# L0 Safety Requirements

020.10.15.10.00-0004-REQ

Status: **RELEASED**

| PREPARED BY | ORGANIZATION | DATE |
|---|---|---|
| J. Bolyard, Safety Group Lead | Manager, Environment, Safety, & Security | 2021-12-16 |

| APPROVALS | ORGANIZATION | SIGNATURES |
|---|---|---|
| J. Meyers, ngVLA Project Manager | ngVLA Department | Jill R. Meyers<br>Jill R. Meyers (Dec 28, 2021 18:57 MST) |
| T. Beasley, Project Director | Director, NRAO | Tony Beasley<br>Tony Beasley (Dec 29, 2021 12:17 EST) |

| RELEASED BY | ORGANIZATION | SIGNATURE |
|---|---|---|
| T. Beasley, Project Director | Director, NRAO | Tony Beasley<br>Tony Beasley (Dec 29, 2021 12:17 EST) |

## Change Record

| Version | Date | Author | Affected Section(s) | Reason |
| --- | --- | --- | --- | --- |
| 1 | 2018-05-07 | J. Bolyard | All | Initial draft. |
| 1.1 | 2018-09-15 | J. Bolyard | All | Updated changes. |
| 2 | 2019-01-16 | J. Bolyard | All | Updated changes from pre-decadal review RIDs. |
| 2.1 | 2019-01-25 | J. Baca | All | Formatted document. |
| 3 | 2019-05-30 | A. Lear | All | Prepared document for review. |
| 4 | 2019-05-31 | R. Selina | 5 | Updated numbering scheme to match requirements management standards. |
| A | 2019-07-17 | A. Lear | All | Prepared PDF for signatures and release. |
| A.01 | 2019-08-30 | J. Bolyard | 2.1 and 5 | Updated ADs, adding requirements to incorporate ADs by reference. |
| A.02 | 2019-08-30 | R. Selina | 2, 5, 6. | Minor reformatting and typo corrections for re-release for StRR. |
| B | 2019-09-03 | A. Lear | All | Prepared PDF for signatures and release. |
| C | 2020-08-14 | J. Bolyard | Reference Documents; Section 5 | Updated from Stakeholder Comments. |
| C.01 | 2021-12-16 | J. Bolyard | 3, 4.1, 4.2 | Updates to design review and team definitions. |
| D | 2021-12-28 | A. Lear | All | Formatting, copy edits; prepared PDF for signatures and release. |

# Table of Contents

# 1 Introduction

## 1.1 Purpose

This document identifies and captures the requirements for safety instrumentation, including hardware, software, and processes and procedures through the entire lifecycle of the Next Generation Very Large Array (ngVLA) effort. The requirements are intended to address the ngVLA efforts through design including reviews and prototyping, construction, commissioning actions, operation, and ultimate decommissioning.

## 1.2 Scope

The scope of this document extends to all Integrated Product Teams (IPTs), project reviews, work practices in labs and worksites, and subcontractors who provide documentation or procedures, or work at any ngVLA site.

## 1.3 Project Background

The ngVLA is a project of the National Radio Astronomy Observatory (NRAO) to design and build an astronomical observatory that will operate at centimeter wavelengths (25 to 0.26 centimeters, corresponding to a frequency range extending from 1.2 GHz to 116 GHz). The observatory will be a synthesis radio telescope constituted of approximately 263 reflector antennas, 244 of 18 meters diameter and 19 of 6 meters diameter, operating in a phased or interferometric mode. The antenna count includes antennas of the Long Baseline Array (LBA).

Construction and integration will be distributed across several existing NRAO and partner sites and in new facilities for this purpose. Operations will be conducted from both the VLA site and an Array Operations Center.

