EUROPEAN SOUTHERN OBSERVATORY
Organisation Européenne pour des Recherches Astronomiques dans l'Hémisphère Austral
Europäische Organisation für astronomische Forschung in der südlichen Hemisphäre

VERY LARGE TELESCOPE

MACAO-VLTI

Detailed Hazard List and Hazards Analysis

Doc. No.: VLT-LIS-ESO-15600-2466
Issue 1.1
Date: 8.03.01

Prepared: R. Arsenault . . . .

Name Date Signature

Approved: N. Hubin . . . .

Name Date Signature

Released: G. Monnet . . . .

Name Date Signature

Contributors: J. Brynnel, R. Donaldson, C. Dupuy, E. Fedrigo, M. Kasper

VLT PROGRAMME * TELEPHONE: (089) 3 20 06-0 * FAX: (089) 320 2362

″

CHANGE RECORD

Issue	Date	Section/Page Affected	Reason/ Remarks
1.0	03/01/01	All	First issue

″

TABLE OF CONTENTS

″

List of Acronyms

ADn	Applicable Document No. n
AIV	Assembly, Integration and Verification
AO	Adaptive Optics
CTC	Cabinet Thermal Control
DM	Deformable Mirror
ESO	European Southern Observatory
FDR	Final Design Review
FOV	Field of View
HD	Hardware Deliveries
I/F	Interface
ICS	Instrument Control Software
ISS	Interferometer Software Superviser
LCU	Local Control Unit
MLE	Maximum Likely Earthquake
OPD	Optical Path Difference
OS	Observing Software
PDR	Preliminary Design Review
PS	Power Supply
RDn	Reference Document No. n
RTC	Real-Time Computer
RTCS	Real-Time Computer Software
SCP	Service Connection Point
SW	Software
TBC	To Be Confirmed
TBD	To Be Defined
TTM	Tip Tilt Mount
UPS	Uninterruptible Power Supply
UT	Unit Telescope
VLT	Very Large Telescope
VLTI	Very Large Telescope Interferometer
VLTISS	Very Large Telescope Interferometer Supervisory Software
WFS	Wave Front Sensor
WS	WorkStation

″

1. SCOPE

This document presents an exhaustive list of Hazards that can cause human injury or substantial instrument damage. In the second part of this document, an analysis of these hazards is performed.

2. REFERENCE DOCUMENTS

The following documents describe the complete design of MACAO-VLTI and have been consulted in order to build the hazard list and to perform the analysis.

	Top-Level Requirements For MACAO-VLTI	VLT-SPE-ESO-15600-2082	v1.2	8.03.2001
	MACAO VLTI Technical Specifications	VLT-SPE-ESO-15600-2245	v1.1	9.03.00
	MACAO VLTI Draft Maintenance Plan	VLT-PLA-ESO-15600-2521	v1.0	Date: 9.03.00
	MACAO-VLTI System Overview	VLT-TRE-ESO-15600-2251	v1.2	15-02-2001
	MACAO-VLTI System Design Analysis	VLT-TRE-ESO-15600-2067	v2.1	02.02.01
	MACAO-VLTI Detailed mechanical design and Analysis report of the Coude AO facilities	VLT-TRE-ESO-15600-2274	v2.0	12.03.01
	MACAO VLTI Electronics – Overview	VLT-TRE-ESO-15600-2268	v2.0	6-Mar-2001
	Macao VLTI Electronics APD	VLT-TRE-ESO-15600-2269	v2.0	06-03-01
	MACAO VLTI Electronics - DM Control	VLT-TRE-ESO-15600-2271	v2.0	6-Mar-2001
	MACAO-VLTI Instrument Control Electronics (LCU)	VLT-TRE-ESO-15600-2270	v2.0	5.03.01
	Effect of DM Dynamics on MACAO Performance	VLT-TRE-ESO-11640-2429	v1.0	31/12/2000
	MACAO-VLTI Wavefront Sensor Optics	VLT-TRE-ESO-15600-2273	v2	15-02-2001
	MACAO Lenslet Array Unit Design Report	VLT-TRE-ESO-11640-2451	v1.0	30.01.2001
	MACAO-SoftwareDesign-ICS	VLT-SPE-ESO-15600-2440	v1.0	12/02/2001
	MACAO-VLTI Software Design – OS	VLT-SPE-ESO-15600-2439	v1.0	12-2-2001

