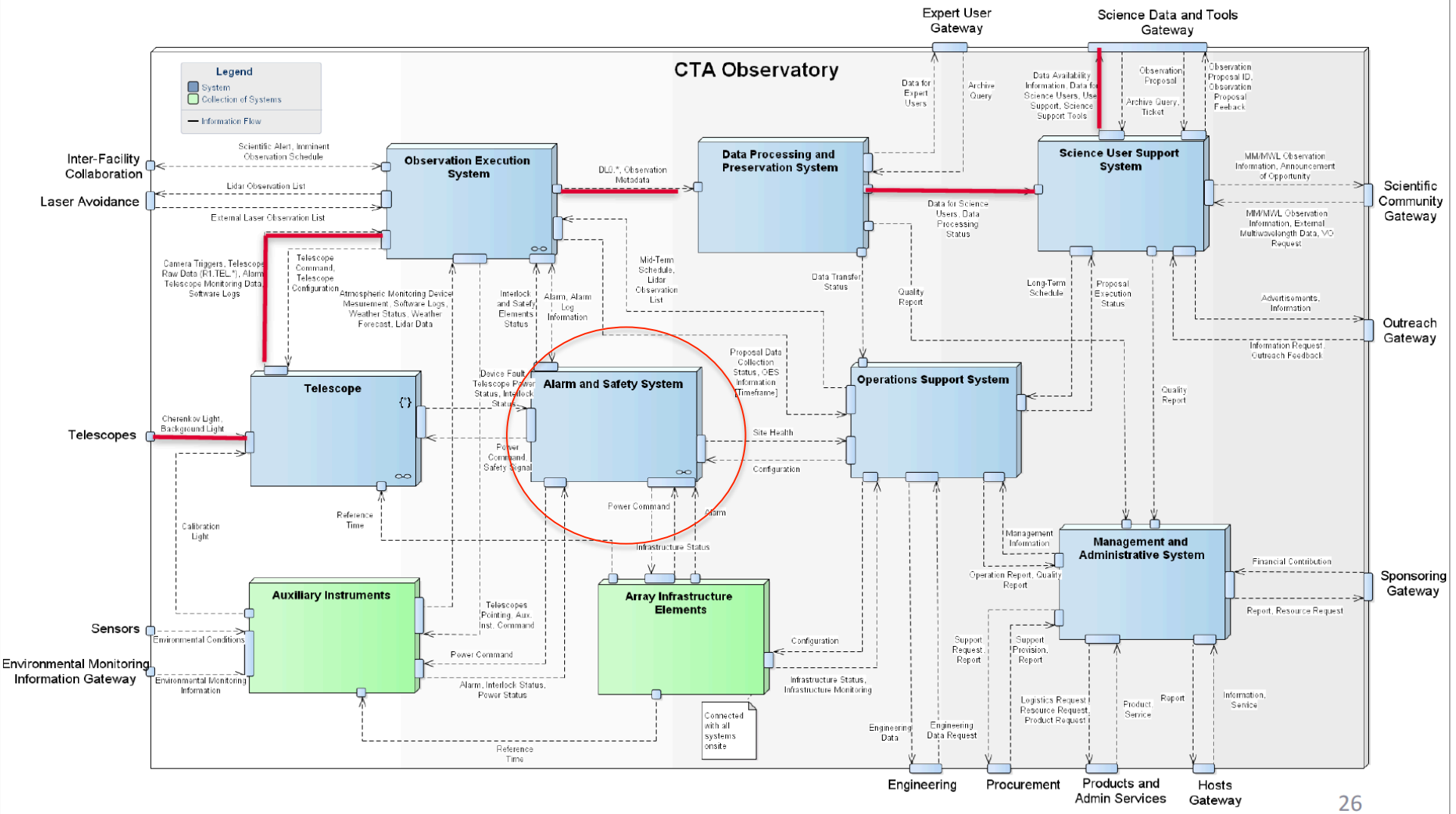
Interlocks: Safety and Alarm System

G. Tosti
(CTAO/University of Perugia)

CTA System Architecture



Safety and Alarm System (SAS) : Scope

- The Safety and Alarm system is envisaged as a high-reliability/low-complexity hardware and software system for monitoring and control of the primary safety-relevant aspects of the Observatory at the two sites. **Do not include Health and Occupational Safety**.

- It provides an interface to Operators and Day Crew to monitor the basic status (for example ok, off, fault) of all array elements and associated systems: (possible alarm sources are e.g. Telescopes and the Array Infrastructure Elements such as onsite ICT components, cooling and power systems), and collects and manages safety-relevant alarms generated by these systems (for example fire alarms, access alarms, telescope alarms) to present operators with the clear information needed to minimize the time taken to diagnose the root problem and decide on a response.

- The SAS collects and provides information on the status of interlocks and power at Telescopes, and control of the power down to sub-system level (Camera, Mount) .
- In addition, the Alarm and Safety System contains the system for controlling access to the array and monitoring which individuals are present within the array at a given time.

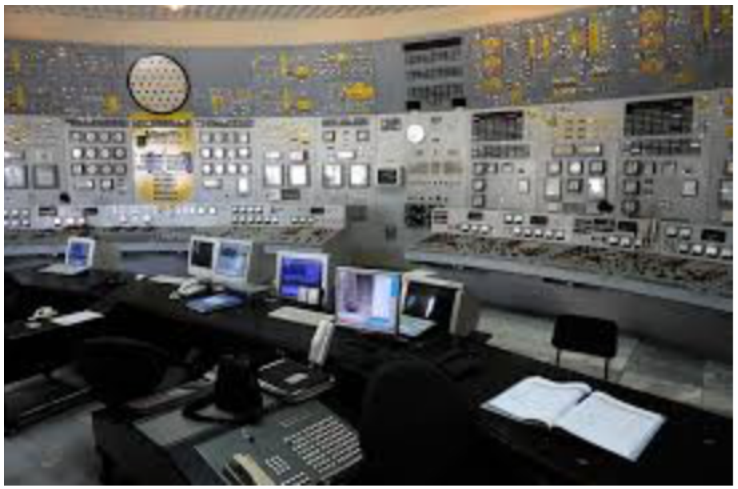
- The SAS must be interfaced to the Observation Execution System to allow alarm information to flow from the Observation Execution System to the SAS and for power/fault/interlock status to be available to the Observation Execution System to allowing Telescope use planning / resource management.

- The SAS must be interfaced to the Operations Support System to provide a long-term record of the basic status of array elements for use in planning and reporting.

