Southern African Large Telescope
SALTICAM

Document Number 3300AE0011:
Safety

Geoff Evans
Etienne Bauermeister
Dave Carter
Willie Koorts
James O’Connor
Darragh O’Donoghue
Faranah Osman
Stan van der Merwe

Issue 1.2
24 October 2002
ACRONYMS AND ABBREVIATIONS

ATP  Acceptance Test Procedure
FDR  Final Design Review
CCAS  Centre of Curvature sensor
CCD  Charge-coupled Device (Camera)
IEC  International Electro technical Commission
HW  Hardware
N/A  Not applicable to this Specification
PDR  Preliminary Design Review
SALT  Southern African Large Telescope
SW  Software
TBC  To Be Confirmed
TBD  To Be Determined
UPS  Uninterruptible Power Supply

Table of Contents

1  Scope........................................................................................................................................... 3
2  Referenced documents .................................................................................................................... 3
3  Definitions (from SALT Safety Analysis Document 1000AA0030 Issue B).................................. 3
   3.1  Hazard SEVERITY categories: .................................................................................................. 3
   3.2  Hazard occurrence FREQUENCY categories: ........................................................................... 4
   3.3  Risk Classes ............................................................................................................................... 4
1 Scope

This document specifies the safety analysis of the SALTICAM subsystem of the Southern African Large Telescope.

The SALTICAM subsystem has two modes of operation:

1. As the telescope Verification Instrument (SALTICAM VI)
2. As an Acquisition and Science Imager (SALTICAM ACSI)

The document identifies the undesirable events, which can cause injuries to personnel, damage to the telescope equipment and interruption of the telescope operation in either of these two operational modes.

Section 5 describes the undesirable events, failure causes and preventive measures.

2 Referenced documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3300AS0001</td>
<td>SALTICAM System Specification</td>
</tr>
<tr>
<td>1000AA0030</td>
<td>SALT SAFETY Analysis Issue B.doc</td>
</tr>
<tr>
<td>IEC 61508-5</td>
<td>Functional safety of electrical/ electronics/ programmable electronic safety related systems</td>
</tr>
</tbody>
</table>

3 Definitions (from SALT Safety Analysis Document 1000AA0030 Issue B)

There are different ways to determine the safety risk level for a specified safety function. SALT shall attempt to have a tolerable risk as low as reasonable practicable (ALARP), as described in IEC standard 61508-5. The basic principle defines the following:

3.1 Hazard SEVERITY categories:

Severity A – **Catastrophic failure**, which may result in severe injury, death or major damage to the telescope.

Severity B – **Critical failure**, which may result in minor injury and also
interruption of telescope operation for more than one week.

Severity C – **Marginal failure**, which may result in interruption of telescope operation and cannot be repaired the same night.

Severity D – **Negligible failure**, which may result in interruption of telescope but can be repaired the same night.

### 3.2 Hazard occurrence FREQUENCY categories:

- **Frequent (F)** – More than 1 per year
- **Probable (P)** – 1 per year
- **Occasional (O)** – 1 per 10 years
- **Remote (R)** – 1 per 100 years
- **Improbable (I)** – 1 per 1000 years

### 3.3 Risk Classes

- **Class I** – intolerable
- **Class II** – undesirable, tolerable only if risk reduction is impracticable and too costly
- **Class III** – tolerable if costs for risk reduction is higher than the improvement gained
- **Class IV** – negligible risk.

The four parameters in the risk classification matrix can be combined with the purpose to identify the tolerable risk levels for different risks. Table 1 is the SALT risk classification matrix; which shall be used to ensure that the designs are practical and safe to implement. For practical use of the matrix the probability categories have to be quantified carefully and the meaning of hazard severity of each system be specified. The effect of hazard and the frequency of occurrence (Probabilities) can be determined by using reliability calculations, failure mode and effects analysis.

<table>
<thead>
<tr>
<th>Hazard Occurrence Frequency (Probability)</th>
<th>Hazard severity Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Critical</td>
</tr>
<tr>
<td>Frequent</td>
<td>I</td>
</tr>
<tr>
<td>Probable</td>
<td>I</td>
</tr>
<tr>
<td>Occasional</td>
<td>I</td>
</tr>
<tr>
<td>Remote</td>
<td>I</td>
</tr>
<tr>
<td>Improbable</td>
<td>II</td>
</tr>
</tbody>
</table>
Table 1

3.4 Status

Each identified undesirable event may be in one of the following four phases of resolutions:

- Initial (Initial) – SALT initial safety analysis
- Unacceptable (U) – No acceptable design solutions found yet (Risk too high)
- Acceptable (A) – Acceptable design solutions found (Risk okay)
- Verified (V) – Solutions has been verified and implemented

3.5 Safety Committee

The Safety Committee shall consist of SALT Subsystem managers, System engineer, Control engineer and co-opted members. The purpose of the Safety Committee is to review the identified hazard and their proposed solutions.
4 Safety Analysis Procedure (from SALT Safety Analysis Document 1000AA0030 Issue B)

Risk identification and risk reduction form an integral part of the acquisition, operation and maintenance, and the disposal phases of product or astronomical telescope and instruments. Figure 2 shows the typical lifecycle phases of the design and development activities of SALT project, the standard project phase related activities and the safety activities focused on safety related equipment and devices.

