidance as early as possible.

M2M-SMA-UTIL-R-2126 Pyrotechnic Inadvertent Function

If inadvertent actuation is catastrophic to crew, vehicle, or mission, the design of the pyrotechnic subsystem shall be in accordance with JSC 62809, *Human Rated Spacecraft Pyrotechnic Specification*.

Rationale: Inhibits should be in place to prevent inadvertent pyrotechnic activation. Payload hardware provider should consult the NASA JSC Pyrotechnics Office for guidance as early as possible.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 92 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-2127 Electrical Explosive Devices

Electrical Explosive Devices (EEDs) shall meet the requirements of JSC 62809, *Human Rated Spacecraft Pyrotechnic Specification*.

Rationale: There are many cross over requirements between [AIAA S-113A](#)-2016, Criteria for Explosive Systems and Devices on Space and Launch Vehicle and JSC 62809, and these two documents are very similar, with the caveat that AIAA S-113A states that modifications and addition (e.g. for manned spaceflight) may be necessary. The JSC Pyro Office typically views these 2 documents to be similar with JSC 62809 providing enhanced quality and lot control requirements for human spaceflight. In one instance (Gateway program), AIAA S-113A-2016 was included as heritage industry components may have been developed to AIAA S-113 and the program wanted to enable the greatest use of heritage devices available.

M2M-SMA-UTIL-R-2128 Pyrotechnic Mechanical Containment

Pyrotechnic devices shall be designed to contain the effects of shock, debris, and hot gasses resulting from operation in accordance with JSC 62809, *Human Rated Spacecraft Pyrotechnic Specification*.

Rationale: This pyrotechnic containment section covers requirements for debris containment from pyrotechnics use, including design, development, and qualification.

Tensile test data is necessary for component parts that are heat treated after receiving from the mill. Tensile test data is also necessary for component parts that have to withstand operating pressures or primary structural loads or both.

A minimum of three standard tensile coupons, in accordance with ASTM E8, Standard Test Methods of Tension Testing of Metallic Materials, are processed with the component parts. Before acceptance, the supplier conducts tensile tests on each coupon as defined by the procuring agency, or if no specific direction is provided, tensile testing is too completed in accordance with ASTM E8.

As a minimum, ultimate strength, 0.2 percent offset yield, and elongation data is obtained from the test coupons and recorded on the lot acceptance data sheets. Failure to meet the minimum material tensile acceptance criteria causes rejection of the component parts associated with those test coupons.

For pyrotechnic device metallic component parts that are not heat treated after machining and are not exposed to operating pressures or primary structural loads, the standard mechanical properties test report delivered with the raw material will suffice, provided all test data required by the material specification are included in the report.

All threaded parts are positively locked. Liquid locking compounds may be used provided the implementation meets the following restrictions:

- *Liquid locking compounds are not to be used as secondary locking features on safety critical fasteners.*

For the purposes of this requirement, safety critical fasteners are defined as:

- *All primary or secondary structural fasteners used in the exterior and interior of flight modules.*

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 93 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

- *All non-structural fasteners used exterior to flight modules, which could pose a FOD risk to vehicle operations and which have not been vibration tested during qualification or acceptance of the hardware.*

Where applicable, locked-shut capability is to be demonstrated with redundant charges operating simultaneously. This demonstration is not applicable to premature initiation failure modes. Demonstration of this capability is not necessary if the release of shrapnel, debris, or hot gasses does not jeopardize crew safety or mission success as verified by analysis using credible failure modes.

The design yield FOS and ultimate FOS of 1.4 are not applicable to the loads generated by the firing of the pyrotechnic charge.

For pyrotechnic devices that are criticality 3 (do not pose a catastrophic hazard to crew or vehicle), an analysis to 1.5 times the maximum operating pressure may be substituted provided it includes 100 percent NDE. The maximum operating pressure is defined as the highest measured operating pressure from a minimum of five firings using nominal cartridge load. If the cartridge design, propellant or application make direct pressure measurements impractical or if a measured transient pressure spike establishes an unrealistic proof pressure requirement, an analytically derived proof pressure requirement may be established.

M2M-SMA-UTIL-R-2129 Transportation of Payloads with Pyrotechnics

Payloads with pyrotechnic devices that are stowed, stored, transported or otherwise within MPCV shall have 3 monitored inhibits. Payloads without a power source do not require monitoring.

Rationale: Payloads with pyrotechnic devices are prohibited from operating within the MPCV habitable volume. Monitoring of inhibits provides confirmation the controls preventing activation of pyrotechnics are in place. Payloads that do not have a power source are not required to provide monitoring of inhibits. [Reference: MPCV requirement MPCV.PLDSAF.033] <TBD-30043-003>

3.24 PLANETARY PROTECTION

M2M-SMA-UTIL-R-2130 Cross-Program Utilization Payload Planetary Protection

Cross-program utilization payloads transported to the lunar surface shall provide a listing of organic and biological materials transported to the lunar surface.

Rationale: Guidance on the planetary protection requirements is provided in NASA-STD-8719.27, Implementing Planetary Protection Requirements for Space Flight. HLS-PLAN-013, HLS Planetary Protection Plan provides the requirements for payloads HLS transports to the Lunar surface.

M2M-SMA-UTIL-R-2131 Cross-Program Utilization Payload Lunar Surface Disposal

Category IIa & IIb Cross-program utilization payloads to the Moon shall report an inventory of volatile organic materials, propellant residuals and combustion products that remain or have

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 94 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

been released into the lunar environment by the propulsion, attitude control and other payload systems in the End of Mission PP Report.

Rationale: Guidance on the planetary protection requirements is provided in NASA-STD-8719.27, Implementing Planetary Protection Requirements for Space Flight. HLS-PLAN-013, HLS Planetary Protection Plan provides the requirements for payloads HLS transports to the Lunar surface.

3.25 SAMPLE RETURN

M2M-SMA-UTIL-R-2132 Sample Return Requirements

Samples that will be returned to Earth shall be packaged to meet M2M natural and induced loads.

Rationale: Returning samples must be packaged in a way that they do not damage HLS, Orion, Gateway, or Pressurized Rover or injuring flight crew or ground crew. In addition, the samples must be packaged such that the internal stratigraphy/integrity is preserved, to benefit curation activities.

3.26 GROUND SAFETY

The interaction of payload, launch site facilities, and ground personnel must tolerate a minimum number of credible failures and/or operator errors to prevent injury to personnel and damage to launch facilities and spacecraft. Each payload processing facility and launch facility has specific safety requirements and are tailorable based on the utilization payload. The requirements listed below are basic safety requirements that would be supplemented using the unique safety requirements for the site selected.