″

	MACAO-VLTI Real-Time Computer Software Design	VLT-SPE-ESO-11640-2352	v1.1	28.02.01
	MACAO-VLTI Software Functional Specs – RTC	VLT-SPE-ESO-15600-2062	v1.2	15.02.01
	Assembly Integration and Tests Plan for MACAO-VLTI	VLT-PLA-ESO-15600-2241	v2.0	14.03.01
	MACAO-VLTI Tip-Tilt-Mirror FEM Analysis	Technical note		7.03.01
	Optical path difference sensors	ONERA		2001-03-08
	Studies on MACAO Software Specifications: Piston Removal from Bimorph Control (WP1),	ONERA		03/2001
	MACAO-VLTI Tip-Tilt Mount Final Design Report	VLT-TRE-ODP-11640-0002	v1.0	22/02/01
	MACAO-VLTI Deformable Mirror Design Report	CILAS		28.02.01
	Technical Specification for the MACAO WFS Lenslet Array Unit	VLT-SPE-ESO-11640-2146	v2.1	02.02.2001
	MACAO Technical Specifications and Statement of Work for the Two Micro Lenslet Arrays	VLT-SPE-ESO-11640-2146	v1.0	02.02.2001
	Technical Specification and Statement of Work for the MACAO Tip-Tilt Mount	VLT-SPE-ESO-11640-2147	v1.1	22-11-2000
	MACAO-VLTI Optical Derotator: Technical Specifications and Statements of Work	VLT-SPE-ESO-15600-2413	v1.0	30.11.00
	MACAO-VLTI Beam Expander: Technical Specifications and Statements of Work	VLT-SPE-ESO-15600-2414	v1.0	1.12.00
	MACAO for VLTI Technical Specifications for the Detailed Design, Fabrication, Assembly and Acceptance tests of the four WFS X-Y Tables of the Coude AO Facilities	VLT-SPE-ESO-15600-2392	v1	28.11.00
	Scope of Work for the Detail Design, Construction, Assemblying, Test & Shipment of the Four WFS X-Y tables for the Coude AO Facilities	VLT-SOW-ESO-15600-2393	v1	28.11.00
	Technical Specification ESO Adaptive	VLT-SPE-ESO-11640-1943	v2.3	14.11.00

″

	Optics System Deformable Mirror Control			
	Technical Specification MACAO APD Counter Module	VLT-SPE-ESO-11640-2262	v1.0	3.08.00
	MACAO-VLTI Deformable Mirrors Technical Specifications	VLT-SPE-ESO-15600-2064	v1.1	7.09.00
	MACAO-VLTI Technical Specification X-Y Table	VLT-SPE-ESO-15600-2126	v1.1	18.09.00

3. INTRODUCTION

The MACAO VLTI consists in four (4) AO modules installed at the Coudé focus of each UT. It shall correct the wavefront coming from the telescopes from atmospheric turbulence, before recombination of the beams in the interferometric laboratory of the VLTI.