# 2 Related Documents and Drawings

## 2.1 Applicable and Reference Documents

The following documents are applicable to this Safety Specification to the extent specified. In the event of conflict between the documents referenced herein and the content of this Safety requirement, the content of the reference documents shall take precedence. In case of conflict, with respect to design, construction, and operation, the most stringent standards shall apply.

| Ref. No. | Document Title | Rev/Doc. No. |
| --- | --- | --- |
| AD01 | Environment, Safety, and Security Policy and Program Manual | Version D, Oct. 2016 |
| AD02 | ngVLA Safety Risk Analysis Procedures | 020.80.00.00.00-0002-PRO |
| AD03 | OSHA General Industry Standard | 29 CFR1910 |
| AD04 | OSHA Construction Standard | 29 CFR1926 |
| AD05 | Environmental Protection Agency Clean Air Act of 1963 | 33 U.S.C.: Navigable Waters |
| AD06 | Environmental Protection Agency Clean Water Act of 1972 | 42 U.S.C. ch. 85, subch. I § 7401 et seq |
| AD07 | National Fire Protection Association, Consensus Standards, including the National Electric Code | |

| Ref. No. | Document Title | Rev/Doc. No. |
| --- | --- | --- |
| RD01 | Project Lexicon and Acronyms | 020.10.10.10.00-0005-LIS-A |
| RD02 | Lifecycle Stages Concepts | 020.10.05.00.00-0001-PLA |

# 3 Safety Scope

The Safety Group Work Package includes safety, physical security, ongoing environmental protection actions, sustainability, and identification of associated risks. In the context of this document, "safety" includes all the aforementioned program elements. The Safety Group scope includes assessing the requirements for all phases of the ngVLA effort.

Per the National Science Foundation (NSF) and in accordance with Executive Order (EO) 13693, the ngVLA effort must include means and methods for sustainable operations including utility usage, waste disposal, and recycling services. Sustainable operations include all facilities that are used as offices, laboratories, information technology rooms or centers, or dormitory spaces.

The Safety Group effort crosses all IPT boundaries and is anticipated to be integrated into all design packages and operational procedures, and extends through the lifecycle of the ngVLA. The ngVLA Safety Group will assist to ensure compliance with federal, state, and local safety requirements. In addition, the effort will examine compliance with international standards, such as may be applicable in Mexico.

The proposed ngVLA project will require compliance with AUI policies for safe planning and management of large facilities. Consequently, there must be significant collaboration with all other IPTs as the requirements influence the Safety support needed. In this document, NRAO will determine areas that need further development to meet the collaborating IPT ngVLA requirements.

# 4 Safety Across the ngVLA Lifecycle

All IPTs shall have a designated central point of contact for safety-related issues and preparation of safety documentation for reviews. All personnel shall be alert to the need to identify potential safety hazards. Once identified, steps shall be taken to eliminate them, or reduce them to levels judged acceptable. The central point of contact for safety matters shall be the IPT safety liaison.

## *4.1 Safety Group Review Support Requirements*

The ngVLA Safety Group is expected to support the Requirements Review for each subsystem to ensure that the relevant safety requirements are appropriate to the plan and meet the safety flow throughout the subsystem through the final system design. Additionally, the ngVLA Safety Group will support the following Design Reviews to ensure that the design is mature enough from the safety perspective to proceed to prototyping and to ensure that the hazard analysis is sufficiently complete.

All Design reviews and their scope are as described in [RD01] and [RD02]. The following reviews shall have a Safety Group member's support:

- Conceptual Design Review (CDR) of the subsystem review to ensure that the safety compliance assessment and safety risk analysis are complete at the subsystem CDR level.
- System Conceptual Design Review (CDR) of the entire project system review to ensure that the safety, security, sustainability, and environmental impacts are addressed and included in the compliance assessment and safety risk analysis at the system CDR level.