3.26.1 TRAINING

M2M-SMA-UTIL-R-3000 Safety and Health

Safety and health inputs to training programs shall be tailored to the task categories involved and included in lesson plans and examinations.

RATIONALE: Safety training of operating personnel is the responsibility of the payload organization.

M2M-SMA-UTIL-R-3001 Facility and Operating Site

The payload organization shall meet the applicable facility and operating site requirements.

RATIONALE: These requirements could be defined in a payload mission specific Launch Site Support and Requirements document, such as the generic GSDO-RQMT-1243. It should be noted that there are certain launch site safety training requirements which are necessary in the process of obtaining area badging permits. Safety training will include such subjects as the following: Hazard types, recognition, causes, and effects; Prevention and control measures; Safe

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 95 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

operating procedures; Checklists; Safeguards and safety devices; Personal protective equipment (PPE); Monitoring and warning devices; and Emergency and contingency procedures.

3.26.2 HAZARDOUS OPERATIONS

M2M-SMA-UTIL-R-3002 Hazardous Ground Operations

The payload organization shall provide drawings/procedures for any activity that can result in injury to personnel, or damage to property.

Rationale: Activities must consider drawings/procedures for the following examples:

- 1) *Work Area/Environment.*
- 2) *Ordnance.*
- 3) *Propellants.*
- 4) *Lifting/Handling.*
- 5) *Radiation.*
- 6) *Toxics/Combustibles/Corrosives*
- 7) *Pressure*
- 8) *Electrical*

NOTE: A ground processing activity is classified as hazardous based on the following considerations:

- a) *Energy is involved and loss of control could result in injury to personnel or damage to equipment.*
- b) *A significant change from ambient condition will occur, e.g., increase or decrease of oxygen content, pressure, or temperature.*
- c) *Presence of hazardous materials or physical agents which presents potential exposure to personnel, flight hardware, or equipment.*

3.26.3 SAFETY EQUIPMENT

M2M-SMA-UTIL-R-3003 Personnel Protection

The payload organization shall ensure that personnel protection is provided if identified.

Rationale: Examples of required PPE are given in (but not exclusively) KNPR 1820.3, Hearing Loss Prevention, KNPR 1820.4, Respiratory Protection, and KNPR 8715.5, Personal Protective Equipment. PPE could be provided by the payload organization or through the mission specific Launch Site Support Requirement Document (LSSRD), such as the generic GSDO-RQMT-1243.

M2M-SMA-UTIL-R-3004 Industrial Safety Practices

Payload processing activities which are considered normal to general industry shall be in compliance with the requirements of accepted industrial safety practices.

Rationale: Payload processing operations which require PPE are identified in the appropriate sections of this requirements document.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 96 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.26.4 PERSONNEL SAFETY

M2M-SMA-UTIL-R-3005 Human Factors for Ground Personnel

The payload organization shall implement human factors (Human Systems Integration Requirements) in the design of GSE and the payload.

Rationale: HF-STD-001, Human Factor Design Standard and NASA-STD-3001, NASA Space Flight Human-System Standard contain guidance on human factors engineering and should be used in the design of GSE.

Valves, gauges, levers, bolts, nuts, and any other item required to be moved, turned, manipulated, or monitored by personnel in protective equipment shall be sized to facilitate operation.

Note: Such items should be located to optimize access to the item while the operator is in a standing position. Allow sufficient clearance to preclude brushing against other surfaces.

M2M-SMA-UTIL-R-3006 GSE Design

GSE shall be designed to minimize the requirement for operations and maintenance personnel to wear protective clothing during normal operations and maintenance.

Rationale: Ground personnel safety.

M2M-SMA-UTIL-R-3007 Human Interfaces

Potential hazards resulting from the human interface shall be identified and mitigated by the payload organization during the Phase Review Process.

Rationale: Ground personnel safety.

M2M-SMA-UTIL-R-3008 Human Error

Potential human errors shall be mitigated for personnel/equipment interface.

Rationale: Human error considerations include, but are not limited to: mismating a connector, throwing the wrong switch, misreading a gauge, etc. Controls will prevent a hazardous condition or damage to the hardware with emphasis on design over procedural controls.

M2M-SMA-UTIL-R-3009 Physical

Payload design shall be such that accidental contact with sharp surfaces or protrusions are prevented.

Rationale: Sharp surfaces or protrusions include edges, crevices, points, burrs, wire ends, screw heads, corners, brackets, rivets, braided cable, cable swages, cable strands, clamps, pins, latches, lap joints, bolt ends, lock nuts, etc., which if contacted, could injure operating personnel. Typical controls for sharp surfaces include, but are not limited to: the use of ductile materials, energy absorbing devices, shields, rounded corners, and flush-mounted features.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 97 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-3010 Temperature

The payload organization shall protect personnel from equipment which can generate high or low temperatures greater than 45°C (113°F) or less than 0°C (32°F).

Rationale: Methods of protection from such equipment include shielding, insulation, isolation, and/or orientation away from personnel, and labeling to warn personnel of the danger.

M2M-SMA-UTIL-R-3011 Radiation

The payload organization shall advise and protect personnel from equipment which radiates ionizing or non-ionizing radiation.

Rationale: Payload developers may want to provide radioactive sources that allow for the calibration of scientific equipment inside of their payload for mission success purposes.

M2M-SMA-UTIL-R-3012 Radiation Program Documents

The payload provider shall comply with applicable radiological health program documents governing uses of ionizing and nonionizing radiation sources, including, as applicable:

- (1) KNPR 1860.1, *Kennedy Space Center Ionizing Radiation Protection Program*
- (2) KNPR 1860.2, *Kennedy Space Center Nonionizing Radiation Protection Program*
- (3) AFI 91-110, *Nuclear Safety Review and Launch Approval for Space or Missile Use of Radioactive Material and Nuclear Systems*
- (4) AFI 40-201, *Managing Radioactive Materials in the USAF*
- (5) 45 SWI 40-201, *Radiation Protection Program*
- (6) ANSI-Z-136.1-2014, *American National Standard for Safe Use of Lasers*

Rationale: The above-mentioned documents contain procedural/administrative requirements for radiation source approvals and usage.

M2M-SMA-UTIL-R-3013 Radiation Sources

All uses of radiation sources shall be reviewed and approved by the appropriate Safety Review Panel.

Rationale: Radioactive materials procurement, use, storage, and transportation at launch/landing sites are subject to specific requirements. Such activities must be coordinated with the launch/landing site Radiation Protection Officer (RPO) at least 60 days in advance of arrival to the launch site to assure compliance with applicable regulations. Identification of the launch/landing site RPO will be provided through the appropriate Safety Review Panel.