In the following we will propose a list of all the potential safety hazards to persons or to the integrity of the instrument. In order to build this list, we will proceed as follow:

- The analysis will be performed by "experts" in the field, in particular the designer team,
- Each "branch" of MACAO-VLTI product tree will be considered,
- For each "branch", the effect hazards will be considered:
  - Mechanical
  - Electrical
  - Thermal
  - Noise
  - Vibration
  - Radiation
- In addition to the above, we will consider the potential dangers generated by:
  - Contact with fluids, gasses, fumes
  - Fire and explosion
- Also, the numerous environmental and design constraints often lead to compromises on ergonomic principles. We will consider:
  - Physiological effects
  - Psycho-physiological effects
  - Human errors

Some time will be spend to see if obvious combinations of the above might lead to a safety hazard. The MACAO-VLTI is a series of 4 identical systems. We perform the analysis on a single unit and it is legitimate to claim that the risks are identical for all four units. On the other hand, we do not believe that the simultaneous use of more than one unit at a time can generate other types of hazard than the ones of a single system.

We do not take into account in this analysis, the hazards which can take place outside of the Telescope building. We assume that Paranal staff follow strict safety rules and standard procedures in the various operations related to transportation of the material. Therefore, these issues will not be analyzed here.

4. HAZARD SEVERITY AND CATEGORIES

In a second step a hazard analysis will be performed. The following hazard severity categories will provide a qualitative measurement for the hazard classification.

Category	**Description**	**Definition**
1	Catastrophic	Death and/or 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 ESO 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

We also define a hazard probability level. They provide a qualitative measurement for hazard classification.

Level	**Definition**	**Description**
A	Frequent	Likely to occur more than once per year
B	Probable	Will occur 6 to 10 times during the whole 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

From the combination of hazard severity and hazard probability we define the following Acceptance/Rejection 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
Occasional	1C	2C	3C	4C	Acceptable (review)
Remote	1D	2D	3D	4D	Acceptable
Improbable	1E	2E	3E	4E	

In other words, all hazards leading to a criteria 1A, 2A, 3A, 4A, 1B, 2B, 3B, 1C and 2C must be dealt with. This means a corrective action must be taken to insure non-occurrence of these. Generic solutions include: change in design, interlocks, alarms, well-defined procedure etc.

In the following analysis, the probability and severity criteria are assessed for the actual design of MACAO-VLTI.

″

5. MACAO-VLTI PRODUCT TREE

MACAO-VLTI Product Tree v1.0 (R. Arsenault 7.12.00)

- MACAO-VLTI 15600
  - 100000: X-Y Table
  - 110000: T-Mount
  - 120000: Beam Exchanger Unit
  - 130000: Optics
  - 140000: Strap System
  - 150000: De-Rotator Prism
  - 160000: TCCD mechanical I/F
  - 200000: Electronics
    - 210000: IC Electronics
    - 220000: RTC Electronics
    - 230000: DM Electronics
    - 250000: APD Counters
  - 300000: Corrective Optics
    - 310000: TTM Assembly
      - 311000: TTM mechanical I/F
      - 312000: TTM Mount
      - 313000: TTM FE
      - 314000: TTM SU Rack
    - 320000: DM Assembly
  - 400000: Test Tools
    - 410000: IR Test Camera
    - 420000: IR Lab. Camera
    - 430000: Test Bench
    - 440000: Turbulence Generator

″

6. HAZARD LIST

Hazards can occur during various phases of the life cycle of the instrument. The ones being analyzed here are:

1. transport and installation within the VLT building
2. assembly & integration at the Coudé focus
3. maintenance & debugging operations
4. normal observing mode

6.1. MACAO-VLTI MECHANICAL ASSEMBLY

In this section we consider the main mechanical parts of the MACAO-VLTI WFS assembly. These are all components at the head of the product tree:

- 100000: X-Y Table
- 110000: T-Mount
- 120000: Beam Exchanger Unit
- 130000: Optics
- 140000: Strap System
- 150000: Derotator Prism
- 160000: TCCD & I/F

All the mechanical parts listed above are assembled on a single mount and performs as a single unit. The analysis will be performed on this unit. The whole can be moved with the XY table. Also, the beam exchanger unit consists of several optical components mounted on a stage. Finally, the whole assembly is located under the M9 tower on the Coudé platform.

