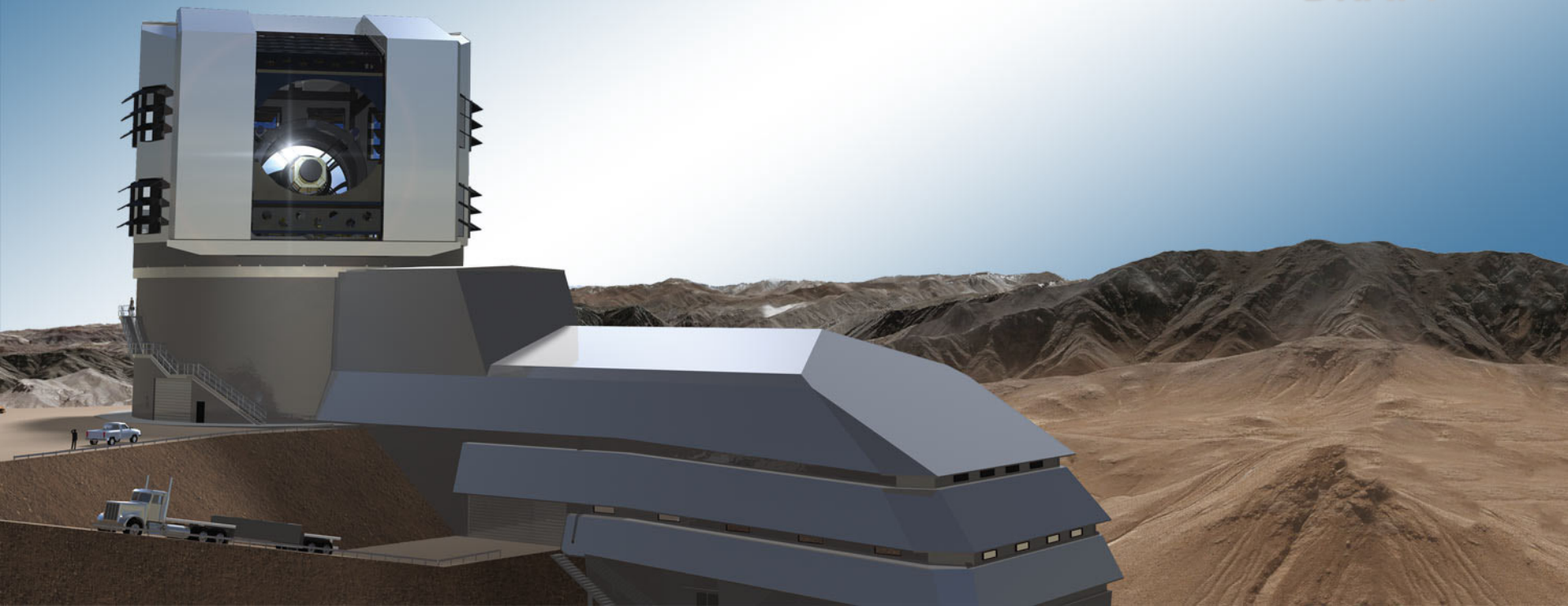
Filter Exchange System Carousel

Protection System analyze & implementation

DRAFT



Camera Hardware Protection List – LCA-140-A

Hazard ID #	State Description	Triggering Activity Activity Description	SS	Mishap Mishap Description	SS	Detection Method Detector and Location	Protective Action Action to be Taken
1	All states	Jamb, excessive friction in rotary drive train on Carousel	Exch	Stall overheats motor	Exch	Torque monitor on drive shaft; current monitor on motor	Turn off motor if it exceeds preset limits
2	All states	Jamb, excessive friction in Changer drive train	Exch	Stall overheats motor; overloading of linkage could cause buckling	Exch	Torque monitor on drive shaft; current monitor on motor	Turn off motor if it exceeds preset limits
4	All states	Driving Changer with Carousel or on-line clamps still engaged	Exch	Clamps, drive system, or filter damaged or derailed by excessive forces	Exch	Limit switches on all clamps monitor their position	Positive signal at clamp retracted position req'd to enable Changer motion
5	All states	Release of one set of filter clamps prior to the second set engaging	Exch	Filter is released and dropped, damaging either it or other hardware	Opt	Limit switches on all clamps monitor their position, with positive signal required to enable action	Release clamps on on positive enable from clamping set that they are engaged
8	All states	Hatches removed to access camera volume for servicing	Cam	Unexpected Changer motion pinches or crushes a finger	Exch	Emergency-off switch on Camera; Lock-out/tag-out procedures	Exchange system locked-out if not being serviced; Crash button stops motion in an emergency
28	All states	Power to Carousel is lost; position sensor signal lost	Exch	Filter or Carousel post collides with flip rails during rotation	Exch	Position sensors on Carousel indicate when it is correctly located for a change	Positive signal that Carousel is rotated into correct orientation req'd to enable flip rail motion; no other obstacles intefere with Carousel rotation
29	All states	Carousel stops in the wrong place for a filter change	Exch	Two filters are damaged when online filter is moved back to Carousel and collides with filter in neighboring socket	Exch	Position sensors on Carousel indicate when it is correctly located for a change	Positive signal that Carousel is rotated into correct orientation req'd to enable Changer motion
33	All states	Driving Changer with Flip Rails still flipped flat	Exch	Filter mounted to trucks is driven right off the end of the rails, causing it to collide with the Carousel	Exch	Limit switchs on flip rails positively determine their position	Positive signal that flip rails are engage is req'd to enable Changer motion
95	During a filter change	Telescope rotator starts to rotate camera		Changer jambs in track and motor stalls; filter clamps damaged	Exch	Tiltmeter and accelerometer track camera body orientation and loads	Turn off power to Exchange system