M2M-SMA-UTIL-R-3014 Radiation Personnel Exposure

Radiation sources and associated equipment shall be designed, constructed, installed, and utilized so as to minimize personnel exposures below applicable regulatory limits.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 98 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: Options for this include, but are not limited to: radiation shielding as part of the payload design that reduces exposure limits to acceptable levels, or radioactive sources could be installed as late as possible during payload processing as practical.

M2M-SMA-UTIL-R-3015 Radiation Safety - Sources

Radiation sources associated with payloads shall be compatible with and have no adverse safety effects on ordnance items, propellants, high pressure systems, critical structure components, or systems of any other payload, the vehicle, or its crew.

Rationale: Safety of operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3016 Radiation Safety - Systems

All radiating systems shall be designed, constructed, and operated to prevent exposure of personnel, facilities, and equipment to extreme temperatures, high voltages, toxic fumes and gases, and unnecessary radiant energy.

Rationale: Safety of operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3017 General Optical Requirements

Optical instruments shall be designed such that harmful light intensities and wavelengths, as defined in ANSI-Z-136.1-2014 or its approved equivalent, cannot be viewed by operating personnel.

Rationale: Suitable protective measures include, but are not limited to: Quartz windows, apertures, or beam stops and enclosures for hazardous wavelengths and intensities unless other suitable protective measures are taken to protect personnel from ultraviolet and/or infrared burns or x-ray radiation.

The potential hazards which should be considered in the design, handling, and operation of optical equipment and associated energy sources may be grouped into five categories as follows:

- (1) Hazardous optical radiation to include ultraviolet, infrared, and visible radiation.*
- (2) Temperature extremes.*
- (3) Shatterable materials.*
- (4) Contamination from gases and cryogenics.*
- (5) High voltage and x-rays.*

M2M-SMA-UTIL-R-3018 Optical - Maximum Permissible Exposure

Light intensities and spectral wavelengths at the eye piece of direct-viewing optical systems shall be limited to levels below the maximum permissible exposure (MPE), as defined in ANSI-Z-136.1-2014 or its approved equivalent.

Rationale: Safety of operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3019 Laser Systems

A list of all lasers and their proposed use shall be provided to the appropriate Safety Review Panel to coordinate registration prior to shipment of the payload and GSE to KSC.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 99 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Rationale: KNPR 1860.2 requires registration of all Class IIIB and Class IV lasers used at KSC.

M2M-SMA-UTIL-R-3020 Laser System Requirements

Any lasers that can be accessed during ground processing shall be designed and operated in accordance with American National Standard for Safe Use of Lasers, ANSI-Z-136.1, and KNPR 1860.2, Kennedy Space Center Nonionizing Radiation Protection Program, or approved equivalents.

Rationale: Safety of operations and potential impact to flight hardware.

3.26.5 PAYLOADS AND GROUND SUPPORT EQUIPMENT (GSE)

M2M-SMA-UTIL-R-3021 Ground Support Equipment

For any payload provided GSE turned over to EGS, the payload provider shall demonstrate that all GSE required for integrating and processing flight elements for ESD missions are properly certified for use prior to delivery to EGS, as described in NASA-STD-5005.

Rationale: Safety of operations at Kennedy Space Center (ESG) and potential impact to flight hardware.

M2M-SMA-UTIL-R-3022 Biomedical Subsystems

The payload operator shall provide complete handling procedures for all hazardous biomedical subsystems.

Rationale: Hazardous biomedical subsystems consist of medical experiment equipment designed to obtain data on human adaptation and performance in the space environment. They also consist of scientific equipment designed to obtain experimental data on the effects of space environments on microorganisms, plant, and animal life.

M2M-SMA-UTIL-R-3023 Electrical Connector - Mismatch

Electrical connectors shall be designed to make it physically impossible to inadvertently reverse a connection or mate the wrong connectors if a hazardous condition can be created.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3024 Electrical Connector – Scoop Proof

Electrical connectors for energized circuits shall be of “scoop-proof” design.

Rationale: This requirement prevents a partial inadvertent mismatch will not provide pin-to-pin contact.

M2M-SMA-UTIL-R-3025 Electrical Cabling

Cables extending across work areas shall be protected against damage from personnel activity or equipment use.

Rationale: Safety of ground operations and potential impact to flight hardware.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 100 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-3026 Electrical Requirements

All GSE shall meet the requirements of the “National Electric Code (NEC), National Fire Protection Association 70 (NFPA 70)” or approved equivalents.

Rationale: Safety of ground operations.

M2M-SMA-UTIL-R-3027 Battery Requirements

Battery charging and conditioning processes and locations shall be reviewed and approved by the appropriate Safety Review Panel and the Technical Authority.

Rationale: Example of charging and conditioning processes to be considered are: battery charging equipment are continuously monitored, charging in hazardous locations, determine if the loss of power during any phase of ground processing is a hazard to personnel or equipment.

M2M-SMA-UTIL-R-3028 Grounding, Bonding, And Shielding

The design and testing requirements for electrical and electronic ground systems for bonding, grounding, shielding, electromagnetic interference, lightning protection, electrostatic discharge protection, and surge protection shall be per KSC-STD-E-0022, Bonding, Grounding, Shielding, Electromagnetic Interference, Lighting and Transient Protection, Design Requirements for Ground Systems or equivalent.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3029 Ground Potential

The design, construction, and installation of equipment shall be such that all external parts, surfaces, and shields are at ground potential at all times.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3030 Electrical Maintenance Operations

Procedures for tagging and lockout of control switches and circuit breakers shall be provided.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3031 Electrical Fuses

Only fuses of proper voltage and current ratings shall be used in circuits. No other material will be used in place of a fuse.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3032 Ordnance Categorization

The payload organization shall categorize all electroexplosive devices (EED’s) for both the pre- and post-installation situations and be able to provide the appropriate Safety Review Panel with supporting data for each categorization.

Rationale: EED classifications are as follows:

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 101 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Category A: Category A electroexplosive devices are those which, by the expenditure of their own energy, or because they initiate a chain of events, may cause injury or death to people or damage to property.

Category B: Category B electroexplosive devices are those which will not, in themselves, or by initiating a chain of events, cause injury to people or damage to property.

M2M-SMA-UTIL-R-3033 Ordnance – Category A

A device shall be assigned Category A prior to installation whenever test data to the contrary is not available.

Rationale: A device assigned Category A prior to installation may be downgraded to Category B after installation if the effects of the device and the subsequent chain of events are controlled to the satisfaction of the appropriate Safety Review Panel. Conversely, a device assigned Category B prior to installation may require upgrading to Category A after installation.