6.1.1. Hazard List for WFS Assembly

No.	Hazards	Phase
WFS1	Fall of WFS assembly during handling, human injury or damage to instrument	Transport/installation
WFS2	Fall during assembly, human injury or damage to instrument	assembly
WFS3	Fall of tools onto the WFS assembly, instrument damage	Assembly/integration or maintenance
WFS4	Crushing of part or person between WFS assembly and M9 tower pilars	Maintenance or integration
WFS5	Crushing of part or person within the structure of the XY table	Maintenance or integration

″

WFS6	Tearing of cables, optical fibers, fluid pipes during displacement of WFS assembly	Normal operation, maintenance or integration
WFS7	Abrasion of electric cables or fluid pipes	Normal operation, maintenance or integration
WFS8	Cooling fluid leak, damage to components	Normal operation, maintenance or integration
WFS9	Noise by the 2 kHz membrane mirror; annoyance leading to human fatigue, stress, hindered verbal communication	Integration or maintenance
WFS10	Human fatigue, back injuries due to low-lying apparatus (on floor)	Assembly/integration and maintenance
WFS11	Head injuries due to low-lying structure above apparatus (M9 tower, IR Test camera)	Assembly/integration and maintenance
WFS12	Damage to optical surfaces	Assembly/integration and maintenance
WFS13	Obstructed diaphragm over membrane	Integration and maintenance
WFS14	Obstructed shutter	Integration and maintenance
WFS15	Obstructed density wheel	Integration and maintenance
WFS16	Driving XY table with brake applied	Integration, maintenance and operation
WFS17	Driving linear motion beyond limit	Integration, maintenance and operation
WFS18	Too high amplification on membrane	Integration
WFS19	Earthquake	Any phase

6.2. 200000: ELECTRONICS

The product tree for electronics components includes the following:

- 210000: IC-LCU cabinet
- 220000: RTC-LCU cabinet
- 230000: DM/TTM cabinet
- 240000: APD cabinet

The DM/TTM electronic cabinet (230000) is located on the azimuth platform, all others are on the Coudé platform.

No.	Hazards	Phase
ELE1	Fall of cabinet, human injury and	Transport/installation

″

	instrument damage	
ELE2	Fluid leak within cabinet, damage to electronic racks within cabinets (short-circuit and/or overheating)	Integration, normal operation
ELE3	Fluid leak in TTM/DM cabinet on azimuth platform, leak in Coudé room	Integration, normal operation
ELE4	Electrocution, HV in DM/TTM electronic cabinet	Integration maintenance
ELE5	APD over illumination	Integration and operation
ELE6	Short circuit	Integration
ELE7	Loss of electrical power	Operation, integration and maintenance
ELE8	Electrostatic discharge	Assembly Integration and maintenance
ELE9	Fiber bundle damage	Assembly Integration and maintenance
ELE10	Earthquake	Any phase

6.2.1. 300000: Corrective Optics

The corrective optics subsystem includes the tip-tilt mount (TTM) and the deformable mirror (DM). The DM is mounted within the TTM, and the unit is mounted on a mechanical I/F with the M8 tower. The whole unit is physically located in one place.

No.	Hazards	Phase
COR1	Fall of parts from the M8 tower, human injury, instrument damage to TTM/DM, or/and M9 tower, dichroic telecentricity lens	Assembly/integration, maintenance
COR2	Fall of tools “ “ “	Assembly/integration, maintenance
COR3	Fall of persons from the M8 tower installation	Assembly/integration, maintenance
COR4	Human minor injury, heavy parts to manipulate	Assembly/integration, maintenance
COR5	Electrocution, HV on DM	Assembly/integration, maintenance
COR6	Damage to optical surfaces	Assembly/integration, maintenance
COR7	Vibration	Operation, maintenance and integration
COR8	DM enters in resonance	Integration and Operation
COR9	TTM enters in resonance	Integration and Operation
COR10	Earthquake	Any phase

″

7. DETAILED HAZARD ANALYSIS

In the previous section we listed all potential hazards. This section deals with the severity of these on the grounds of how critical they are and their probability of occurrence as described in section 4. The column "Residual Risk" takes into account the actual design aspects of MACAO-VLTI that reduces this index to an acceptable level.

