ngVLA Safety: Risk Analysis Procedures

020.80.00.00.00-0002-PRO-A-SAFETY_RISK_ANALYSIS

Status: **RELEASED**

PREPARED BY	ORGANIZATION	DATE
J. Bolyard	Environmental Safety & Security Div., NRAO	2019-06-10

APPROVALS (Name and Signature)		ORGANIZATION	DATE
R. Selina, Project Engineer	R Selina 2019.07.10 15:11:36 -06'00'	Electronics Div., NRAO	2019-07-10
M. McKinnon, Project Director	Mark McKinnon Digitally signed by Mark McKinnon Date: 2019.07.11 06:59:57 -06'00'	Asst. Director, NM-Operations, NRAO	2019-07-10

RELEASED BY (Name and Signature)		ORGANIZATION	DATE
M. McKinnon, Project Director	Mark McKinnon Digitally signed by Mark McKinnon Date: 2019.07.11 07:00:14 -06'00'	Asst. Director, NM-Operations, NRAO	2019-07-10

Change Record

VERSION	DATE	AUTHOR	REASON
1	2019-03-28	Bolyard	Initial Draft
2	2019-06-10	Lear	Formatted, copy-edited; reorganized sections for consistency
3	2019-07-09	McKinnon	Minor edits throughout
A	2019-07-10	Lear	Prepared document for approvals and release

Table of Contents

1 Introduction

1.1 Purpose

To ensure safe operation of a product, process, work activity, or design, it is necessary to have a procedure to identify risks as well as apply appropriate controls to manage risks. This procedure is commonly referred to as a Risk Analysis.

To be beneficial, the Risk Analysis must be granular enough to produce an overall view of which health, safety, and environmental problems exist and to rank them in order of severity. The Risk Analysis also provides information to allow judgments to be made on the safety of the design. The Risk Analysis must start in the early design process and follow development up to the final acceptance.

A complete Risk Analysis includes some or all of the following:

1. A determination of the limits of the design (Section 4.1) is required for all manufactured items.
2. A Preliminary Hazard List (PHL) identifies hazards and estimates analyzed risk levels (Section 5.2). This is required for all manufactured items.
3. A Preliminary Hazard Analysis (PHA) evaluates the hazards and design solutions to the hazards identified in the Preliminary Hazard List. The Preliminary Hazard Analysis is not always required but is based in part on the Preliminary Hazard List results (Section 5.3). The Safety IPT will assist in determining if the PHA or any further action is needed.
4. A Safety Compliance Assessment (SCA) verifies compliance with applicable safety regulations (Section 5.4).
5. A System Hazard Analysis (SHA) examines the safety of the design as a whole (Section 5.5).
6. A Safety Review and Documentation developed based on the above activities provides a fully documented review of the hazards (Section 5.6).

Risk Analysis relies on the judgment and decisions of the designer. These decisions must be supported by qualitative methods and if possible, by quantitative methods. Quantitative methods are particularly appropriate when the foreseeable severity and extent of harm are high.

The Risk Analysis must be conducted so that it is possible to document the procedures and the results achieved under consideration of the whole lifecycle of the product, process, work activity, or design. This document provides the safety design requirements, including hardware, software, and processes and procedures through the entire ngVLA lifecycle.

The choice of the relevant essential safe design requirements must be based on the hazards in a given product. Therefore, designers need to carry out a hazard analysis to determine the essential requirements applicable to the product. This analysis must be documented and included in the technical documentation.

1.2 Scope

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

This document outlines and details the requirements for identifying the risk associated with safe design of a product, process, work activity, or design. The Risk Analysis must be completed by the project personnel responsible for any design and their interface to the design as a whole. For items procured outside of the ngVLA project, the manufacturer is responsible to comply with these or equivalent national standards.

1.3 Project Background

The Next Generation Very Large Array (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 of 6 or 18 meters diameter, operating in a phased or interferometric mode. The antenna count includes antennas of the Long Baseline Array (LBA).

2 Related Documents and Drawings

2.1 Applicable 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 former shall take precedence.

Reference No.	Document Title	Rev/Doc. No.
AD01	ngVLA Preliminary System Requirements	020.10.15.10.00-0003-REQ
AD02	NRAO Environment, Safety, and Security Policy and Program Manual	Version D, Oct. 2016.
AD03	ngVLA L1 Safety Requirements	020.80.00.00.00-0001-REQ
AD04	ngVLA L0 Safety Requirements	020.10.15.10.00-0004-REQ

2.2 Reference Documents

The following references provide supporting context:

Reference No.	Document Title	Rev/Doc. No.
RD01	OSHA General Industry Standard	29 CFR 1910
RD02	OSHA Construction Standard	29 CFR1926
RD03	Environmental Protection Agency Clean Air Act of 1963	33 U.S.C.: Navigable Waters
RD04	Environmental Protection Agency Clean Water Act of 1972	42 U.S.C. ch. 85, subch. I § 7401 et seq
RD05	National Fire Protection Association, Consensus Standards	NFPA

3 Safety Scope

The Safety IPT 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 scope of the Safety IPT includes an assessment of the requirements for all phases of the ngVLA effort.