This will translated in product Level B requirememts

Safety and Alarm are related

- Alarm systems are instrumented systems designed to notify an operator that a process is moving out of it's normal operating envelope to allow them to take corrective action.



- Alarm systems that are designed to reduce the risk of accidents can be considered as a Safety System.

Some Standards

- Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems IEC 61508
- Safety of machinery. Electrical equipment of machines general requirements EN 60204-1
- Occupational Health and Safety [OHS] https://osha.europa.eu/en/safety-and-health-legislation/european-directives
- Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems IEC 61508
- Safety of machinery. Electrical equipment of machines general requirements EN 60204-1
- European directtive 2006/42/EC on machinery (sections 1, 3, 4 and 6 of Annex I)
- Host Countries Standards

Functional Safety (IEC 61508)

- IEC 61508 must be applied to safety-relevant systems if these contain one or more of the following devices:
  - Electrical equipment (E)
  - Electronic equipment (E)
  - Programmable electronic equipment (PE)

CTA System Elements have a lot of E/E/PE

Functional Safety (IEC 61508)

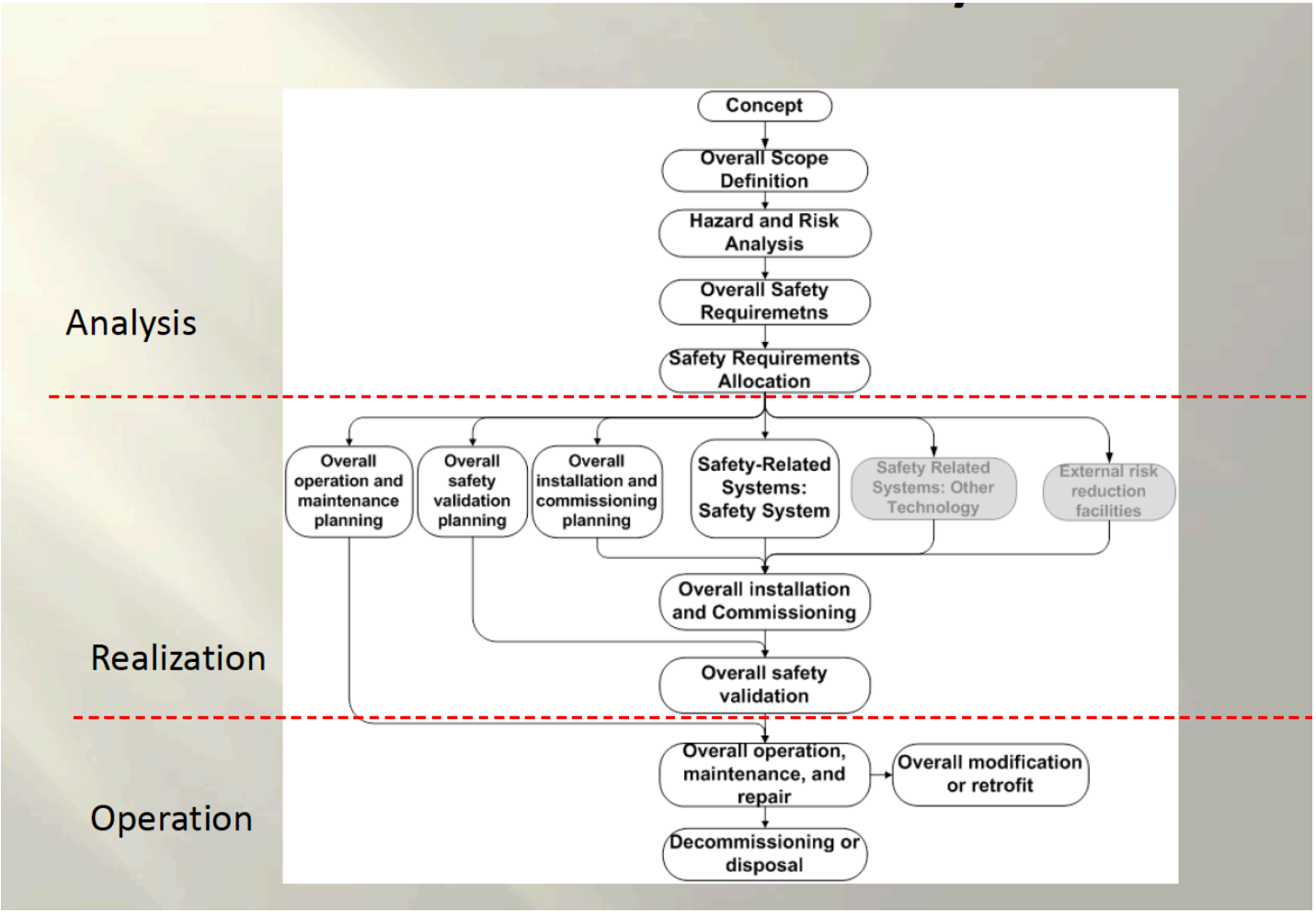
- **Functional safety**. The standard requires the provision of so-called safety functions for the mitigation of risk associated with functions of the system in the cases in which this risk deemed to be too high.

- A **safety function** is an action to be implemented, which is intended to achieve or maintain a safe state for the equipment under control, in respect of a specific hazardous event.

- **Safety Integrity Level** (SIL) of a required function. There are four degrees of SIL, SIL 1 through SIL 4, ranging from moderately stringent to very stringent integrity.

Safety integrity level	**High demand or continuous mode of operation** (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Safety life-cycle IEC 61508