M2M-SMA-UTIL-R-3034 General Ordnance Requirements

All ordnance systems shall comply with the requirements of NASA-STD-8719.12, Safety Standard for Explosives, Propellants and Pyrotechnics.

Rationale: See section 3.23 Pyrotechnic Systems for flight hardware requirements.

M2M-SMA-UTIL-R-3035 Ordnance Testing

Items which have not previously been classified shall be tested in accordance with T.O. 11A-1-47/DLAR 8220.1, "Explosives Hazards Classification Procedures," or approved equivalent and classified accordingly.

Rationale: NASA-STD-8719.12, and AFMAN 91-201, "Explosive Safety Standards," will be used for guidance for storage, handling, and transportation of ordnance and propellants.

M2M-SMA-UTIL-R-3036 Ordnance Operations

Ordnance shall be processed only in those areas licensed or sited for ordnance operations.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3037 Ordnance Operation Location

Ordnance shall be processed only in areas approved by the Launch Site Safety Officer. Solid/liquid propellants designated for one payload shall not share an operating location with items designated for another payload except for payload integration activities.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3038 Ordnance Test Equipment – Limited Energy Input

Test equipment used to check component and circuit operation must be of a type that limits energy input and must be approved by the appropriate Safety Review Panel.

Rationale: See Ordnance Test Equipment for additional requirements.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 102 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-3039 Ordnance - In-Calibration Test Equipment

Electrical continuity and resistance checks of ordnance circuitry shall be performed using only in-calibration test equipment approved by the appropriate Safety Review Panel.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3040 Ordnance – Materials Susceptibility

Materials susceptible to the generation, collection, and holding of static electrical charges shall be reviewed and approved by the appropriate Safety Review Panel.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3041 Ordnance – Disposal

Disposal of surplus or defective ordnance items shall be determined jointly by the appropriate Safety Review Panel and the payload organization.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3042 Ordnance – EED Faraday Caps

EED Faraday caps shall be required during storage, handling, and after mechanical installation and not be removed until electrical connections are to be made.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3043 Ordnance – Nonflight Color-Coded

Nonflight items shall be color-coded, and this color-coding shall be submitted to the appropriate Safety Review Panel as part of the ground safety data package.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3044 Ordnance Test Equipment

Ordnance test equipment shall be approved by the appropriate Safety Review Panel for use in accordance with KNPR 8715.3-1, *KSC Safety Procedural Requirements Volume 1, Safety Procedural Requirements for Civil Servants/NASA Contractors*, Chapter 9 Explosives, Propellants, and Pyrotechnics.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3045 GSE Materials List

A list of materials shall be provided for each piece of GSE which interfaces with hazardous fluids.

Rationale: Hazardous fluids include, but are not limited to, gaseous oxygen, liquid oxygen, gaseous hydrogen, liquid hydrogen, hydrazine, nitrogen tetroxide, monomethyl-hydrazine, Freon-21, ammonia, and potassium hydroxide. This list will be of sufficient detail to permit an evaluation of the compatibility of the GSE design with the environment in which it is to be used.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 103 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-3046 GSE - Degradation / Contamination

The GSE shall not degrade or contaminate flight or ground systems while it is being used, checked out, serviced, or otherwise handled.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3047 GSE - Mercury Use

Mercury in liquid or vapor form shall not be used in GSE if a substitute of equivalent performance exists or an appropriate alternate design or method can be used.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3048 Mercury Contamination / Personnel Exposure

Mercury shall not be used in any applications where contamination of flight hardware or exposure to personnel could result.

Rationale: Safety of ground operations and potential impact to flight hardware.

M2M-SMA-UTIL-R-3049 Cleaning Solvents / Adhesives

Cleaning solvents and adhesive materials shall be contained in NFPA-approved safety containers.

The use of and quantity of cleaning solvents allowed in the payload processing work area shall be discussed/coordinated with appropriate Safety Review Panel.

Rationale: All users of these materials must comply with local fire, safety, and health regulations. Except where approved by the appropriate Safety Review Panel, the use of glass containers is prohibited in all payload processing work areas.

M2M-SMA-UTIL-R-3050 Plastic Films, Foams, and Adhesive Tapes

Plastics films, foams, and adhesive tapes shall be selected from the list in KTI-5212, Material Selection List for Plastic Films, Foams, and Adhesive Tapes, be submitted for testing, including per NASA-STD-6001 Test 1, electrostatic discharge testing per KSC/MMA-1985-79, Standard Test Method for Evaluating Triboelectric Charge Generation and Decay, and testing for incidental exposure to hypergols per NASA-STD-6001, Supplemental Test A.2.7, as applicable, or a Material Usage Permit obtained.

Rationale: Safety of ground operations

M2M-SMA-UTIL-R-3051 Plastic Films, Foams, and Adhesive Tapes - SDS

The material, quantity, and location of use of plastic films, foams and adhesive tapes shall be included in the Safety Data Sheet (SDS).

Rationale: Safety of ground operations

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 104 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

M2M-SMA-UTIL-R-3052 GSE – Shatterable Materials

GSE containing components made of shatterable materials which is to be used inside the vehicle, or in areas where it could fall into the vehicle, shall be designed to provide positive containment to prevent fragments from entering the vehicle.

Rationale: Safety of ground operations

M2M-SMA-UTIL-R-3053 GSE – Flammability Requirements

GSE designed for use directly in the vehicle must meet the same materials flammability requirements as the payload/experiment itself.

Rationale: For these requirements, see NASA-STD-6001.

M2M-SMA-UTIL-R-3054 GSE – Painted Or Coated Materials

GSE used in the vehicle shall not be painted or coated with materials subject to chipping, flaking, or scaling.

Rationale: Paint flakes or chips can cause severe damage to spacecraft when colliding at high relative velocities.

M2M-SMA-UTIL-R-3055 Contamination - Nutrients for Biological Agents

Materials should be selected which are not nutrients for biological agents such as mold, mildew, fungus, etc.

Rationale: Experiments in habitable areas should not provide a source of contamination. Materials which are nutrients should be hermetically sealed or treated to render the exposed surfaces resistant to biological attack.

M2M-SMA-UTIL-R-3056 Industrial Hygiene

Descriptive information concerning proposed uses of hazardous materials and physical agents shall be provided by the payload organization to the appropriate Safety Review Panel.