Hazard 1

Hazard ID #	State	Triggering Activity		Mishap		Detection Method	Protective Action
	Description	Activity Description	SS	Mishap Description	SS	Detector and Location	Action to be Taken
1	All states	Jamb, excessive friction in rotary drive train on Carousel	Exch	Stall overheats motor	Exch	Torque monitor on drive shaft; current monitor on motor	Turn off motor if it exceeds preset limits

- **Level 1**
  - **Motor current is limited and monitored by the motor controller**
- **Level 2 (OPT interne LSST FRANCE)**
  - **Motor temperature could be monitored by the Local Protection Module**
  - **Then LPM send a 'Quickstop signal' to the motor controller (-> 1 digital signal)**
  - **Need 1 analog data per motor**
- **Protection system operation:**
  - **In the actuator area**
  - **Real-time (continuous test when actuator enabled)**

Hazard 4

Hazard ID #	State	Triggering Activity		Mishap		Detection Method	Protective Action
	Description	Activity Description	SS	Mishap Description	SS	Detector and Location	Action to be Taken
4	All states	Driving Changer with Carousel or on-line clamps still engaged	Exch	Clamps, drive system, or filter damaged or derailed by excessive forces	Exch	Limit switches on all clamps monitor their position	Positive signal at clamp retracted position req'd to enable Changer motion

- **Answer**
  - Each carousel clamp status is checked with 2 analog sensors (-> 3 analog signals)
  - 2 offset for each clamp (-> 2 analog signals)
  - Analog signal digitized on the carousel and send to the flange with a safety-bus
- **Backup**
  - None…
    (clamp status can't be check from the static part)
  - Dedicated board for signal treatment (logic output)
- **Protection system operation:**
  - In the Filter Exchange area (Carousel/Changer)
  - Non-real-time (test before action)

Hazard 5

Hazard ID #	State	Triggering Activity		Mishap		Detection Method	Protective Action
	Description	Activity Description	SS	Mishap Description	SS	Detector and Location	Action to be Taken
5	All states	Release of one set of filter clamps prior to the second set engaging	Exch	Filter is released and dropped, damaging either it or other hardware	Opt	Limit switches on all clamps monitor their position, with positive signal required to enable action	Release clamps on on positive enable from clamping set that they are engaged

- **Answer**
  - **Each carousel clamp status is checked with 2 analog sensors (-> 3 analog signals)**
  - **Analog signal digitized on the carousel and send to the flange with a safety-bus**
- **Backup**
  - **None…**
    (clamp status can't be check from the static part)
- **Protection system operation:**
  - **In the Filter Exchange area (Carousel/Changer)**
  - **Non-real-time (test before action)**

Hazard 28

Hazard ID #	State	Triggering Activity		Mishap		Detection Method	Protective Action
	Description	Activity Description	SS	Mishap Description	SS	Detector and Location	Action to be Taken
28	All states	Power to Carousel is lost; position sensor signal lost	Exch	Filter or Carousel post collides with flip rails during rotation	Exch	Position sensors on Carousel indicate when it is correctly located for a change	Positive signal that Carousel is rotated into correct orientation req'd to enable flip rail motion; no other obstacles intefere with Carousel rotation

- **Answer**
  - **No power for the Carousel mean no rotation**
  - **Carousel is set in rotation only if there is no obstacles**

- **Comment:**
  - **No more 'Flip rail' in the design**
  - **Carousel rotation enable only when changer is online (and stop)**
  - **Carousel will use an absolute encoder to know the current position**

Hazard 29

Hazard ID #	State	Triggering Activity		Mishap		Detection Method	Protective Action
	Description	Activity Description	SS	Mishap Description	SS	Detector and Location	Action to be Taken
29	All states	Carousel stops in the wrong place for a filter change	Exch	Two filters are damaged when online filter is moved back to Carousel and collides with filter in neighboring socket	Exch	Position sensors on Carousel indicate when it is correctly located for a change	Positive signal that Carousel is rotated into correct orientation req'd to enable Changer motion