The safety integrated product team crosses all IPT boundaries and is anticipated to be integrated into all design packages, operational procedures, and extends through the lifecycle of the ngVLA. The ngVLA Safety IPT 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 the AUI policies for safe planning and management of large facilities. Consequently, there must be significant collaboration with all other Integrated Product Teams (IPTs) as the requirements influence the safety support needed.

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 Design Activities

Safety assurance matters shall conform to the requirements defined in the NRAO Environment, Safety, and Security Policy and Program Manual [AD02], 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 this document.

Any safety hazards that cannot be eliminated during the design process shall be reported to the Safety IPT 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.

4.2 Operations Activities

Operations activities are not addressed in this document and shall follow the NRAO ES&S Policies governing operational safety as described in the Environment, Safety, and Security Policy and Program Manual [AD02].

4.3 Definitions

For the purpose of this document, the following terms and definitions apply:

- Accident: An undesired event resulting in death, injury, damage to health, damage to property or other form of loss.
- Hazard: A biological, chemical, or physical agent or condition with the potential to cause a harm. Hazards can be qualified to define its origin or the nature of the expected "harm" (e.g., electric shock hazard, crushing hazard, cutting hazard, fire hazard).
- Hazard Identification: Identification of biological, chemical, and physical agents capable of causing adverse health effects.
- Hazard Verification: All activities performed to demonstrate that the design meets or is capable of meeting the specified safety requirements.
- Risk: An expression of the likelihood of injury or harm resulting from a hazard, calculated as a combination of the probability of an adverse health effect and the severity of that effect.
- Protective Measure: Means used to reduce risk. Protective measures include risk reduction by inherently safe design, protective devices, personal protective equipment, information for use and installation, and training.

5 Risk Analysis Procedures

5.1 General Considerations

Use the following procedure in the Risk Analysis for all products, and process activities, work activities, or designs. The following steps must be conducted by the designer or manufacturer in cooperation with the appropriate IPT prior to the completion of the PDR. These steps may be somewhat informal but must be an integral part of the design consideration.

1. Review the Feasibility of a Suitably Safe Design: The first general consideration and examination of the effort must not lead to a fundamental objection to the feasibility of a safe design. Conduct a review of the entire design concept for the subsystem, component, or article as appropriate.
2. Consider Functional Uses: List and describe the parts and the intended functions and modes of operation.
3. Evaluate Time and Life: Describe how, when, and in which stages of the lifecycle it will be operated by workers.
4. Determine Applicable Laws & Regulations: As the design is developed, the designer shall formulate the design based on applicable safety requirements and document the standards to which the product is designed. ngVLA Safety will assist and support these efforts with technical clarifications with respect to regulatory requirements as requested.

5.2 Preliminary Hazard List (PHL)

A Preliminary Hazard List (PHL) is needed early in the project lifecycle to enable the project and design teams to choose the hazardous areas on which to put safety management emphasis. Every product or item manufactured for the ngVLA project must perform a PHL to identify the primary hazards and accident scenarios associated with the specific (sub)system being designed. The Preliminary Hazard List is carried out by a checklist-based approach (see Section 7.2).

5.2.1 PHL Task Description

The IPT safety liaison (or a delegate) shall examine the design concept and compile a PHL identifying possible hazards that may be inherent in the design. The IPT safety liaison shall further investigate selected hazards or hazardous characteristics identified by the PHL as directed by the ngVLA management and/or AUI/NRAO to determine their significance.

5.2.2 PHL Requirements

The Preliminary Hazard List contains the following information:

- A brief description of the design, and its domain
- A brief description of any subsystems identified, and the boundaries or interfaces between them
- A description of the design functions and safety features or controls
- A reference to all source documents used, including versions, dates, and status
- Details of any similar designs, including hazards, accidents, and initiating events
- A list of hazards identified which are applicable to the design, including a description of the hazard, and a unique reference to the identified hazard
- A list of identified accidents applicable to the design including a description of the accident, and a unique reference to the identified accident
- A description of human error which could create or contribute to accidents
- Conclusions and recommendations

The PHL describes the risk and estimates the probability of occurrence of a harm. The risk estimation considers the frequency and duration of the exposure of persons to the hazard, probability of occurrence of a hazardous event, the technical and human possibilities to avoid or limit the harm (e.g., emergency stop equipment, reduced speed enabling device, awareness of risks), and severity of harm. In many cases, these elements cannot be determined exactly but can only be estimated. (See Section 6 for procedures to estimate risk).