7.1. HAZARD ANALYSIS FOR WFS ASSEMBLY

No	Hazard source	Hazardous mode	Effects	Sev.	Occ. Prob	Prevention	Residual Risk	Action/Remark
WFS1	Fall of WFS assembly during Handling	Transport within VLT building	• Damage to physical integrity of assembly • Human injury	1-2	E	Proper handling procedure and qualified personal	1E	There is proper handling points on T-mount
WFS2	Fall of WFS assembly during handling	Assembly under M9 tower	• Damage to physical integrity of assembly • Human injury	2	E	Proper handling procedure and qualified personal	2E	Final location is on the ground; potential energy during handling low
WFS3	Fall of tools onto WFS assembly	Maintenance, assembly of WFS or M9/Telecentric lens or M8 tower; Assembly/Integration of WFS	Damage to instrument	3	D	Adequate procedure; covers on WFS assembly when work on M9 tower. No tools resting on surface above WFS assembly	3D	
WFS4	Crushing person or part between M9 pillar and	XY table operational means during integration	• Damage to instrument	1	E	Interlock; XY table disabled during maintenance	1E	Slow movement; time to react to avoid personal injury

″

	WFS	or maintenance	• Human Injury					
WFS5	Crushing part or person within the structure of XY table	Implies XY table operational and T-mount not on; assembly or maintenance	• Damage to instrument • Human Injury	1	E	Interlock; XY table disabled during maintenance	1E	Slow movement; time to react to avoid personal injury
WFS6	Tearing of cables	During integration or maintenance	Cables destruction/damage	4	C	Emergency switch	4C	Slow movement; time to react to avoid damage
	Tearing of cables	During normal operation	Cable destruction/damage	4	D	Proper routing of cables; clear procedure for cabling	4D	
	Tearing of optical fibers	During integration or maintenance	Fibers destruction/damage	2	C	Emergency switch	2C	Slow movement; time to react to avoid damage
	Tearing of optical fibers	During normal operation	Fibers destruction/damage	2	D	Proper routing of fibers; clear procedure for cabling	2D	
	Tearing of fluid pipes	During integration or maintenance	Optics flooded/stained coating damage	4	D	Emergency switch	4C	Slow movement; time to react to avoid damage

″

	Tearing of fluid pipes	During normal operation	Optics flooded/stained coating damage	4	E	Proper routing of pipes; clear procedure for connecting; fluid detector connected to interlock	4D	
WFS7	Abrasion of cables	During integration or maintenance	Cables destruction/damage	4	E	Emergency switch	4E	Slow movement; time to react to avoid damage
	Abrasion of cables	During normal operation	Cable destruction/damage	4	E	Proper routing of cables; clear procedure for cabling	4E	
	Abrasion of optical fibers	During integration or maintenance	Fibers destruction/damage	2	E	Emergency switch	2E	Slow movement; time to react to avoid damage
	Abrasion of optical fibers	During normal operation	Fibers destruction/damage	2	E	Proper routing of fibers; clear procedure for cabling	2E	
	Abrasion of fluid pipes	During integration or maintenance	Optics flooded/stained coating damage	2	E	Emergency switch	2E	Slow movement; time to react to avoid damage