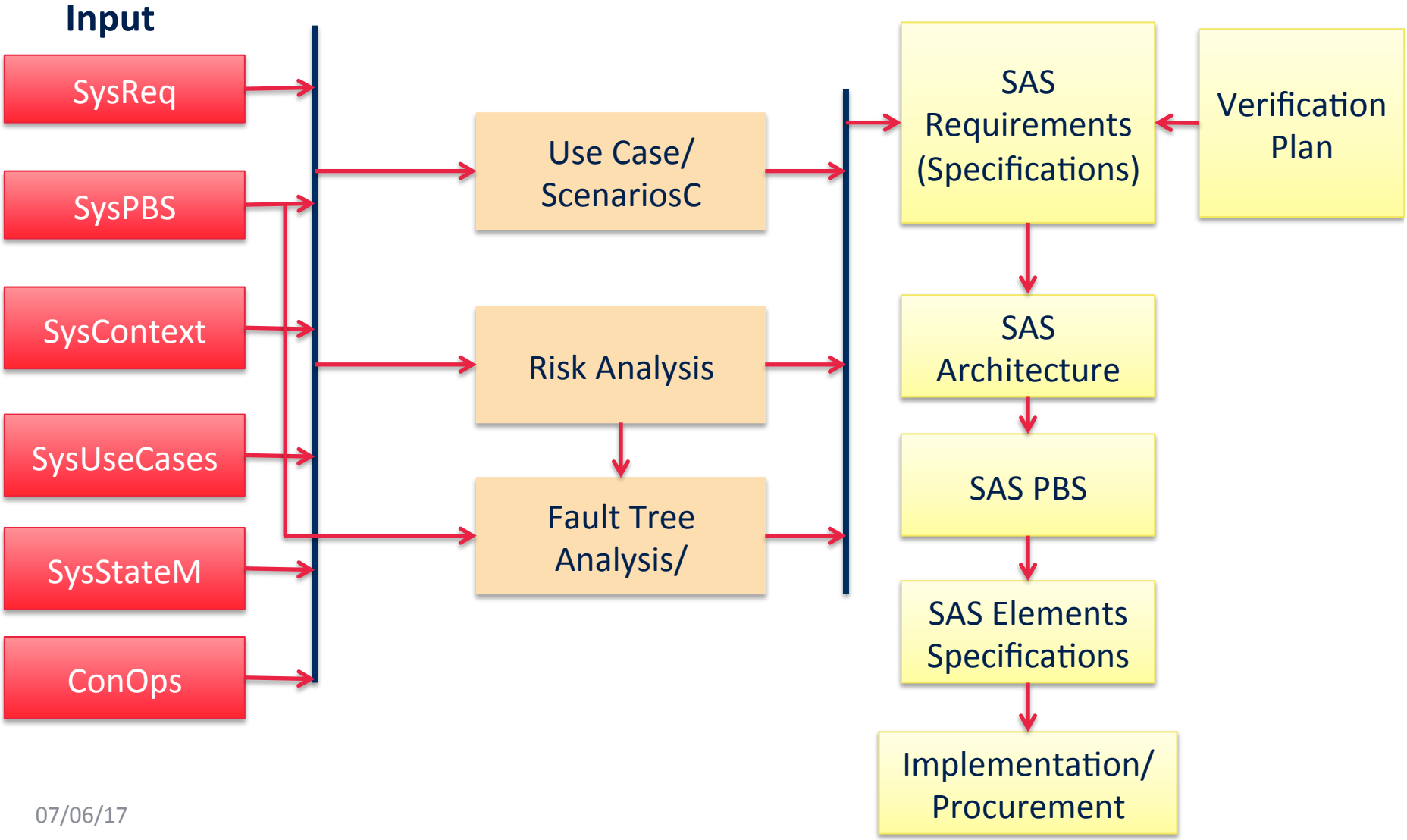
Analysis

- Scoping
  - Determine the physical equipment to be included in hazard/risk analysis
  - Determine the subsystems associated with the hazards
  - Determine what external events will be included
  - Determine types of accident-initiating events

- Hazard & Risk Analysis
  - Develop hazards list & events
  - Includes fault conditions & misuse
  - Abnormal & infrequent operation modes
  - Determine event sequences
  - Determine the likelihood & consequences for each event
  - Evaluate the risk

- Safety Requirements
  - Specify necessary safety functions
  - Determine necessary risk reduction
  - Determine safety integrity requirement for each safety function

SAS definition (simplified Life Cycle)



Risk Assessment

- Risk assessment and risk analysis of technical systems can be defined as a set of systematic methods to:
  - Identify hazards
  - Quantify risks
  - Determine components, safety measures and/or human interventions important for System safety