Rationale: The Safety Data Package should contain information on chemical exposure hazards and related controls. The SDP will describe engineering controls provided to mitigate chemical emissions. Where engineering controls alone fail to reduce chemical emissions to an acceptable level, the SDP will also describe administrative measures, (e.g., establishment of controlled work areas, warning signs) and use of PPE. The payload organization will provide a list of all hazardous materials as defined in 29 CFR 1910 (1200, Hazard Communication) containing names, quantities, locations, and proposed uses, as well as the applicable SDS materials.

M2M-SMA-UTIL-R-3057 Industrial Hygiene – Hazardous Materials / Physical Agents Exposure

Equipment which contains, possesses, or emits hazardous materials and/or physical agents shall be designed, constructed, installed, and operated in a manner to ensure the potential for exposure is kept as low as feasible.

Rationale: Safety of ground operations

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 105 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

3.27 PAYLOAD DISPOSAL

Payloads will have to be disposed. The process and disposal location will be considered in the payload concept of operations. M2M Elements will work with the payload project to determine the specific requirements that ensure safety for that M2M Element impacted.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 106 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

4.0 VERIFICATION

It is the responsibility of each payload project to establish and control the traceability between each of the Safety Requirements defined in this document and the corresponding design implementation data, as documented in the relevant payload Specification or System Requirement Document (SRD).

Final verification of SMA requirements is a payload project responsibility. M2M SMA participates in the verification process by Inspection of Records (IoR) method to ensure the cross-program safety risks are acceptable.

Example verifications are provided in Appendix C, Verification Matrix. [<FWD-30043-009>](#)

4.1 VERIFICATION METHOD DEFINITIONS

The following verification methods are defined and shall be used to qualify the system.

4.1.1 Analysis

Analysis (A) is the technical evaluation process of using techniques and tools such as mathematical models and computer simulation, historical/design/test data, and other quantitative assessments to calculate characteristics and verify specification compliance. Analysis is used to verify requirements compliance where established techniques are adequate to yield confidence or where testing is impractical. (e.g., testing would cause damage to the payload, or the on-orbit environment cannot be adequately duplicated).

When conducting Verification by Analysis, the models, simulations, and analysis tools must be accredited by the Program and Element/Modules to certify appropriate fidelity and software development quality. The accreditation authority ensures that the tools have sufficient pedigree to provide usable information for decision-making, at the level of criticality required.

4.1.2 Demonstration

Demonstration (D) is the qualitative determination of compliance with requirements by observation during actual operation or simulation under preplanned conditions and guidelines. (i.e., observing proper operation or response of the payload during expected flight-like usage). The primary distinction between demonstration and test is that demonstrations provide qualitative results, whereas tests provide quantitative results.

4.1.3 Inspection

Inspection (I) is a physical measurement or visual evaluation of the payload and associated documentation. Inspection is used to verify construction features, drawing compliance, workmanship, and physical condition. The verification of operational controls are an inspection that the inputs to a procedure (crew or ground command procedure of a certified center), flight rule, or crew training have been made or sent to the flight product authors. Crew Training inputs are the least preferred of the three approved methods of implementation. The procedures, Flight Rules, and Training products should not be complete until after the Hazard Reports are approved, so the inputs are the verification closure documentation.

4.1.4 Test

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 107 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Test (T) is actual operation of the payload, normally instrumented, under simulated or flight equivalent conditions or the subjection of parts or payload to specified environments to measure and record responses in a quantitative manner. Testing can be at flight equivalent conditions (acceptance testing) or at levels above flight conditions to prove safety margins (qualification testing).

4.1.5 Similarity

Verification by similarity is the process of analyzing prior data, configuration, processes, or applications to confirm that the item under verification is similar or identical to another item that has previously been verified to equivalent or more stringent specifications or validated to an equivalent use or function. Similarity is a form of Analysis that can be used to show that the verification records for components, subsystems, systems and elements of similar form, fit and function are suitable as V&V data for components, subsystems, systems, and elements to be used for flight.

The elements will perform an applicability assessment for any verification data generated under a previous qualification/certification effort when that data is being used for the purposes of fulfilling verification requirements under the Program. Such an assessment will inform verification planning, will be a constituent of verification compliance documentation, will only be valid if citing source data that is accessible upon demand, and will take into consideration:

- all changes to the configuration of the product being verified
- all changes to the fabrication or quality processes used to create the product
- all changes to imposed functional or performance requirements
- all differences to loads, environments, or interface conditions to which the product is exposed.

All hardware, whether heritage or not, needs to be qualified for its expected environment and operational usage. All heritage flight hardware shall be fully qualified and verified for use in its new application. In order to minimize cost, elements are allowed to use previous qualification data to the extent possible when qualifying for the new operational uses.

Similarity analysis may be combined with other verification methods, such as delta qualification testing, to accomplish verification of an integrated system. This qualification will take into consideration necessary design modifications, changes to expected environments, and differences in operational use.

4.1.6 Limited Life Item Verification

The periodic re-verification or discontinuation from use of any limited life item used as a hazard control must be considered when documenting the verification process for the end item. The safe design life and safe operational life of an end item must be assessed and are based on the certified life of safety-related component(s) (e.g., materials, seals, relief valves, regulators, electronic components, batteries, structures). Where applicable, limited life is covered in more detail in the technical requirements.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 108 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

APPENDIX A - ACRONYMS AND ABBREVIATIONS AND GLOSSARY OF TERMS

A1.0 ACRONYMS AND ABBREVIATIONS

A	Analysis
AC	Alternating Current
ACB	ACD Control Board
ACD	Artemis Campaign Development
ACGIH	American Conference of Governmental Industrial Hygienists
AIAA	American Institute of Aeronautics and Astronautics
AIT	Analysis and Integration Team
ALARA	As Low As Reasonably Achievable
ASTM	American Society for Testing and Materials
BRB	Biosafety Review Board
BSL	Biosafety Level
CDC	Centers for Disease Control
CDMP	Configuration and Data Management Plan
CE	Conducted Emissions
CESD	Common Exploration Systems Development
CFR	Code of Federal Regulations
COTS	Commercial Off The Shelf
CR	Change Request
CS	Conducted Susceptibility
D	Demonstration
DC	Direct Current
DCS	Decompression Sickness
DoD	Department of Defense
DOT	Department of Transportation
ECLSS	Environmental Control and Life Support System
EED	Electrical Explosive Devices
EEGS	Emergency Egress Guidance Systems
EGS	Exploration Ground System
EHP	Extravehicular Activity and Human Surface Mobility Program
EIRP	Effective Isotropic Radiated Power
EME	Electromagnetic Effects
EMI	Electromagnetic Interference
EPCE	Electrical Power Consuming Equipment
EPS	Electrical Power System
ESD	Electrostatic Discharge