Where risk has been identified, the following measures are necessary to prevent injury:

- Assess design measures: Determine if measures are appropriate to the level of risk. First, eliminate hazards by design, manage remaining risks, and notify and train users on remaining risk.
- Verify compatibility of design measures: Ensure that design features and measures will not defeat other measures or modes of operations.

5.3 Preliminary Hazard Analysis (PHA)

The Preliminary Hazard Analysis (PHA) is an inductive method of analysis in the design stage whose objective is to broadly generalize from observation, identify safety critical areas, evaluate hazards, and identify the design criteria to be used. The PHA is based on the results of the PHL.

A PHA involves making a study during concept or early development of a design or facility to determine the hazards that could be present during operational use.

5.3.1 PHA Task Description

The IPT safety liaison shall perform and document a Preliminary Hazard Analysis to obtain an assessment of the concept or design. The PHA effort shall be started during the preliminary design phase of the program so that safety considerations are included in design alternatives. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to ngVLA and NRAO shall be considered.

To avoid obscuring important hazards with insignificant detail, develop an approach to select accident sequences for consideration. For example, include the criteria for the exclusion of rare events, and the exclusion of the effect of multiple (e.g., three or more), independent random component failures occurring concurrently.

Analyze major hazards associated with the design. Control these hazards by engineering or by re-design. Hazards not previously identified in the Preliminary Hazard List shall be addressed at this time.

5.3.2 PHA Hazard Considerations

The Preliminary Hazard Analysis (PHA) generates a detailed list of hazards associated with the design. The main purpose of Preliminary Hazard Analysis is to identify the hazardous states of a design and their implications. The PHA must consider the following for hazard identification and evaluation at a minimum:

- Hazardous components (e.g., electrical systems, cooling fluids, toxic substances, hazardous construction materials, pressure systems, lasers, and other energy sources).
- Safety related interface considerations among various elements of the design, e.g., material compatibility, inadvertent activation, fire initiation and propagation. Design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, or designated undesired events) shall be identified and appropriate action taken to incorporate them in the software and related hardware specifications.

- Environmental constraints including transport, handling and operating environments, (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, and pressure).
- Operating, testing, maintenance and emergency procedures (e.g., human errors, tasks, and requirements; factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance, and environmental conditions).
- Facilities, support equipment (e.g., provisions for storage, assembly, checkout, proof-testing of hazardous designs/assemblies which may include toxic, flammable, corrosive or cryogenic fluids; electrical power sources) and training (e.g., training and certification pertaining to safety operations and maintenance).
- Safety related equipment, safeguards, and possible alternative approaches (e.g., interlocks, system redundancy, fail-safe design considerations, personal protective equipment, ventilation, and access barriers).

5.3.3 PHA Requirements

The PHA requirements for completion include the following information. A form sheet and instructions for a PHA are provided in Section 8.

- Establish, for the analysis, the overall design structure and functionality.
- Establish, for the analysis, the boundaries between the design, any designs with which it interacts, and the domain.
- Identify a detailed list of the hazards of the design based on the Preliminary Hazard List.
- The accident risk classification adopted (Section 6).
- Preliminary probability levels including predicted probabilities for each accident or accident sequence.
- Identify the accidents and, to a practicable extent, the events in the accident sequence including any sequences that may be subsequently discounted.
- Assign each accident and accident sequence a hazard severity categorization.
- Assign each hazard a probability target based on the designer's best judgment.
- Document any safety features or controls that are to be implemented during the design and development phases.

5.4 Safety Compliance Assessment (SCA)

The purpose of this task is to perform and document a Safety Compliance Assessment to verify compliance with national codes, and specifications imposed contractually or by law to ensure safe design, and to comprehensively evaluate the risk being assumed prior to testing or operation or at contract completion.

5.4.1 SCA Task Description

The IPT safety liaison shall initiate the Safety Compliance Assessment. The Safety IPT Lead shall be invited to participate with and assist the Safety Compliance Assessment to identify and document compliance with appropriate design and operational safety requirements. The compliance assessment includes a review of design drawings, procedural reviews, and equipment inspections.

The following documents must be reviewed in the Safety Compliance Assessment and contained in the Safety File:

- The Preliminary Hazard List prepared for the Design Phases (Section 5.2), updated where necessary, giving implementation details and updates for information obtained from newly identified hazards
- Safety relevant reference and requirements documents, including the PHA prepared for the Preliminary Design Review (PDR) and/or the Critical Design Review (CDR)

- Safety certificates that were delivered by the suppliers. These may be documents like Material Safety Data Sheets, verification of conformity, specifications, etc.
- Inspection reports of instrument assemblies (handling equipment, vacuum and cryogenic equipment, etc.)
- Operating and Maintenance Manuals as relating to safety issues
- Observatory work procedures (lockout/tagout procedures, handling of liquid nitrogen, working hours, work and driving in high altitude, etc.) relevant to the installation, commissioning and operation of the product

The assessment shall incorporate the scope and techniques of PHA to the extent necessary to assure the safe design, operation, maintenance, and support of the system.