˝

	Abrasion of fluid pipes	During normal operation	Optics flooded/stained coating damage	4	E	Proper routing of pipes; clear procedure for connecting	4E	
WFS8	Cooling fluid leak	During normal operation		2	E	Covers on during operation; fluid deflected not to fall onto critical components	2E	
		During maintenance or integration	Potential damage to optics, motors/encoders of XY table	2	D	Proper maintenance and integration procedure	2D	
WFS9	Noise from 2kHz membrane mirror	During maintenance or integration	Annoyance only when person in proximity	4	C	Sound insulating cover on membrane mirror unit; during maintenance or integration personal should wear hearing protection gear	4C	Annoyance will grow with time spent in Coude environment by individuals
WFS10	Low-lying apparatus	During maintenance or integration	Human fatigue, back injuries	3	D	Proper handling procedure and handling tools;	3D	
WFS11	Low-lying apparatus with structure overhead	During maintenance or integration	Head injuries	3	D	Wearing of safety helmet	3D	

”

WFS12	Crammed space, small setup	During maintenance or integration	Damage to valuable optical pieces	2	E	Proper maintenance and integration procedure; work performed by trained personal	2E	
WFS13	Work performed in close proximity of membrane unit	During maintenance or integration	Damage to membrane or to diaphragm	3	E	Proper maintenance and integration procedure; work performed by trained personal	3E	There will be spares of the membrane provided since they are fragile components; risk decreased by unit enclosed in housing
WFS14	Tool left on shutter	During maintenance or integration	Damage to shutter	3	E	Proper maintenance and integration procedure; work performed by trained personal	3E	
WFS15	Tool left in instrument	During maintenance or integration	Damage to wheel or filters or drive	3	E	Proper maintenance and integration procedure; work performed by trained personal	3E	Unit enclosed in housing
WFS16	Defective XY table brake	During operation or maintenance	Damage to motors	2	E	Brake status checked before motion; interlock cutting of motor power	2E	

″

WFS17	Hard limit defective	Operation	Damage to motor or mechanical stage	3	D	Time out on motion	3D	Spares available; only happens if simultaneous soft. Limit failure
WFS18	Membrane wear or too high input signal	Operation or integration maintenance	Membrane destroyed	3	D	Limiting voltage will be defined at development stage;	3D	Spare membranes provided
WFS19	Earthquake	Any phase	Damage to persons or material	4	E	Low-mass system, low potential energy	4E	System re-homing/alignement might be required

7.1.1. Remarks on Analysis of Mechanical assembly

- Shearing of pieces within the XY table structure could only occur during maintenance work or integration because the system would be operational (connected) and opened (covers removed). However, there is a plate closing the bottom of the T-Mount, preventing insertion or fall of parts within the XY table structure.
- Lower probabilities of all abrasion hazards is justified by a proper routing of all cables, fluid pipes and optical fibers.

7.2. ELECTRONICS HAZARD ANALYSIS

No	Hazard source	Hazardous mode	Effects	Sev.	Occ. Prob	Prevention	Risk	Action/Remark
ELE1	Fall of cabinet	Installation or transport	Electronics damage or human injury	1	E	Proper handling tool and lifting points on cabinets; handling done by qualified personal	1E	

˝

ELE2	Fluid leak in cabinet (Coudé room)	Operation	PCB damage	4	E	Quality plumbing; cooling unit in bottom of cabinet	4E	
	Fluid leak in cabinet (Coudé room)	Maintenance or integration	PCB damage	4	D	Standard fluid connectors;	4D	Human intervention to correct failure
ELE3	Fluid leak in Azimuth platform cabinet	Operation	PCB damage	4	E	Quality plumbing; cooling unit in bottom of cabinet	4E	
	Fluid leak in Azimuth platform cabinet	Maintenance or integration	PCB damage	4	D	Standard fluid connectors;	4D	Human intervention to correct failure
	Fluid leak from azimuth platform cabinet to Coudé room	Operation	Damage to components and systems in Coudé room	2	E	Quality plumbing; cooling unit in bottom of cabinet	2E	Alarm implementation ?
	Fluid leak from azimuth platform cabinet to Coudé room	Maintenance or integration	Damage to components and systems in Coudé room	2	E	Standard fluid connectors;	2E	Human intervention to correct failure
ELE4	Electrocution with HV DM	Maintenance or Integration	Human injury	1	E	Proper grounding; HV interlock, off when not connected	1E	