This document shall be used to develop and compare alternative concepts during concept design phase to satisfy the original design. All the concepts shall be analysed by the project team with respect to the inherent manufacturing, test, installation, operation, maintenance hazards and risks. Based on the results of the analysis overall safety requirements shall be defined for SALT system.

This document initially contains a preliminary safety analysis for SALT. Subcontractors shall review and expand this analysis to adequately assess the risk of safety related failures of their supplied equipment. During this process, they shall provide details of the safety measures proposed or/ and implemented in their equipment for approval by the SALT Safety Committee. This document shall be updated accordingly. The subcontractors shall demonstrate that the safety measures proposed have been implemented and they provide adequate protection. Risks of class I (as defined in Table1) are not acceptable. All risks of class II and III need to be approved by the SALT Safety Committee. Figure 1 below clearly demonstrates the three regions that Subcontractors may use as a test in regulating risks in their designs.

Figure 1
<table>
<thead>
<tr>
<th>Design and Development Activities</th>
<th>Life Cycle Phase</th>
<th>Safety Related Activities</th>
</tr>
</thead>
</table>
| The product life cycle phase during which the requirements are specified | Concept Definition And Design Phase | 1. Initial Hazard Risk Analysis  
2. Definition of safety requirement  
3. Subsystem Safety Analysis  
4. Safety requirement allocation to risk reduction methods (s/w, h/w, elect, mech.) |
| The product life cycle phase which h/w and s/w are created and documented as designs and documentation such as operation and maintenance instructions are produced | Design & Development Phase | 1. Risk reduction method specification  
2. Safety requirement allocation to h/w and s/w  
3. Overall risk reduction operation, maintenance, installation planning  
4. Hardware and software design and development  
5. Review subsystem safety analysis and preventive measures  
6. Review and update SALT safety analysis  
7. Assess system safety |
| The product life cycle phase during which product / system is produced, and system is assembled. | Manufacturing Phase | 1. Realisation of all h/w and s/w  
2. Risk reduction method integration and safety verification  
3. Functional verification of the risk methods and measures |
| The product life cycle phase during which the product / system is installed. | Installation Phase | 1. Installation, commissioning and verification of the risk reduction methods  
2. Safety visit and inspection of equipments |
| The product life cycle phase during which the product / system is put to use, maintained and supported. | Operation and Maintenance Phase | 1. Overall operation and maintenance  
2. Controlled modifications |