A Safety Compliance Assessment must

- Identify contractual safety specifications, standards and codes applicable to the design, and document compliance of the design and procedures with these requirements;
- Identify and evaluate residual or remaining hazards inherent in the design or that arise from design-unique interfaces, installation, test, operation, maintenance, or support;
- Identify necessary specialized safety design features, devices, procedures, skills, training, facilities, support requirements, and personal protective equipment;
- Identify hazardous materials and the precautions and procedures necessary for safe storage, handling, transport, use and disposal of the material; and
- Conclude with a signed statement that all identified hazards have been eliminated or their associated risk minimized to levels contractually specified as acceptable.

This Safety Compliance Assessment report is prepared by the IPT safety liaison which must be submitted to the ngVLA Project Director and the Project Office before safety acceptance will take place. The review of the Safety File as part of the report will be coordinated with the Safety IPT Lead. During the assembly, integration, verification, and commissioning periods, the Safety Compliance Assessment report may require update by the Project Team, (advised by the IPT Lead and Safety IPT Lead). The final version is signed by the IPT lead and the ngVLA Project Director as part of the acceptance procedure.

A CE-marked and/or UL-listed product does not require an ngVLA SCA for the product itself but must be included as a subsystem in the Risk Analysis procedures of the whole design. Therefore, all product related safety certifications must be available. It is acceptable to generate an SCA and formally certify project acceptance for the first shipment only, provided that subsequent identical units conform to the same design and manufacturing controls. It is the responsibility of the IPT Lead to ensure items procured outside of the ngVLA project are used in the manner intended, and safety certified/compliant.

The Safety Compliance Assessment will result in a report certifying that the design, product, work activity, machinery, or design has been designed, built, and operated in accordance with applicable safety regulations. Each SCA will ensure that a statement of conformity is prepared and provided to the Safety File.

5.5 System Hazard Analysis (SHA)

The System Hazard Analysis is conducted by the Systems Engineering IPT and is based on the documentation provided by the IPTs. The System Hazard Analysis is used to look at the design as a whole in the event that a hazard is introduced when individual subsystem components are placed in service together.

5.6 Safety Review and Documentation

If appropriate, an inspection will be made at the site where the product is being tested. The product should be fully operational. This implies that the review should be held with a time margin sufficient to organize a second review or take corrective action in case safety relative deficiencies are found. The chief product responsible individuals (i.e. group leader, engineers responsible for mechanics, handling tools, electronics and cryogenics as well as documentation, drawings etc.) should be available in case points must be clarified. Normally, the review team shall consist of at least the person responsible to organize the safety review and an appropriate engineer. Internal or external experts may be added when necessary or a separate review arranged.

After the inspection, the IPT lead shall receive a report from the IPT safety liaison on the safety review of the instrument and the Safety File. Any missing or incomplete documentation, additional tests, necessary modifications and areas of concern shall be pointed out and remedial measures suggested to ensure safety during installation, commissioning and operation of the product. If the safety review is satisfactory, the final safety documents will be presented to the ngVLA Project Director and released. The ngVLA Project Manager as well as the Safety IPT Lead will receive a copy of the safety review report and the safety documents prepared for the final acceptance.

Safety inspections or reviews shall be scheduled with the Safety IPT Lead with sufficient time to organize a subsequent review or take corrective action where safety related deficiencies are found. The instrument/product must be fully operational and integrated for the safety review. About one to two weeks should be reserved for the review with no other major modifications of the (sub) system. The IPT Safety Liaison should be available to clarify any questions. Internal and external experts may be added when necessary.

The Risk Analysis process will result in the assembly of a Safety File, which contains all safety-relevant information. Documentation of standard operating and maintenance procedures for each phase in the lifecycle of the design including manufacture, installation, testing, operation, environmental influence, and disposal and decommissioning is a requirement. The top-level document in the Safety File is the Safety Compliance Assessment report that results from the Safety Compliance Assessment (Section 9).

6 Risk Estimation

All hazards, hazardous conditions and hazardous events associated with the design shall be identified. To identify hazards not previously recognized, additional methods covering the specific situation should be used. These may include use of working groups and brainstorming, surveys and interviews, experiential or documented knowledge, outputs from "what if" scenario analyses, historical information, and lessons learned.

The Preliminary Hazard Checklist (Section 7.3) provides a more detailed checklist for use in consideration in the hazard identification. Hazard verification includes all activities performed to demonstrate that the design meets or is capable of meeting the specified safety requirements.

6.1 Hazard Severity Categories

The following hazard severity categories are defined to provide a qualitative measure for mishap classification.