″

ELE5	Point to bright astronomical source or bright source scanned during slewing	Operation	APD destroyed	2	E		2E	
	Room illumination or flashlight shined onto APD	Integration or Maintenance	APD destroyed	2	E	Trained personel and proper procedure; indirect lighting (housing over WFS unit) Shutter closed at shutdown; Software watchdog active; HW interlock active	2E	
	Computer crash, HW interlock failure & high illumination (!)	Operation	APD destroyed	2	E		2E	Very Low probability organized sequence of low probability events
ELE6	Short circuit	Integration	Burning of cables and /or equipment; contamination of instrument and telescope	2	E	Properly dimensioned over current protection	2E	
ELE7	Loss of electrical power; power surge	Operation, Integration, maintenance	Electronic components damage	2	E	All powered on UPS	2E	

″

ELE8	Electrostatic discharge	Assembly, Integration and maintenance	Sensitive Electronic components destroyed	2	D	Trained personal and well defined procedure; provision of ESD; wrist-straps; proper grounding	2D	
ELE9	Wrong connection, disconnection procedure	Assembly, Integration and maintenance	Broken optical fibers; micro-lens damaged; lens-fiber I/F damage; flux loss	2	D	Trained personal manipulate fragile components; proper procedure	2D	Spare available
ELE10	Earthquake	Any phase	Human injury, cabinet damage	2	E	Low center of gravity cabinet (1.2m high), bolted to floor	2E	

7.2.1. Remark on Analysis of Electronics

Concerning damage caused to APD modules by high illumination, we are confident that our safety scheme is sufficient to insure a *very low* probability of this occurrence. Several conditions would need to be met simultaneously:

- Shutter opened (assumes we are in normal operation then all other safety measures active; if not it would have been closed or has 50% probability of being closed)
- Intense light shined directly into the instrument (either through telescope or operator flashlight; in case of ambient light from APD would still be protected by housing)
- Software watchdog inoperative (computer crash; or power failure but improbable since powered by UPS)
- Hardware interlock in APD counter modules defective

Late information seems to confirm that a substantial illumination must be encountered in order to cause damage to APD i.e. > 10^{16} photons/sec

″

7.3. CORRECTIVE OPTICS HAZARD ANALYSIS

No	Hazard source	Hazardous mode	Effects	Sev.	Occ. Prob	Prevention	Risk	Action/Remark
COR1	Fall of parts from M8 tower	Maintenance or integration	Human injury	1	E	Avoidance zone under M8 tower during maintenance or integration; implementation of cover of M8 to M9 well	1E	
	Fall of parts from M8 tower	Maintenance or integration	Damage to M9 and Telecentricity lens	1	E	Cover on M8 to M9 well; use of covers on M9	1E	
	Fall of TTM/DM assembly	Maintenance or assembly/integration	Damage to TTM/DM	1	E	Proper installation procedure; spares avalaible; qualified personal operation	1E	
COR2	Fall of tools	Maintenance, assembly and/or integration	Damage to M9 and Telecentricity lens	1	E	Cover on M8 to M9 well; use of covers on M9; M8 tower maintenance platform offers safe tool resting space	1E	

″

COR3	Fall of persons	Maintenance, assembly and/or integration	Human injury	1	E	Safe railguard on maintenance platform; locking access gate	1E	
COR4	Human injury	Maintenance, assembly and/or integration	minor human injury	3	D	Help form proper handling tool; proper procedures; manipulation of heavy parts from azimuth platform; modular units	3D	Heavy parts to manipulate in awkward position
COR5	Electrocution by HV DM	Maintenance, assembly and/or integration	Human injury	1	E	Proper grounding; HV interlock, off when not connected	1E	
COR6	Damage to optical surface	Maintenance, assembly and/or integration	Instrument damage; expensive component	2	D	Spare available; use protective cover during installation; done by trained personal	2D	
COR7	Resonant DM while RTC drives at too high freq.	Integration and Operation	Damage to DM	2	D	HV controller filtered high freq. Components	2D	