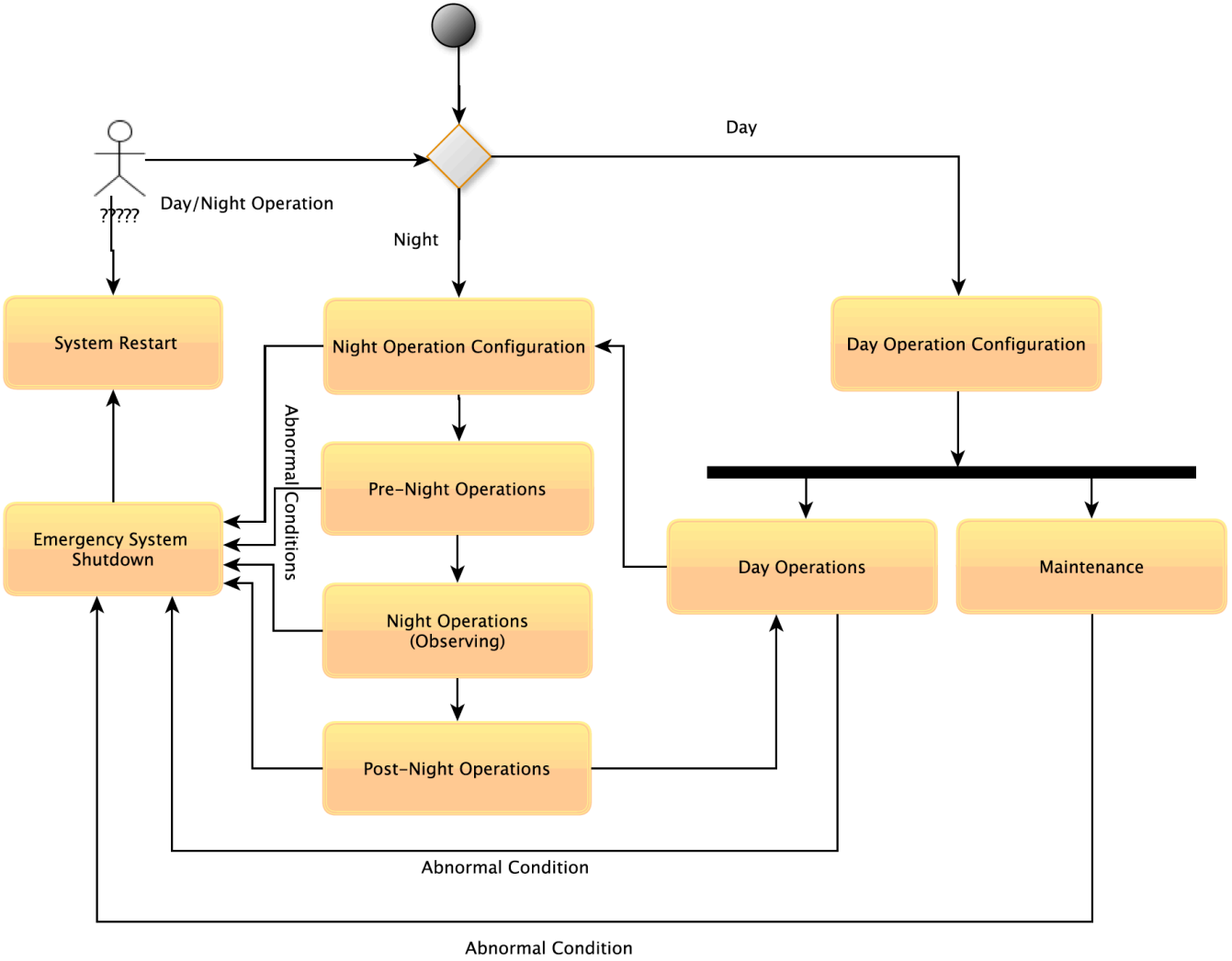
SAS → Observatory Protection Scenario

- SAS must provide all needed hardware and software elements need to maintain and protect the Observatory in case of risks that can compromise the operation and the integrity of the facility.

- Critical events can be different for the two sites and a detailed Risk analysis at level of Observatory will provide all needed input to optimally design the SAS.

  - Earthquakes
  - Weather
  - Power outage
  - Loss of the telecommunication connection
  - Networking Fault

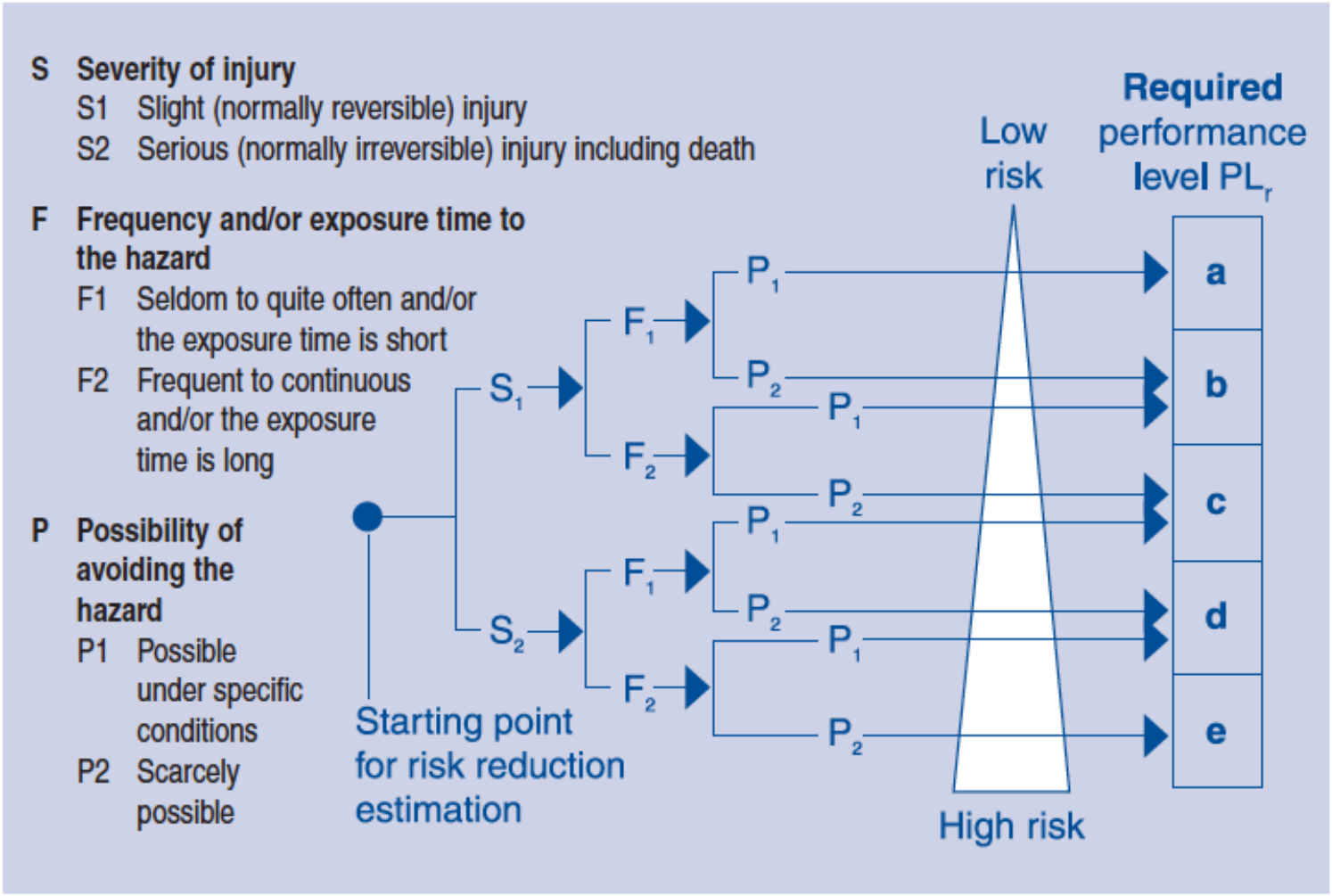
System Operation States



Some Technical Risks to be assessed

- Equipment failures leading to electrical shock.
- Control systems failure leading to malfunction of an equipment/telescope.
- Disturbance / interruption of the power source leading to malfunction of any System Element.
- Safety related control circuit failure leading to failure of safety functions.
- EMC problems leading to malfunction of a device/equipment/ telescope.
- Release of stored energy leading to unexpected movements / electrical shock.
- High surface temperatures leading to burns.
- Critical Control & Monitoring parameters

Risk Assessement (ISO 13849-1)



Safety control Categories (ISO 13849-1)