Category	Severity Description	Mishap Definition
1	Catastrophic	Death and/or the instrument is more than 4 weeks out of operation or it cannot be recovered at a reasonable cost.
2	Critical	Severe injury, severe occupational illness, and/or the instrument can be repaired, but support from the supplier/industry is necessary and/or the instrument is up to 4 weeks out of operation.
3	Marginal	Minor injury, minor occupational illness, and/or the instrument can be repaired by ngVLA staff, and/or the instrument is up to one week out of operation.
4	Negligible	Less than minor injuries, less than minor occupational illness, and/or the instrument is less than one day out of operation.

Table 1 - Probability of hazard occurrence.

6.2 Hazard Probability Levels

The probability that a hazard will occur during the total lifetime of an instrument is defined in the following form:

Level	Probability Description	Definition
A	Frequent	Likely to occur more than once per year
B	Probable	Will occur 6 to 10 times during the total lifetime
C	Occasional	Will occur 2 to 5 times during the total lifetime
D	Remote	Unlikely but possible to occur once during the total lifetime
E	Improbable	So unlikely that an occurrence can be assumed not to be experienced.

Table 2 - Severity of occurrence.

Type	Description
O	Occupational exposure, i.e. hazard has potential impact only for workers in immediate area.
F	Could impact workers in the facility but not likely to impact the outside environment.
E	Hazard that could have environmental consequences, e.g., a solvent spilled in large enough quantities to cause environmental pollution outside the facility.
P	Hazard that could have consequences to the off-site public.

Table 3 - Scope of hazards.

6.3 Risk Acceptance/Rejection Criteria

Figure 1 prioritizes identified hazards for corrective actions and clearly indicates those hazard risk levels which are unacceptable to AUI/NRAO.

Frequency of Occurrence	Hazard Categories				Accept/Reject Criteria
	Catastrophic	Critical	Marginal	Negligible	
Frequent	1A	2A	3A	4A	Unacceptable
Probable	1B	2B	3B	4B	Undesirable; NRAO decision required.
Occasional	1C	2C	3C	4C	Acceptable with NRAO review.
Remote	1D	2D	3D	4D	Acceptable without NRAO review.
Improbable	1E	2E	3E	4E	Acceptable without NRAO review.

Figure 1 - Risk acceptance and rejection criteria, indicating hazard risk levels and follow-up if needed.

7 Risk Analysis Procedure

7.1 Preliminary Hazard List (PHL)

Instructions to Fill Out the Preliminary Hazard List

1. Every product or item (article, unit, etc.) for the ngVLA project must have a completed Preliminary Hazard List (PHL) using the following checklist-based approach.
2. The IPT safety liaison, or a designee, must examine the unit and identify the possible hazards inherent in the design.
3. If there are issues not indicated in the hazard list, describe those at the bottom of the form.
4. The column labeled “Probability” is the probability that a hazard will occur during the instrument life.
5. The column labeled "Severity" is intended to allow a subjective seriousness rank of the hazard.
6. The column labeled “Scope” is used to indicate the scope of the hazard as follows. Enter all letters that apply.
7. Comment on the means to avoid or limit the harm and the severity of harm.

Preliminary Hazard List

Date_____ Version _____ Responsible IPT_____

Describe the unit(s):

_____

_____

Describe any subsystems identified, and the boundaries or interfaces between them:

_____

_____

Describe safety features or controls:

_____

_____

_____

List all design source documents used, including versions, dates:

_____

_____

_____

7.2 Preliminary Hazard Checklist Procedure

Use Table 1, Table 2, and Table 3 to fill out the Hazard Checklist.

7.3 Preliminary Hazard Checklist

Potential Hazard	Severity	Probability	Scope	Comments
Mechanical Hazards (article, parts, or work piece)				
Overall article, items for consideration: a) shape b) relative location c) mass and stability (potential energy of elements which may move under the effect of gravity) d) mass and velocity (kinetic energy of elements in controlled or uncontrolled motion) e) inadequacy of mechanical strength f) elastic elements (springs) g) liquids and gases under pressure h) the effect of vacuum				
Crushing hazard				
Shearing hazard				
Cutting or severing hazard				
Entanglement hazard				
Drawing-in or trapping hazard				
Impact hazard				
Stabbing				
Friction or abrasion hazard				
High pressure fluid injection or ejection hazard				
Electrical Hazards				
Low voltage/high current				
Exposed 115 V, 230 V				
Approach to live parts under high voltage				
High voltage/power				
Stored energy/capacitors/inductors				
Electrostatic discharge including lightning				
Battery electric shock				
Contact of persons with live parts (direct contact)				
Contact of persons with parts which have become live under faulty conditions (indirect contact)				
Other: projection of molten particles and chemical effects from short circuits, overloads, etc.				
Thermal Hazards				
Radiation of heat sources (high temperature equipment)				
Battery bank and UPS equipment				
Flames or explosions				