- Preliminary Design Review (PDR) that includes a thorough safety and environmental review of the updated design package. This will verify that any modifications and adjustments identified at the CDR review have been incorporated into the PDR planning.
- Final Design Review (FDR) that includes review of the management documents for safe procedures, safe inspection requirements, and preventive maintenance procedures for safe operation.
- Manufacturing readiness review of final documentation and to offer signoff review of safe machinery. This includes safety acceptance of manufacturer-provided equipment and components.
- Test Readiness Review (TRR) to verify that the test procedures are approved and the equipment and software under test are in their final deliverable configuration. The TRR shall include confirmation that the safety approval has been received.
- Product Acceptance to accept delivery from subcontractors, if applicable, and deliver the Safety Data Package documentation as part of the Acceptance Data Package. This includes but is not limited to:
    - Safety Procedures, if not described in the operator manual;
    - Declaration of Conformance; and
    - Hazard Analysis in accordance with ngVLA Safety Risk Analysis Procedures.

## *4.2 Design Activities*

Safety assurance matters shall conform to the requirements defined in the NRAO Environment, Safety, and Security (ES&S) Policy and Program Manual [AD01], and with site-specific safety directives.

Potential hazards shall be identified as a part of the normal design process and eliminated or reduced as far as possible. Safeguards shall be determined for outstanding hazards, which will reduce their possible effects to the lowest reasonable level in accordance with ngVLA Safety Risk Analysis Procedures. Any safety hazards that cannot be eliminated during the design process shall be reported to the Safety Group Lead at the design review and to the ngVLA Project Office. Any progress shall be reported, including necessary proof that the relevant requirements have been satisfied.

## *4.3 Construction Activities*

Construction work shall conform to requirements of the NRAO ES&S Policy and Program Manual [AD01] and Safety Work Plans provided by project contractors. Any design documentation affecting construction activities shall be provided in contract documents and procurement requirements. The Safety Group shall support all construction activities with programmed meetings and reviews of contractor documentation, and shall sign off on acceptance of each completed construction site.

## *4.4 Operations Activities*

Operations activities are not addressed in detail in this document and shall follow NRAO ES&S Policies governing operational safety as described in the ES&S Policy and Program Manual [AD01].

# 5 Safety Requirements

The following requirements shall be fulfilled ***as a minimum*** to achieve acceptable levels of safety across the ngVLA project.

| Req. ID# | Requirement Name | Requirement |
| --- | --- | --- |
| SAF0028 | Design for all lifecycle phase safety | The ngVLA shall be designed to meet or exceed personnel health and safety performance requirements in all phases of the project lifecycle in accordance with standards applicable to the work. |
| SAF0029 | Comply with ES&S manual | All aspects of the design and construction shall comply with the ES&S Policy and Program Manual [AD01]. |
| SAF0030 | Develop safe procedures | Where appropriate, each IPT shall develop procedures for personnel and equipment safety throughout the design, construction, and operation phases to address working conditions and use procedures, as well as identify the design features, that impact safety, environmental protection, and sustainability. |
| SAF0031 | Follow safe design priorities | The priority for safe design shall address safety of personnel, followed by safety of equipment, and then the integrity of the data. |
| SAF0032 | Follow mitigation order of precedence | The ngVLA system shall govern the hazard analysis and safety practices in an order of precedence as follows:<br>1) Design for minimum risk: The primary means for mitigating risk shall be to eliminate the hazard through design.<br>2) Incorporate safety devices: Protective devices shall be used as part of system design to reduce hazard risks to an acceptable level where possible.<br>3) Provide warning devices: When neither design nor safety devices can effectively minimize a hazard risk, devices shall be used to detect the hazard condition and alert personnel of its presence.<br>4) Procedures and training: Only when it is impractical to substantially eliminate or reduce the hazard, or where the condition of the hazard indicates additional emphasis, special operating procedures and training shall be used. All such procedures shall be fully documented. |
| SAF0033 | Intentionally deleted | |
| SAF0034 | Intentionally deleted | |
| SAF0035 | Intentionally deleted | |
| SAF0036 | Document safety compliance | Each completed design element must document safety compliance with the safety system specifications. |
| SAF0037 | Describe process to achieve safe state | Each element must describe processes and address details to achieve safe state including potential sequencing of events. |
| SAF0038 | Describe additional safety requirements | Each element must describe any additional measures required during validation, and describe consequences of failure to follow sequential processes. |