Safety Cat.	General Safety System Requirements	General Safety System Behavior
B	Safety system designed to meet operational requirements and withstand expected external influences. (This category is usually satisfied by selecting components compatible with the application conditions … e.g. temperature, voltage, load, etc.)	A single fault or failure in the safety system can lead to the loss of the safety function.
1	Safety system must meet the requirements of Category B, but must use "well-tried" safety principles and components. "Well-tried" principles and components include those which: • avoid certain faults … e.g. short circuits. • reduce probability of faults … e.g. over-rating selected components, over-dimensioning for structural integrity. • detect faults early … e.g. ground fault protection. • assure the mode of the fault … e.g. ensure an open circuit when it is vital that power be interrupted should an unsafe condition arise. • limit the consequences of the fault.	A single fault or failure in the safety system can lead to the loss of the safety function. However, the use of "well tried" safety principles and safety components results in a higher level of safety system reliability.
2	Safety system must meet the requirements of Category B. In addition the machine shall be prevented from starting if a fault is detected upon application of machine power, or upon periodic checking during operation. (Single-channel operation is permitted provided that the input devices … such as machine guard interlocks, E-stop pushbuttons, et al … are tested for proper operation on a regular basis.)	Here, too, a single fault or failure in the safety system can lead to the loss of the safety function between the checking intervals. However, periodic checking may detect faults and permit timely maintenance of the safety system.
3	Safety system must meet the requirements of Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function. And, where practical, the single fault will be detected. (This requires redundancy in the safety circuit monitoring module and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function and, where possible, will be detected.
4*	Safety system must meet the requirements of Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function and will be detected at or before the next demand on the safety system. If this is not possible, then the accumulation of multiple faults must not lead to the loss of the safety function. (This also requires redundancy in the safety circuit and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc. Here the number of allowable faults will be determined by the application, technology used, and system structure.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function, and it will be detected in time to prevent the loss of the safety function.

*Category/Level 4 safety requirements are usually associated with extremely high-risk applications. Since general machine design practice respects classic safety hierarchy, in which most machine hazards are either:
- designed out,
- guarded against (if they cannot be designed out), and,
- (as a last resort) warned against,

Level 4 requirements may arise relatively infrequently.

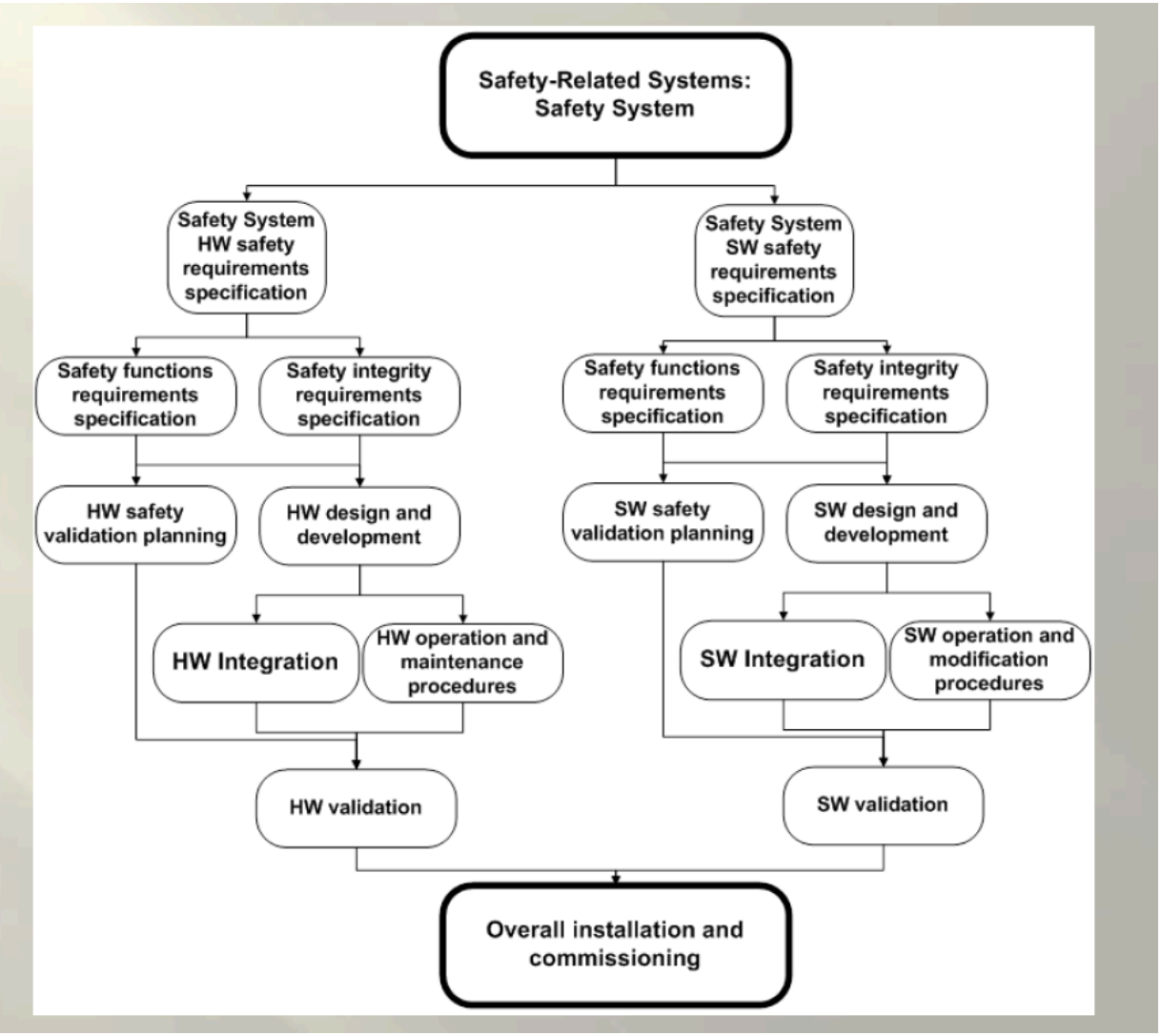
Preliminary General SAS Specifications (mainly from Standards and SysReq)

- In general terms SAS enforces the safety of the Observatory by continuously monitoring the state of connected equipment, systems and sensors and taking appropriate action as soon as an unsafe condition is detected.