Hazards Generated by Noise resulting in:				
Hearing loss (deafness), other physiological disorders (e.g., loss of balance, loss of awareness)				
Interference with speech communication, acoustic signals				
Hazards Generated by Vibration				
Use of hand-held machines resulting in a variety of neurological and vascular disorders				
Whole body vibration, particularly when combined with poor postures				
Hazards Generated by Radiation				
X and gamma rays				
Lasers				
Low frequency, radio frequency radiation, microwaves				
Intense light sources				
Radiation check sources				
Hazards Generated by Materials and Substances (and their constituent elements)				
Hazards from contact with or inhalation of harmful fluids, gases, mists, fumes, and dusts				
Fire and explosion hazard				
Biological and microbiological (viral and bacterial) hazards (i.e. water)				
Hazards Generated by Neglecting Ergonomic Principles in Design as, e.g., hazards from:				
Unhealthy postures or excessive effort				
Inadequate consideration of hand-arm or foot-leg anatomy				
Neglected use of personal protection equipment				
Inadequate local lighting				
Mental overload and underload, stress and strain				
Human error, human behavior				
Inadequate design or location of visual display units				
Repetitive motion				
Unexpected Start-Up, Unexpected Overrun/Overspeed (or any similar malfunction) from:				
Failure/disorder of the control system				
Restoration of energy supply after an interruption				
External influences (gravity, wind, etc.)				
Errors in the software				
Errors made by the operator (due to mismatch of machinery with human characteristics and abilities)				
Systems redundancy and diversity				
Interlocks				

Potential Hazard	Severity	Probability	Scope	Comments
Operating, Test, Maintenance, and Emergency Procedures				
Human factors considerations				
Adequacy and effectiveness of instruction, training				
User error, including failure to activate				
Effect of factors such as equipment layout, ergonomics and lighting				
Crash safety, egress, rescue and survival				
Variation in the speed of tools				
Impossibility of stopping in the best possible condition				
Mechanical Hazards and Hazardous Events				
Loading/unloading (i.e. load falls, collisions, machine tipping)				
Emergency response/spill clean-up				
Packaging hazardous materials				
Bad road conditions (e.g., icy)				
Uncontrolled amplitude of movements				
Inadequate holding devices/accessories				
Insufficient mechanical strength of parts				
Inadequate design of pulleys, drums				
Inadequate selection of technical equipment and accessories and their inadequate integration				
Abnormal conditions of assembly/testing/use/maintenance				
Motion Hazards				
Falling of person from person carrier				
Moving vehicles, carts, forklifts				
Material grinding, cutting, drilling				
Work with roads and grounds equipment				
Powered platforms				
Overspeed of person carrier				
Chemical Hazards				
Acids, solvents, toxic agents and hazardous liquids				
Heavy metals such as lead				
Chemical reactions				
Toxicity in smoke or fumes				
Welding fumes				
Carbon monoxide				
Carcinogens				
Chemical exposure				

Potential Hazard	Severity	Probability	Scope	Comments
Personnel Hazards/ Hazards Generated by Neglecting Ergonomic Principles				
Vacuum tanks				
Pinch hazards				
Confined spaces /insufficient means for evacuation/emergency exit				
Restricted movement of persons				
Lifting/carrying heavy objects				
Working at heights				
Slips, trips & falls				
Hazards requiring PPE				
Inadequate seating				
Inadequate lighting				
Insufficient visibility				
Inadequate location of manual controls				
Lack or inadequacy of visual or acoustic warning means				
Construction Hazards				
Heavy equipment				
Possibility of hitting utilities				
Scaffolding				
Ladder				
Compressed gas				
Earth moving equipment				
Material Handling Hazards				
Ejected objects				
Cranes & hoists				
Fork lift operation				
Chemical spills				
Falling objects				
Hazardous tools, equipment and machinery				
Storage/handling of toxic materials				
Environmental Hazards				
Hazardous waste				
Surface water discharges				
Endangered species issues				
Archeological requirements				
Regulated chemical wastes				
Groundwater protection				
Ozone depleting substances				
Sewer discharges				
Drinking water quality				

Potential Hazard	Severity	Probability	Scope	Comments
Fire Hazards				
Electrical				
Flammable substances, solid, liquid or gaseous				
Welding				
Spark producing tools near combustibles				
Spontaneous combustion				
Storage of combustibles				
Mobile structures (portakamps)				
Transportation (rail/vehicle fueling)				
Boiler, furnace, heating systems and appliances				
Stationary combustion engines				
Oxygen Deficiency Hazards				
Cryogenic spills				
Cryogenic gas or liquid leak				
Chemical spills				
Leak of supplied gases				
Hazardous Components				
Explosives				
Asphyxiants, toxic or corrosive substances				
Hazardous construction materials				
Pressure systems				
Hydraulic machinery				
Other energy sources including motion				
Hazardous surfaces				
Factors Due to Operating Domain, or that the System May Add to the Operating Domain				
Drop				
Shock and vibration, including seismic				
Extreme pressures and climatic conditions				
Noise				
Exposure to toxic or corrosive substances				
Adequacy of Safety Related Equipment, Safeguards, and Failure Containment Measures				
Fire suppression systems				
Relief valves				
Energy containment vessels				
Electrical protection				
Toxic substance control				
Electrical, air and hydraulic supplies				
Personal protective equipment				
Ventilation				
Noise or radiation barriers				
Alarms and warnings				

7.4 PHL Acceptance Criteria

Are there any hazards identified as UNACCEPTABLE, UNDESIRABLE, or ACCEPTABLE WITH REVIEW?