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 109 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

EVA	Extravehicular Activity
FHL	Flammability Hazard Level
FOD	Foreign Object Debris
FORP	Fuel-Oxidizer Reaction Products
FoS	Factor of Safety
GP	Gateway Program
GSDO	Ground Systems Development and Operations
GSE	Ground Support Equipment
HEOMD	Human Exploration and Operations Mission Directorate
HEPA	High Efficiency Particulate Air
HLS	Human Landing System
HMST	Hazard Materials Summary Tables
HQ	Headquarters
HR	Hazard Report
I	Inspection
IACUC	Institutional Animal Care and Use Committee
ICD	Interface Configuration Document
INFO	Information
IoR	Inspection of Records
IR	Infrared radiation
IRD	Interface Requirements Document
ISS	International Space Station
IVA	Intravehicular Activity
J	Joules
JSC	Johnson Space Center
KOZ	Keep Out Zones
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
LoC	Levels of Containment
LoC/C	Levels of Containment/Control
LRU	Line Replacement Unit
LSA	Load Sensitive Areas
M2M	Moon to Mars
M2MCB	M2M Control Board
MAPTIS	Materials and Processes Technical Information System
MDP	Maximum Design Pressure
MEVR	Maximum Effective Vent Ratio
MLI	Multi-Layer Insulation

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 110 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

MMH	Monomethyl Hydrazine
MMOD	Micrometeoroid and Orbital Debris
MNWF	Must Not Work Function
MWF	Must Work Function
MPCV	Multi Purpose Crew Vehicle
MPE	Maximum Permissible Exposure
MSFC	Marshall Space Flight Center
NAMS	NASA Academic Mission Services
NC	Noise Criterion
NCR	Non-Compliance Report
NDE	Non Destructive Evaluation
NIH	National Institutes of Health
NIR	Non-Ionizing Radiation
NPR	NASA Procedural Requirement
NRC	Non-Compliance Report
NSI	NASA Standard Initiators
NTA	No Touch Areas
OCA	Oxygen Compatibility Assessment
OPR	Office of Primary Responsibility
ORU	Orbital Replacement Unit
OSHA	Occupational Safety and Health Administration
OSMA	Office of Safety and Mission Assurance
PD	Payload Developer
PEP	Portable Equipment Panel
PNP	Probability of No Penetration
PPE	Personal Protective Equipment
psia	Pounds per Square Inch (Absolute)
R	Requirement
rDNA	recombinant Deoxyribonucleic Acid
RE	Radiated Emissions
RF	Radio Frequency
RIVA	Requirements, Interfaces, Verification, Analysis
RQMT	Requirement
rRNA	recombinant Ribonucleic Acid
RS	Radiated Susceptibility
SBU	Sensitive But Unclassified
SDP	Safety Data Package
SEE	Single Event Effects

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 111 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

SI	International System of Units
SLS	Space Launch Systems
SMA	Safety and Mission Assurance
SME	Subject Matter Expert
SPF	Specific Pathogen Free
SPL	Sound Pressure Level
SPRT	Subsystem Problem Resolution Team
SRAG	Space Radiation Analysis Group
SRR	System Requirements Review
SSP	Space Shuttle Program
STD	Standard
T	Test
TDRS	Tracking and Data Relay Satellite
TIA	Tailoring Interpretation Agreement
TID	Total Ionizing Dose
THL	Toxicological Hazard Level
TLV	Threshold Limit Values
TMG	Thermal Micrometeoroid Garment
TTE	Time to Effect
TWFPB	Thin Walled Flexible Pressure Boundary
UDHM	Unsymmetrical Dimethyl Hydrazine
UHR	Unique Hazard Report
UTIL	Utilization
UV	ULTRAVIOLET
VV	Visiting Vehicle

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 112 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

A2.0 GLOSSARY OF TERMS

Term	Description
Catastrophic Hazard	Personnel: Loss of life or permanently disabling injury. Facilities, Equipment, Assets: Loss of M2M vehicle prior to completing its mission, or loss of essential flight/ground assets. <FWD-30043-010>
Critical Hazard	Personnel: Injury or occupational illness requiring definitive/specialty hospital/medical treatment resulting in loss of mission. Facilities, Equipment, Assets: Loss of M2M mission, condition that requires safe-haven, or major damage to essential flight/ground assets.
Control (Hazard)	Design or operational features that provide a verifiable method of preventing the hazardous event from occurring (e.g., a switch that interrupts the power to a hazardous function).
Cross-Program Utilization Payload	Cross-Program Utilization payloads are payloads that can interface with more than one Lunar exploration vehicle. They include payloads dedicated to utilization, such as science, research, development, test and evaluation, public outreach, education, and commercialization, and does not cover CESD Primary or Co-Manifested Payloads (CPLs), or secondary payloads with the SLS Program (or other Programs) that fall outside of the Artemis utilization campaign. (Reference ACD-CHTR-022 Artemis Payload Integration Working Group Charter)
Element (M2M Element)	Elements are the M2M spacecraft and launch vehicles as well as other major systems like Pressurized Rover and Lunar Surface Habitat. This term (Element) is used to represent these major systems.
Exemption A	Payload developers should check with the assigned Lead Program for additional clarification on Exemptions A and B (below). The listed text is based on HEOMD-003, Crewed Deep Space Systems Human Rating Certification Requirements and Standards for NASA Missions requirement 5.2.2. An exemption to the failure tolerance requirement. Failure of primary structure, structural failure of pressure vessel walls, and structural failure of pressurized lines are exempted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.
Exemption B	Other potentially catastrophic hazards that cannot be controlled using failure tolerance are exempted from the failure tolerance requirements with approval from the safety review panel and mandatory concurrence from the Technical Authorities and the Director, JSC (for crew risk acceptance) provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. For selected cases where a reliability-informed approach is used, as agreed by the respective programs Technical Authorities and the Center Director, JSC, the reliability requirements shall be verified with appropriate confidence intervals using robust reliability approach that is substantially anchored in actual test data verifying margins to environments (natural and induced), life requirements, operational boundaries, and failure modes.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 113 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Exemption A and B Guidelines	The specific data required to justify a failure tolerance exemption will depend on the specific hazard cause and exemption requested. Exemptions may require specific additional supporting data tailored to the exemption request. However, the following contains guidelines that are typical information required by the reviewing authorities for Exemption B items. Exemption A items are typically satisfied by review of guidelines d-f. For a system to fully comply with Exemption A, it is expected to continue to operate within the full set of margins (1.4 safety factor, 4x live, etc.) as those imposed for nominal operations. The information presented for an exemption request should be similar to the rationale and supporting data for a waiver. - However, an exemption request submitted as part of the hazard report is not a waiver to the failure tolerance requirement, and a failure tolerance exemption is not a substitute for a waiver to additional applicable design requirements (see d. below). Why is an exemption needed? What benefit does it offer? Be reasonably specific regarding the impacts of implementing failure tolerance. In cases where the impact of implementing failure tolerance is not clear, the concurring authorities may request failure tolerance design options to be identified and the impacts characterized. In addition, the system safety risk of options with and without failure tolerance may be requested as well. For those limited cases where implementing failure tolerance is clearly impractical (e.g., "part a", primary structure), exemption rationale should focus on methods by which risk is controlled or mitigated (items below) and not focus on "why" the exemption is required or developing design trades. - What is the duration of exposure to the hazard? Shorter durations may support lower risk of hazard occurrence. - What is the time to effect from when the hazard occurs until the effects manifest? If there is less than acceptable time to detect and react to the hazard, this would dictate additional reliance on the robustness of design controls, possibly necessitating a change in the control strategy. - What are the specific design requirements and standards that apply to the exemption? The use of a conservative analytical approach to the design reduces the risk. Use of higher margins in the design may offset the need to modify the control strategy. Deviations and waivers to the approved design requirements or standards may result in a need to change the control strategy. - What are the design environments that apply to the exemption? New design environments or existing environments with significant unknowns may dictate the need for a change in the control strategy. Transportation, handling, and installation environments should be considered. - What are the test and verification plans? Deviations or waivers to Program-approved qualification and acceptance testing requirements may result in the need to modify the control strategy. Usage of analyses, rather than tests, may necessitate a modification of the control strategy. - Does the design have previous flight history and what is the record of performance? In cases where there is an established record (i.e., extensive ground and flight history in relevant environments) of proven performance, less demand exists to modify the control strategy. In
------------------------------	---