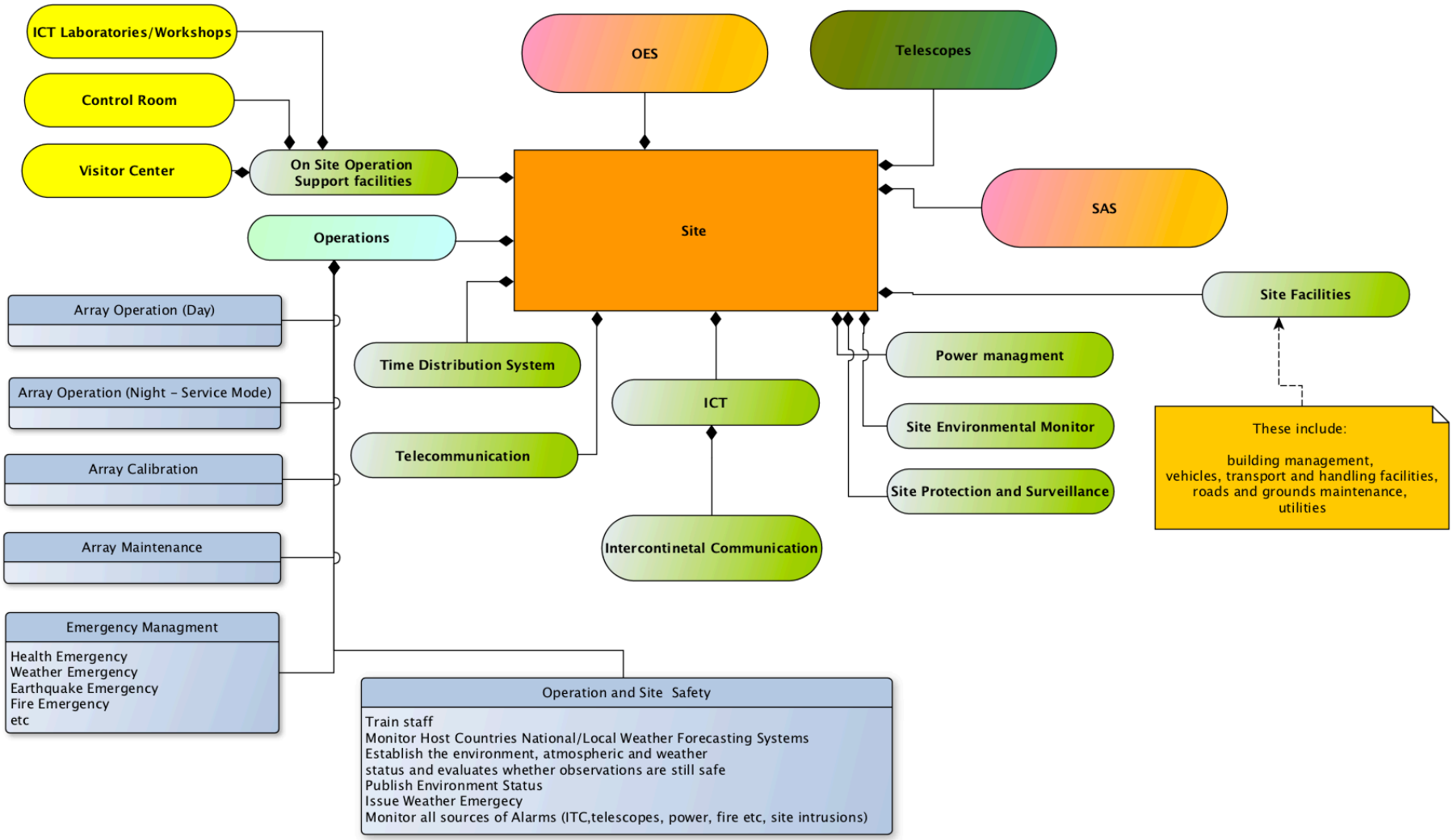
- SAS Interlock system must use fail-safe devices
- SAS must use Safety PLC (Functional Safety) to manage Interlocks.
- SAS Interlocks System must be fault tolerant. (Dual channel / ring network topology ????)
- Access to SAS must be allowed only to Safety Operators/engineers
- The SAS operation does not rely on the availability of any other systems other than power.
- The SAS must be independent from any safety systems contained in, for example, a Telescope and its assemblies.
- SAS provides fault, interlock and emergency stop monitoring and control.
- SAS provides and control independent audible and visual warning devices.
- SAS detects all hazardous condition (including presence in hazardous areas like around a telescope (I would suggest to use some presence sensors around the telescope area, during the day) or the switch of the fence)
- SAS provides an indication to the OES that an interlocks request is requires.
- Any Interlock rised by SAS should be reset manually by the operator (???)
- The SAS shall provide different operational modes that support: Science Operations, Maintenance Operations; Fault and Interlock Recovery

IEC61508 Implementation Phase

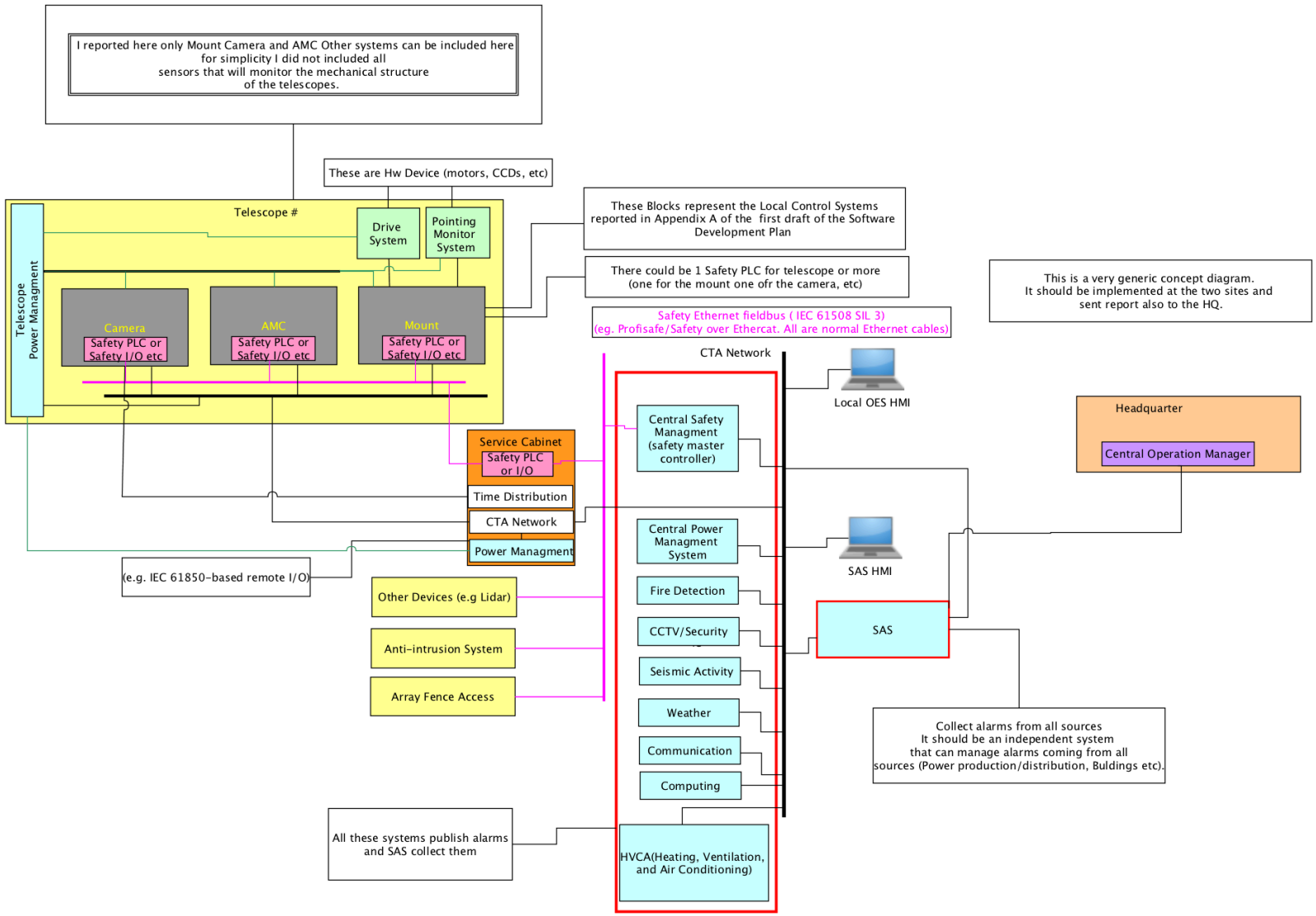
- Technology & Architecture selections
- Determine test philosophy Perform reliability and safety evaluation to determine if you met your target SIL requirement
- Develop conceptual design
- Prepare detailed design document (wiring diagrams; installation plans, etc.)