☐ If YES, do NOT sign the next section; go to Section 8 – Preliminary Hazard Analysis.

☐ If NO, proceed to the next section (Section 7.5 – PHL Signatures).

Acceptance Criteria

Frequency of Occurrence	Hazard Categories				Accept/Reject Criteria
	Catastrophic	Critical	Marginal	Negligible	
Frequent	1A	2A	3A	4A	Unacceptable
Probable	1B	2B	3B	4B	Undesirable, NRAO decision required.
Occasional	1C	2C	3C	4C	Acceptable with NRAO review.
Remote	1D	2D	3D	4D	Acceptable without NRAO review.
Improbable	1E	2E	3E	4E	Acceptable without NRAO review.

7.5 PHL Signatures

The following signatures certify that no unacceptable hazards were identified in the PHL of the unit described in this document. File copies of this document with the Safety IPT, SE IPT, and maintain a copy for the generating IPT. Go to Section 8.3 – Preliminary Hazard Analysis (PHA) Form.

Title	Signature
IPT Lead	
IPT Safety Liaison	

The following signature(s) indicate that the PHL has been reviewed and the Safety File initiated.

Title	Signature
Safety IPT Lead	

8 Preliminary Hazard Analysis (PHA)

8.1 Instructions for Completion of the PHA

1. The IPT is responsible to complete the PHA. Obtain all available information about the functional and operational requirements. Then break down the unit into subsystems or component operations.
2. For each hazard identified, assign a unique numeric identifier. Proper hazard identification requires consideration of the items listed in the Preliminary Hazard List.
3. Describe the hazard source. A hazard source is the source that generates or causes the hazard. For example, a hazard of engine repair operations is carbon monoxide; carbon monoxide is the source that generates the hazard.
4. Cause factors create or significantly contribute to the hazard. In this case, failure to provide adequate exhaust ventilation is one potential cause factor. Another might be failure to control generation of CO by running internal combustion engines or failure to provide workplace monitoring to detect carbon monoxide levels. All identified cause factors should be listed.
5. Describe potential effects in terms of the path between the source and the object that requires protection. The effect of inhaling CO, which enters the bloodstream and interferes with the delivery of oxygen to the tissues, can lead to death or serious injury.
6. If not previously done in the PHL, assign a hazard category, which is a determination of the hazard's severity and probability of occurrence. For this example, a Risk Index of 2A would be assigned based upon the high severity and probability factors associated with this hazard.
7. Prioritize Means for Prevention or recommendations on controlling the hazard by concentrating on the energy source first and then following points along the flow or path of the energy. In this way, last efforts are directed at the item or person requiring protection. This might be reflected in the example by first recommending that internal combustion engines be replaced by electric motors, which remove the energy source (and hazard) altogether.

8.2 Preliminary Hazard Analysis Form

Describe the unit:

_____

_____

Describe any hazardous components (e.g., electrical systems, cooling fluids, toxic substances, hazardous construction materials, pressure systems, lasers, and other energy sources):

_____

_____

Describe environmental constraints including transport, handling and operating environments, (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, and pressure):

_____

_____

_____

_____

Describe safety related considerations of the design and design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, or designated undesired events).

_____

_____

_____

Describe operating, testing, maintenance, and emergency procedures.

_____

_____

_____

Detail facilities, support equipment (e.g., provisions for storage, assembly, checkout, proof-testing of hazardous designs/assemblies which may include toxic, flammable, corrosive or cryogenic fluids; electrical power sources) and training (e.g., training and certification pertaining to safety operations and maintenance) requirements.

Identify any environmental constraints including transport, handling and operating environments,(e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, and pressure).