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 114 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

	cases where there are unexplained or unresolved failures, this may indicate the need to modify the control strategy. h. Address results from qualitative (e.g., FMEA) and quantitative (e.g., reliability predictions) reliability analyses, and identify proposed numerical reliability requirements applicable to the item or system, with confidence limits (if applicable), and the proposed testing program to verify those requirements. i. What is the contribution of the control strategy to system risk as determined via the application of PRA? Is there an increase or decrease in system risk? j. What information supports the producibility of the design within acceptable risk? For example, the use of qualified vendors, control of critical processes, control of materials and piece parts, and use of AS9100-equivalent Quality Management Systems (QMS). k. Address any operational limitations beyond those normally required to execute the mission, requirements for flight crew, or ground operator actions to control the hazards. l. Address the ability to perform maintenance and restoration of critical functions prior to time to effect, with margin. Such a strategy must consider the availability of spare parts, tools, procedures, and training.
Factor of Safety (FoS)	The Factor of Safety (Safety Factor) is a multiplying factor to be applied to limit loads or stresses for purposes of analytical assessment (design factors) or test verification (test factors) of design adequacy in strength or stability.
Fail Safe Fasteners	When a certain number of fasteners can be lost without overall failure
Failure	The inability of a system, subsystem component or part to perform its required function within specified limits.
Failure Tolerance	The ability to sustain a certain number of failures and still retain capability. Single failure tolerance would require a minimum of two failures for the hazard to occur. Two-failure tolerance would require a minimum of three failures for a hazard to occur. Fault tolerance is a subset of failure tolerance.
Flight	This is the sequence of events that takes place between liftoff and landing of a transportation vehicle.
Fracture Control	Fracture control is a set of policies and procedures involving the application of analysis and design methodology, manufacturing technology and operating procedures to prevent catastrophic structural failure due to the initiation of and/or propagation of flaws or crack-like defects during fabrication, testing, and service life.
Fault	A fault can be seen as a defect or an abnormal situation that may cause a reduction in, or a loss of, the capability of a functional unit to perform a required function.
Hazard	A state or a set of conditions, internal or external to a system, that poses a threat to life, health, vehicle, or environment. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 115 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Hazardous Command	Hazardous Command - A command that can create an unsafe or hazardous condition which potentially endangers the crew or a M2M Element. Hazardous commands are those that can: • Remove inhibits to a hazardous function. • Activate an unpowered hazardous system. • Reduce safety critical redundancy or reduce failure tolerance. • Create a hazardous condition. • Control actively safed systems (such as robotics) during the timeframe the system is safed (or not in use).
Inhibit	Hardware implementation: A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.). Software implementation: A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available.
Level of Containment (LoC)	The failure tolerant design approach applied to contain hazardous materials that requires concentric independent layers (physical barriers) in the end item design where each individual layer is of a design integrity able to contain the hazardous material. The required number of independent levels of physical barriers is based on the hazard severity.
Levels of Containment /Control (LoC/C)	Levels of containment and levels of control used as alternatives to containment are collectively referred to as LoC/C. These can be combined to prevent the release of hazardous materials. One example of a combined approach for LoC/C is utilization of a capillary tube inside a plastic bag for the launch and stowage phases and removal of the plastic bag and utilization of MPAC (such as adhesion of the hazardous material to the inside surface of the capillary tube) during the end item operations phase. The quantity of levels in this example is based on critical hazard severity. The capillary tube and plastic bag would be qualified as a level of containment and the MPAC would be qualified as a level of control.
Lunar Exploration Systems	Lunar exploration systems include major Artemis systems such as Artemis spacecraft (e.g., Orion, HLS, Gateway), lunar rovers, lunar spacesuits, and lunar habitats.
Mechanisms	Movable mechanical system.
Monitoring	The ability to ascertain and communicate the status of functions, devices, inhibits, and parameters. Monitoring can be either real-time or on a periodic basis.
Operational Control	The control of a hazard by the real-time activities of the on-orbit crew, issuance of a ground command or the implementation of a preplanned decision by the Flight Control Team.
Operational Mitigation	Operational activity or response that helps reduce the probability of realizing the hazardous event consequence but has limitations or uncertainties that do not constitute a full level of control of the hazard (e.g., cleanup following release of a hazardous substance).