Safety and Alarm System concept design



Safety and Alarm System concept design



Safety and Alarm System concept design

Operator GUI

SAS Engineer GUI

SAS

Alarms and Monitoring points
(only the relevant one)

System Software

System Hardware

SAS High Priority Interfaces Definition

- Interface to Telescopes
  - Telescope - Observatory Interlocks System Interfaces
- Interface to Infrastructure
  - Power System
  - Network System
  - Time distribution system

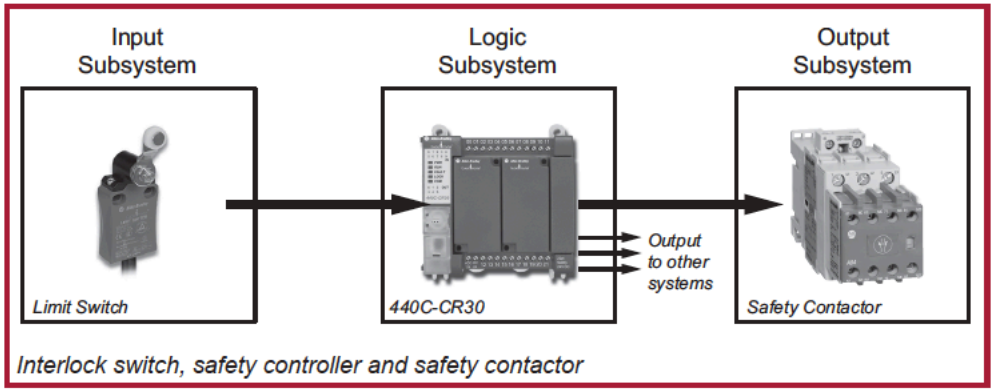
SAS/telescope Interface:
UC: Cold Start of the Array

- The OES send a request to SAS to power-on one or more telescopes
- (Assumes that the telescope is off) →
- The Power management system of the telescope will power on
  - the internal network switch
  - The Local Safety Unit
  - the drive system LCU
  - the Camera LCU
  - All other Local control Units (LCUs)
- The LCUs start monitoring all sensors/switches etc.
- The SAS receive a signal about the completion of power on. (these means only that from the electrical point of view all systems were ok)
- SAS send an OK to the OES signal
- The Telescope Manager checks the communication with all Local Control Units and if all ok communicate to OES that the telescope is in Safe state.

Functional Safety and Interlocks

- An example of an appropriate application of safety functions is in interlock systems.

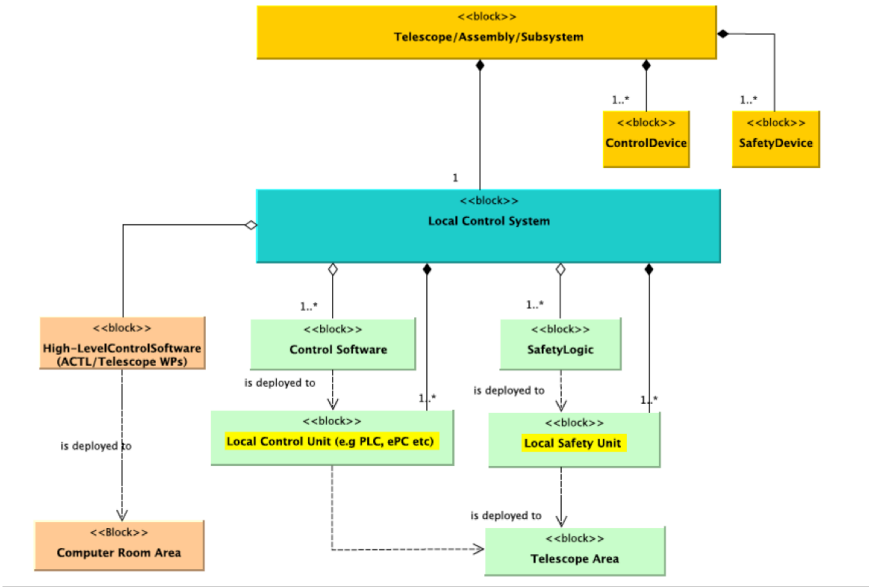
- Interlocks are protective HW/SW systems devoted to minimizing risk to people, property, and environment.