8.3 Preliminary Hazard Analysis (PHA) Summary Form

UNIT DESCRIPTION (name and number) _____

Number	Hazard Source	Cause Factors	Effects/ Severity	Severity	Occurrence Probability	Risk Index	Means for Prevention	Actions/ Remarks
(EXAMPLE) 1a	*Carbon Monoxide*	*Failure to control CO emissions*	*Inhalation can cause loss of consciousness or death*	*Category A – Frequent*	*Category 2 – Critical*	*2A*	*Replace internal combustion engines with electric motors.*	
(EXAMPLE) 1b	*Carbon Monoxide*	*Failure to provide adequate exhaust ventilation*	*Inhalation can cause loss of consciousness or death*	*Category A – Frequent*	*Category 2 – Critical*	*2A*	*Install and test exhaust ventilation.*	
(EXAMPLE) 1c	*Carbon Monoxide*	*Failure to monitor for CO in the workplace*	*Inhalation can cause loss of consciousness or death*	*Category A – Frequent*	*Category 2 – Critical*	*2A*	*Provide CO monitors.*	

8.4 PHA Acceptance Criteria

Are there any unmitigated hazards identified in the PHA as UNACCEPTABLE, UNDESIRABLE, or ACCEPTABLE WITH REVIEW?

☐ **YES**, do NOT sign the next section; go to Section 8.6 – PHA Risk Acceptance.

☐ **NO**, proceed to Section 8.5 – PHA Signatures.

8.5 PHA Signatures

The following signatures certify that all identified hazards have been mitigated to acceptable levels. This review incorporated the hazards identified in the PHL. File copies of this document with the Safety IPT and SE IPT, and maintain a copy for the generating IPT.

Title	Signature
IPT Lead	
IPT Safety Liaison	

The following signature(s) indicate that the PHA has been reviewed and the Safety File initiated.

Title	Signature
Safety IPT Lead	

8.6 PHA Risk Acceptance

The following signatures acknowledge that the identified risks have been mitigated to the extent feasible. Any identified residual risks must be addressed with personnel training, protective equipment, and other administrative procedures. Proceed to Section 9 – Safety Compliance Assessment.

Title	Signature
IPT Lead	
Safety IPT Lead	
ngVLA Project Director	

9 Safety Compliance Assessment (SCA)

9.1 Instructions for Completion of the SCA

1. The IPT is responsible for performing the Safety Compliance Assessment, including a review of design drawings, procedural reviews, and equipment inspections.
8. Identify contractual safety specifications, standards, and codes applicable to the design and document compliance of the design and procedures with these requirements.
9. A CE-marked and/or UL-listed product does not require an ngVLA SCA for the product itself but must be included as a subsystem in the Risk Analysis procedures for the whole design. Therefore, all product-related safety certifications must be available.
10. It is acceptable to generate an SCA and formally certify project acceptance for the first shipment only, provided that subsequent identical units conform to the same design and manufacturing controls.
11. It is the responsibility of the IPT Lead to ensure items procured outside of the ngVLA project are safety certified and compliant.
12. Conclude with a signed statement that all identified hazards have been eliminated or their associated risk minimized to levels contractually specified as acceptable.
13. Each SCA will ensure that the signed statement is prepared and provided to the Safety File.

The signed statement or declaration of conformity is the procedure by which the manufacturer (or IPT) declares that the machinery complies with all the applicable essential health and safety requirements.

Before drawing up the declaration of conformity, ensure and be able to guarantee that the documentation listed below is available for inspection:

- An overall drawing of the machinery together with drawings of the control circuits,
- Full detailed drawings, accompanied by any calculation notes, test results, etc., required to check the conformity of the machinery with the essential health and safety requirements,
- The essential requirements of the standards, and other technical specifications, which were used when the machinery was designed,
- A description of methods adopted to eliminate hazards presented by the machinery,
- If desired, any technical report or certificate obtained from a competent body or laboratory,
- Any technical report giving the results of tests carried out at either by the designer or by a competent body or laboratory,
- A copy of the instructions for the machinery.
- For series manufacture, the measures that will be implemented to ensure that the machinery remains in conformity.

9.2 Statement of Compliance or Declaration of Conformity

The IPT declares that the supplied model of…

_____

_____

Description of machinery or machinery part, i.e. make, type, serial number, and where applicable, additional details relevant to its type and safe use.

…is intended to be incorporated into machinery or assembled with other machinery to constitute machinery and is in conformity with the article, device, or component specified safety requirements.

Other regulations or directives taken into account…

_____

_____

If parts are covered by other directives or regulations, these shall also be listed.

Applied harmonized standards:

_____

_____

Where applicable, not mandatory. National standards and/or technical specifications may also be cited here.

_____

Signature/Date

Signature of person who signed on behalf of the IPT, manufacturer, or his/her authorized representative(s).

File copies of this document with the Safety IPT, SE IPT, and maintain a copy for the generating IPT.

END of RISK ANALYSIS unless notified by the SE IPT.

10 Appendix

10.1 Abbreviations and Acronyms

Acronym	Description
AD	Applicable Document
CDR	Critical Design Review
ICD	Interface Control Document
IPT	Integrated Product Team
ngVLA	Next Generation VLA
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
RD	Reference Document
RFI	Radio Frequency Interference
SCA	Safety Compliance Assessment
SHA	System Hazard Analysis
SE	Systems Engineering
TBD	To Be Determined
VLA	Jansky Very Large Array