″

COR8	Resonant TTM while RTC drives at too high freq.	Integration and Operation	M8 optics mis-alignment (!)	3	D	HV controller filtered high freq. Components	3D	
COR9	Vibration	Operation	Instrument damage	2	E	Low vibrating mass	2E	
COR10	Earthquake	Maintenance, assembly and/or integration	Human injury, Instrument damage	1	E	High Stiffness; use of ESO designed (REOSC) mechanical I/F	1E	

________________________**oo0oo**________________________

8. SUMMARY OF THE ANALYSIS

We recall below the different categories of unwanted hazards. From the combination of hazard severity and hazard probability we define the following Acceptance/Rejection 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
Occasional	1C	2C	3C	4C	Acceptable (review)
Remote	1D	2D	3D	4D	Acceptable
Improbable	1E	2E	3E	4E	

8.1. UNACCEPTABLE HAZARDS

There were no instances where unacceptable were predicted. Appropriate design measures were taken to avoid, or minimize the probability of such events.

8.2. UNDESIRABLE HAZARDS

Occurrences of marginal hazards were recorded mainly in the category catastrophic but improbable and a few critical but remote:

Catastrophic-Improbable (1E)	**Critical-Remote (2D)**
WFS1, WFS4, WFS5, ELE1, ELE4, COR1, COR2, COR3, COR5, COR10	WFS8, ELE8, ELE9, COR6, COR7

These are all related to the handling, assembly, integration and maintenance phases. This stresses the need for well defined procedures at Paranal during these phases. We also assume that normal work habits and standard safety measures in handling and manipulating of equipment should minimize these hazards. We wish to stress that these hazards are certainly not typical MACAO-VLTI but more of the type of operation carried out during these phases.

8.3. ACCEPTABLE HAZARDS (REVIEW)

A few occurrences of marginal hazards were recorded mainly in the category critical but improbable and a few marginal but remote:

Critical-Improbable (2E)	**Marginal-Remote (3D)**	**Negligible-Occasional (4C)**
WFS2, WFS7, WFS8, WFS12, ELE3, ELE5, ELE6, ELE7, ELE10, COR9	WFS3, WFS10, WFS11, WFS17, WFS18, COR4, COR8	WFS6, WFS9

These hazards are typical of the phases operation and maintenance. In particular if non-proper disconnecting/reconnecting occurs, manipulation of handtools, such hazards are more likely

″

to occur. Good procedures and trained personal should again limit these occurrences. The last columns are typical occurrences of cable/connector damage. These do not represent severe hazards. Furthermore, ESO has experience in the field of proper cables and connectors and these type of hazards should be minimized by choice of the usual good quality supplies. The developer of MACAO-VLTI will take particular care in proper cable routing and holding of the cable to keep the risk of these hazards low.

8.4. ACCEPTABLE HAZARDS

All these hazards are either improbable or negligible:

Marginal-Improbable (3E)	Negligible-Remote (4D)	Negligible-Improbable (4E)
WFS13, WFS14, WFS15, WFS16	ELE3	WFS7, WFS19, ELE2, ELE3

A few of these hazards are related to human error. Again proper training and qualified staff will minimized these.

9. CONCLUSIONS

The following conclusion can be drawn from this analysis:

- MACAO-VLTI does not present any unacceptable hazards neither in its operation nor installation at Paranal .
- The risk of human injury is higher during handling and installation of the instrument. These risks are more related to the nature of the operations than to the particular type of instrument. Properly trained personal will decrease the probability of personal injury.
- Instrument damage is much more probable during maintenance and integration tasks. Well defined procedures and qualified personal should perform these tasks to insure their low probability of occurring.
- Very few hazard leading to instrument damage are likely to take place during operation. This is partly due to the relative simplicity of the instrument but also because several aspects of the design address directly these questions.