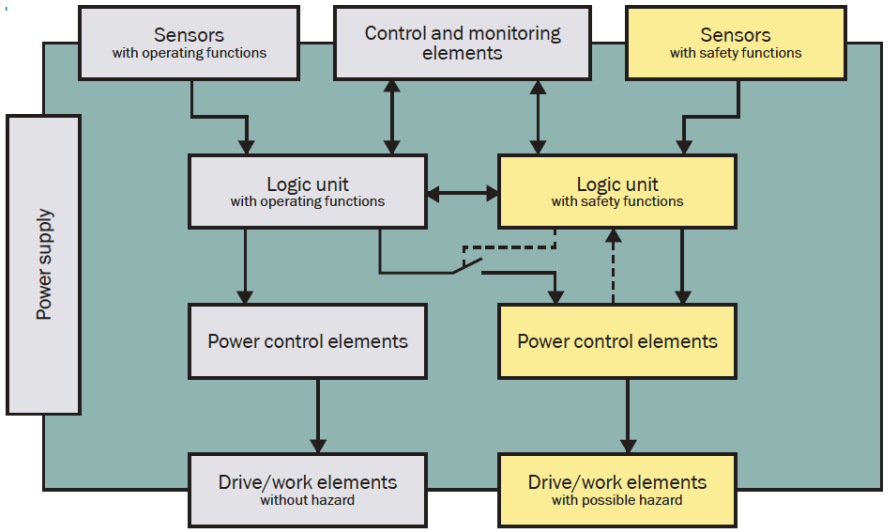


Interlock switch, safety controller and safety contactor

SAS – Telescope Interface

- I assumed the following HW/SW schematic architecture for interface to telescope and SAS





Telescope Interlocks

- Includes the all interlocks and safety related components required to guarantee person and equipment safety of the Telescope.

- Telescope Interlocks system designed by the telescope team based on the Requirements and Hazard and Risk Assessment Analysis.

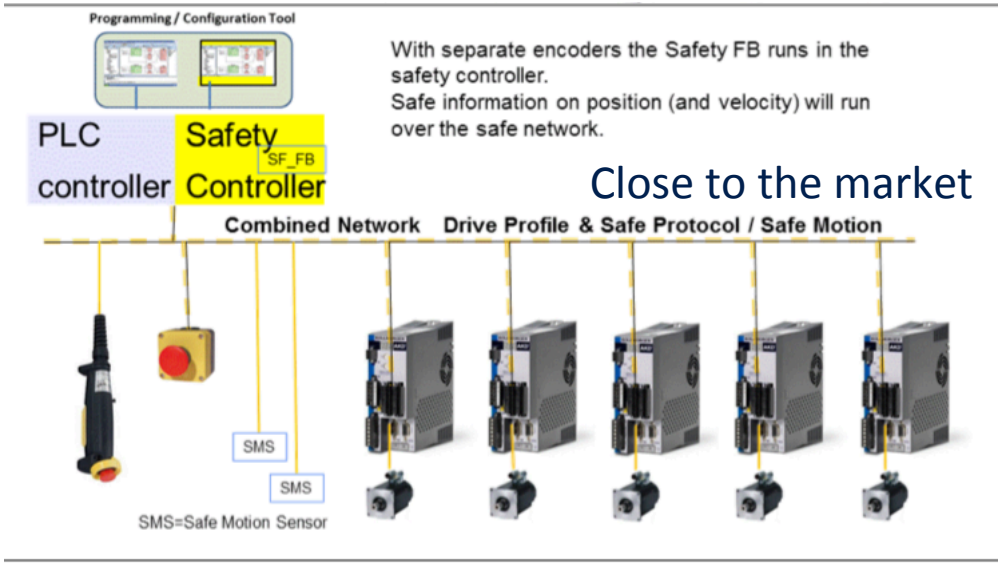
Possible Requirements:

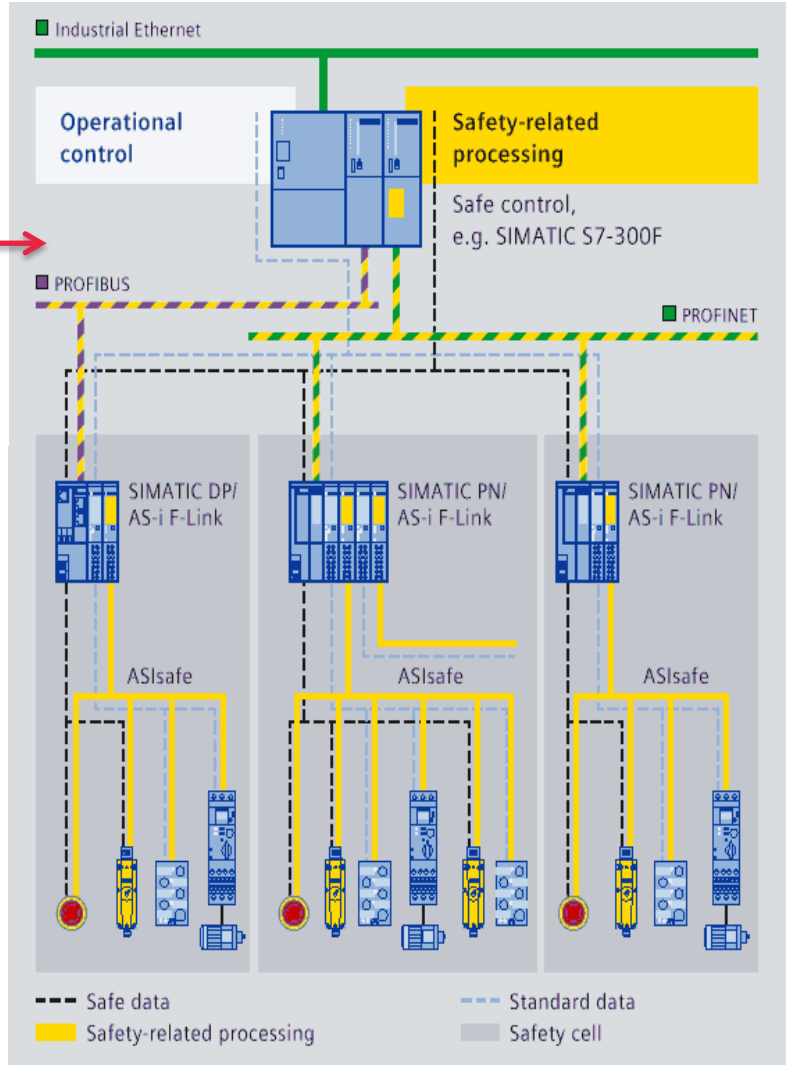
- Safety Interlocks Sensor and Actuators must be used.

- Safety logic controller must be used.

- Safety logic controller must be connected to the SAS.

Example of Implementation of Safety related system in Motion Control systems





(PLCopen)

SAS/telescope interface: how to proceed

- Approach simila to tah followed to define the camera and Telescope Assemblies Common State machine:
  - 1st Step: Distribution to the telescope Teams of the SAS concept with more details than in these slides and eventually some preliminary scenario to define better the interaction between SAS and Telescopes in case of System(CTA) hazard conditions.
  - 2nd Step:dedicated teleconf with the telescope SE to enter in the details to define a common and agreed path to define the full interface.