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 116 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

Planetary Protection Mission categories	Lunar missions are be assigned a final categorization of Category II, IIa, or IIb. The assignment of specific missions to a planetary protection category is based on the following: - For orbital and flyby missions to Earth's Moon, assignment to Category II. - For missions landing on Earth's Moon, but not a PSR and the lunar poles, assignment to Category IIa. - For missions landing or conducting surface operations on Earth's Moon within a PSR and the lunar poles then the mission shall be assigned Category IIb. See NASA-STD-8719.27 for the full list of mission categories and associated requirements.
Pressure Vessel	A pressure vessel is a component of a pressurized system designed primarily as a container that stores pressurized fluids and: - Contains stored energy of 19,310 joules (14,240 foot-pounds) or 0.01 pounds trinitrotoluene (TNT) equivalent) or greater based on adiabatic expansion of a perfect gas; or - Will experience a design limit pressure greater than 100 psia; or Contains a fluid in excess of 15 psia that will create a hazard if released.
Safe	A general term denoting an acceptable level of risk, relative freedom from, and low probability of personal injury; fatality; damage to property; or loss of function to critical equipment.
Safety Critical	Safety critical refers to a condition, event, operation, process, function, or feature with potential to create a critical or catastrophic hazard. A safety critical feature of a design is a feature whose failure or malfunction has the potential to create a critical or catastrophic hazard.
Safety Critical Software [NASA-STD-8739.8B]	Software is classified as safety-critical if the software is determined by and traceable to a hazard analysis. Software is classified as safety-critical if it meets at least one of the following criteria: - Causes or contributes to a system hazardous condition/event, - Controls functions identified in a system hazard, - Provides mitigation for a system hazardous condition/event, - Mitigates damage if a hazardous condition/event occurs, e. Detects, reports, and takes corrective action if the system reaches a potentially hazardous state.
Safe State (Safe) [NASA-STD-8739.8B]	A system state in which hazards are inhibited, and all hazardous actuators are in a non-hazardous state. The system can have more than one Safe State.
Sealed Container	A sealed container is any single, independent container (not part of a pressurized system), component, or housing that is sealed to maintain an internal non-hazardous environment and that does not meet the definition of a pressure vessel.
Structure	All components and assemblies designed to sustain loads or pressures, provide stiffness and stability, or provide support or containment.
Thin Walled Flexible Pressure Boundary (TWFPB)	A thin-walled flexible pressure boundary (TWFPB) hardware item is classified as fracture critical if a single leakage or rupture/burst event

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 117 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

	involving the TWFPB could result in a catastrophic hazard (i.e., zero fault tolerant, 0FT).
Vented Container	An enclosure which is not intentionally sealed or is provided with vents such that it will not create a hazard in the event of depressurization or repressurization of the surrounding volume.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 118 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

APPENDIX B - OPEN WORK

B1.0 TO BE DETERMINED

The table To Be Determined Items lists the specific To Be Determined (TBD) items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within carets. The TBD item is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<TBD-XXXXX-001>** is the first undetermined item assigned in the document). As each TBD is resolved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBDs will not be renumbered.

TABLE B1-1 TO BE DETERMINED ITEMS

TBD	Section	Description
TBD-30043-001	2.1 Table 2.1-1, 3.2, M2M-SMA-UTIL-R-2002	Update when the M2M SMA Plan is released. This includes the hazard severity definitions.
TBD-30043-002	3.9, M2M-SMA-UTIL-R-2044	Add the applicable M2M Element documents that list the RF radiating devices requirements.
TBD-30043-003	3.23, M2M-SMA-UTIL-2129	MPCV requirement document that captures the updated payload pyro requirements will be added once released

B2.0 TO BE RESOLVED

The table To Be Resolved Issues lists the specific To Be Resolved (TBR) issues in the document that are not yet known. The TBR is inserted as a placeholder wherever the required data is needed and is formatted in bold type within carets. The TBR issue is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<TBR-XXXXX-001>** is the first unresolved issue assigned in the document). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBRs will not be renumbered.

TABLE B2-1 TO BE RESOLVED ISSUES

TBR	Section	Description
TBR-30043-001	3.11, M2M-SMA-UTIL-R-2049	Additional discussions are required to resolve internal and deployable payload concerns associated with M2M-SMA-UTIL-R-2049, Cross-program Utilization Payload Monitoring.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 119 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

B3.0 FORWARD WORK

The table forward Work lists the specific Forward Work (FWD) items in the document that are not yet known. The FWD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within carets. The FWD issue is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<FWD-XXXXX-001>** is the first unresolved issue assigned in the document). As each FWD is resolved, the updated text is inserted in each place that the FWD appears in the document and the issue is removed from this table. As new FWD issues are assigned, they will be added to this list in accordance with the above described numbering scheme. Original FWDs will not be renumbered.

TABLE B3-1 FORWARD WORK

FWD	Section	Description
FWD-30043-001	1.3 NOTE	Reference JICB Action JICB-0550: M2M SMA to provide a path to fill the gap in +16 sec after deployment to end of SPL mission, including potential additional safety requirements and the associated safety process. Work with FOD, Orion, SLS, EGS, and IHAITT and return to JICB with a proposal for path forward following closure of JICB action JICB-0550.
FWD-30043-002	3.7, 3.18.5 Table 3.18.5-1	Biomedical instrumentation safety requirements are in development to address the unique M2M oxygen rich atmosphere. SSP 51721 section 4.3.4 Biomedical Instrumentation is a starting point.
FWD-30043-003	3.7, M2M-SMA-UTIL-R-2029	Develop Safety Requirements for the use of Electrolytic Capacitors for Payloads.
FWD-30043-004	3.14.1	Safety requirements for animals will be developed at a later time.
FWD-30043-005	3.15	It is forward work to determine if a payload requirement is necessary to limit lunar dust returned to the crew compartment. The M2M lunar dust team is evaluating dust removal methods.
FWD-30043-006	3.17.2	Work with the M2M Elements to determine if new requirements or a table of requirements should be added to address detection and suppression design requirements that would be levied and verified via each M2M Elements ECLSS documentation, or this section removed.
FWD-30043-007	3.20	M2M 30040, M2M Graphical User Interface (GUI) Standard is not baselined at this time. Revisit the GUI requirements after M2M 30040 is baselined to see if updates are required.
FWD-30043-008	3.22	Safety requirements for payloads with propulsion systems will be developed at a later time.
FWD-30043-009	4.0 and Appendix C	Appendix C Verification Matrix that includes example verifications will be added in the next revision.
FWD-30043-010	A2.0	Update when the M2M definition for Catastrophic is updated.

Revision: Initial Release (Draft)	Document No: M2M-30043
Release Date: TBD	Page: 120 of 120
Title: M2M Cross Program Utilization Payload Safety Requirements	

FWD	Section	Description
FWD-30043-011		M2M will consider moving this requirement document into a more usable matrix format. This will be coordinated with M2M SE&I and if approved will be released in a future revision of this document.
FWD-30043-012	3.19	Revisit Section 3.19 EVA section to incorporate the EVA safety requirements after EHP 10028 stabilizes.