Figure 2
## 5 SALTICAM Subsystem

<table>
<thead>
<tr>
<th>UNDESIRABLE EVENTS</th>
<th>FIRST LEVEL CAUSES</th>
<th>SECOND LEVEL CAUSES</th>
<th>PREVENTIVE MEASURES</th>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 SALTICAM falling off the telescope</td>
<td>This undesirable event can occur as a result of first level causes 1 or 2 and 3</td>
<td></td>
<td></td>
<td>A</td>
</tr>
</tbody>
</table>
| 1. Multiple parts loosening on mount. | • Excessive vibration  
• Not bolted on properly | • SALT designed for minimum of vibration  
• Torque nuts and bolts  
• Use chemical locking compounds or aircraft-type locking nuts. | | |
| 2. Dropping components during installation or maintenance | • Inadequate handling equipment  
• Safety net not used  
• Untrained personnel  
• Bottom cover removed | • Install applicable handling equipment  
• Use safety net  
• Train personnel  
• Leave cover on as safety net if possible | | |
<p>| 3. Crane operator error | | | • Only trained dome crane operators shall carry out such operations | |
| 5.1.2 Electrical shock | | | | A |
| 1. Chaffed mains cabling | • Bad cable routing | • Route cables correctly | | |
| 2. Power not switched off | • No Power switch | • Install power switch | | |</p>
<table>
<thead>
<tr>
<th>UNDESIRABLE EVENTS</th>
<th>FIRST LEVEL CAUSES</th>
<th>SECOND LEVEL CAUSES</th>
<th>PREVENTIVE MEASURES</th>
<th>SEVERITY</th>
</tr>
</thead>
</table>
| 5.1.3 CCD’s mechanically damaged or destroyed on the telescope | 1. Frame Transfer Mask physically damages CCD’s | • Poor design  
• Material choice | • Failsafe design  
• Use of appropriate materials | B |
| | 2. Loose mounting hardware physically damages the CCD’s | • Fasteners not tightened to correct torque | • Torque fasteners correctly | |
| 5.1.4 CCD’s electronically or electrically damaged or destroyed on the telescope | 1. Electronic fault | • Short circuit of CCD signals  
• Power supply fault | • Good quality connectors and wiring  
• Good wiring practices  
• Failsafe power supply | B |
| | 2. Static damage due to incorrect handling | • Personnel not following procedures  
• Lack of knowledge  
• Inappropriate clothing | • Train maintenance personnel as per 3360AE0002  
• Warning signs on connectors/ cables that must not be unplugged  
• Sound ESD practices | |
| | 3. CCD destroyed by ion bombardment | • Ion pump switched on with its permanent magnet removed | • Train personnel  
• Appropriate warning signs | |
| 5.1.5 Vacuum pump falls off pumping platform | 1. Pump not secured | • Untrained personnel  
• Vibration | • Operator training  
• Use clamp system that cannot be loosened by vibration | B |
| 5.1.6 Sub units or small parts including fasteners and cover panels falling off SALTICAM with the possibility of injuring people or damaging the primary mirror | 1. Loose nuts or bolts | • Vibration | • Torque nuts and bolts  
• Use chemical locking compounds or aircraft-type locking nuts | B |
| | 2. Tools or components not secured to harness | • Unsafe tracker position  
• Personnel not using safety procedures  
• Human error  
• Leaving tools on the tracker  
• No Safety net under tracker | • Move tracker to lower limit if possible to protect mirror  
• Accessible components and fasteners to be captive  
• Wear hard hats  
• Use controlled toolboxes  
• Use safety net | |
| 5.1.7 SALTICAM catching fire | 1. Electrical fault | • Oversized trip switch  
• Short circuit due to damaged insulation | • Use correct trip switch  
• Route cables correctly  
• Use quality cables | B |
| | 2. Explosion of flammable gas or liquid – Cryotiger working fluid | • Open flame | • No open flames near Cryotiger system  
• Appropriate warning signs on Cryotiger compressor | |
<table>
<thead>
<tr>
<th>UNDESIRABLE EVENTS</th>
<th>FIRST LEVEL CAUSES</th>
<th>SECOND LEVEL CAUSES</th>
<th>PREVENTIVE MEASURES</th>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Electronics overheating</td>
<td>• Failure of glycol cooler</td>
<td>• Monitor electronics temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Glycol pipe bursts or leaks</td>
<td>• High Pressure, Corrosion, Ageing, Poor glycol line routing</td>
<td></td>
<td>• This is the responsibility of SALT</td>
<td></td>
</tr>
<tr>
<td>UNDESIRABLE EVENTS</td>
<td>FIRST LEVEL CAUSES</td>
<td>SECOND LEVEL CAUSES</td>
<td>PREVENTIVE MEASURES</td>
<td>SEVERITY</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 5.1.8 Damage to sensitive electronic equipment due to static | 1. Maintenance procedures not followed | • Low humidity  
• Nylon clothing  
• Lack of knowledge | • Design in ESD protection  
• Train maintenance personnel  
• Warning signs on connectors/ cables that must not be unplugged | B |
| 5.1.9 Moisture in electronics | 1. Condensation | • Cooler box too cold | • Monitor cooler box temperature  
• Facility responsibility | B |
| 5.1.10 SALTICAM cooling system fails | 1. Tracker damages Cryotiger pipes | • Poor pressure hose routing | • Ensure safe routing away from tracker motions  
• Monitor SALTICAM CCD temperatures and warn user | C |
| 5.1.11 SALTICAM subsystem damaged. | 1. Poor Quality Escom power | • Overloaded circuits | • Circuits not to be overloaded  
• SALTICAM to be UPS powered | C |
| 5.1.12 Frame transfer Mask failure | 1. Mechanism jamming | • Foreign materials  
• Electronics drive failure  
• Software bugs | • Assembly in clean room  
• Conservative design  
• Fully tested software  
• Drive Motor power limited | D |
| 5.1.13 SDSU Controller power supply failure | 1. Power surges | • Component failure  
• Age of power supply | • SALTICAM to be UPS powered  
• SALT provided spare SDSU power supply unit | C |
| 5.1.14 SDSU Controller failure | 1. Component failure | • Integrated circuit infant mortality  
• Age of controller | • SALT provided spare SDSU controller | C |
| 5.1.15 Cryotiger compressor failure | 1. Mechanical failure | • Age of compressor | • SALT provided spare Cryotiger compressor | C |
| 5.1.16 Shutter mechanism failure | 1. Jammed mechanism | • Poor quality shutter  
• Foreign materials | • Use quality mechanisms  
• Design suitable covers  
• Routine maintenance | D |
| 5.1.17 Filter mechanism failure | 1. Jammed mechanism | • Foreign materials | • Design suitable covers  
• Routine maintenance | D |
<table>
<thead>
<tr>
<th>UNDESIRABLE EVENTS</th>
<th>FIRST LEVEL CAUSES</th>
<th>SECOND LEVEL CAUSES</th>
<th>PREVENTIVE MEASURES</th>
<th>SEVERITY</th>
</tr>
</thead>
</table>
| 5.1.18 Electronics circuit failure | 1. Power surges | • Poor circuitry design | • SALTICAM to be UPS powered  
• Conservative, thoroughly tested circuit design | D        |
| 5.1.19 SALTICAM computer failure | 1. Power surges | • Age of computer | • Use UPS power  
• Use good quality computers | D        |
|                      | Hard drive failure | • Mechanical failure  
• Electronic failure | • SALT provided spare drive with SALTICAM system software installed |          |
| 5.1.20 Software bugs | 1. Software not fully tested | • Poor programming | • Good programming practices  
• Test all software fully | D        |