| Req. ID# | Requirement Name | Requirement |
| --- | --- | --- |
| SAF0039 | Design facilities for safe operational use | The ngVLA Facility shall be designed to safely meet its technical requirements and operational specifications at the following physical locations. The Facility includes the main radio antennas, service areas, utility equipment, and all other infrastructure necessary to safely execute all the operational functions and secure all ngVLA assets. The Facility design must provide the space and functional equipment to maintain all system assets operating on the site. |
| SAF0040 | Design controls for safe operation | The control capabilities throughout the system shall include both local and remote exclusive control modes for safe operation. Note this applies to any system that has potential for motion. |
| SAF0041 | Ensure initial safe state for subsystem power up | Each Facility in the ngVLA Observatory shall implement a non-software-based safety system(s) in areas where injury or harm to personnel and or equipment can occur. Each subsystem when powered up shall be initialized into a known safe state without human intervention. |
| SAF0042 | Ensure subsystems are standalone safe | Each subsystem shall maintain its own technical health, safety, and status without any other subsystem operational. |
| SAF0043 | Address facility security in design | The project shall affirmatively address site and facility security needs in the design in accordance with the NRAO security policy(ies). |
| SAF0044 | Address sustainability in design | The project shall affirmatively address sustainability goals in ngVLA design and ongoing operations. |
| SAF0045 | Comply with the ngVLA Safety Risk Analysis Procedures | All aspects of the project design shall comply with the Risk Analysis procedures. |
| SAF0046 | Comply with the requirements of OSHA General Industry Standard 1910 | All general work activities (non-construction) are subject to the General Industry Standard. All work and workers shall comply with the 1910 requirements (Personnel Safety Requirement). |
| SAF0047 | Comply with the requirements of the OSHA Construction Standard | All construction activities performed by the ngVLA project team and contractors shall be subject to compliance with the OSHA 1926 construction standard. (Construction Safety Requirement). |
| SAF0048 | Comply with the requirements of the Environmental Protection Agency Clean Air Act of 1963 | All project elements shall comply with the requirements of the EPA CAA (Cooperative Agreement Requirement). |
| SAF0049 | Comply with the requirements of the Environmental Protection Agency Clean Water Act of 1972 | All project elements shall comply with the requirements of the EPA CWA (Cooperative Agreement Requirement). |

| Req. ID# | Requirement Name | Requirement |
|---|---|---|
| SAF0050 | Comply with the National Fire Protection Association, Consensus Standards, including the National Electric Code | All project elements shall comply with the requirements of the National Electric Code and applicable NFPA standards for fire and life protection. |
| SAF0051 | Safety Critical Software (contrast Safety-related) | No project elements shall solely rely on software to prevent a failure or malfunction that may result in death, severe damage to equipment, or environmental harm. |
| SAF0052 | Most stringent standards | Project elements designed, constructed, and operated in varying jurisdictions shall comply with the most stringent standard applicable. Note this applies to international efforts. |
| | | |

# 6 Appendix

## 6.1 Abbreviations and Acronyms

| Acronym | Description |
| --- | --- |
| AD | Applicable Document |
| CAA | Clean Air Act |
| CDR | Critical Design Review |
| CFR | Code of Federal Regulations |
| CWA | Clean Water Act |
| EPA | Environmental Protection Agency |
| ES&S | Environment, Safety, and Security |
| ICD | Interface Control Document |
| IPT | Integrated Product Team |
| ngVLA | Next Generation VLA |
| NEC | National Electric Code |
| NFPA | National Fire Protection Association |
| NSF | National Science Foundation |
| OSHA | Occupational Safety and Health Administration |
| RD | Reference Document |
| RFI | Radio Frequency Interference |
| TBD | To Be Determined |
| VLA | Jansky Very Large Array |