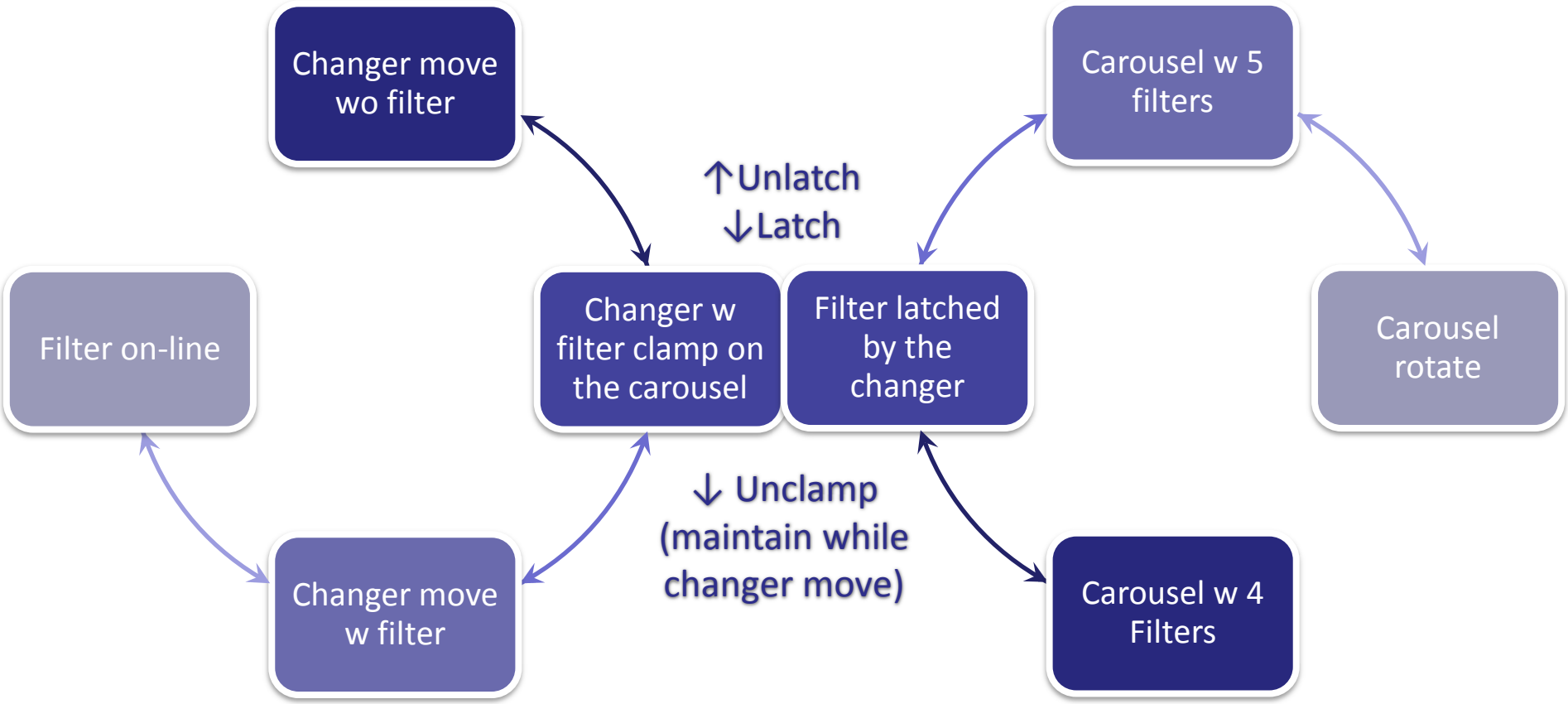
- **Level 1**
  - **Carousel will use an absolute encoder to know the current position**
- **Level 2**
  - **Sensor on the carousel to detect the exchange position for each socket**
  - **Need 5 digital signals (redundant)**
- **Protection system operation:**
  - **In the Filter Exchange area (Carousel/Changer)**
  - **Non-real-time (test before action)**

Hazard 95

Hazard ID #	State	Triggering Activity		Mishap		Detection Method	Protective Action
	Description	Activity Description	SS	Mishap Description	SS	Detector and Location	Action to be Taken
95	During a filter change	Telescope rotator starts to rotate camera		Changer jambs in track and motor stalls; filter clamps damaged	Exch	Tiltmeter and accelerometer track camera body orientation and loads	Turn off power to Exchange system

- **Level 1**
  - **Filter-exchange Control System stop the system in a secure position**
- **Level 2**
  - **Master Protection Module send a 'ES signal' to LPM**
  - **LPM send a 'Quickstop signal' to the motor controllers (-> 1 digital signal)**
- **Protection system operation:**
  - **Global: Camera area**
  - **Real-time**

Exchange Sequence



Carousel constrains

- **Encumbrance on the carousel**
  - **Need 30 analog inputs + 5 digital inputs (redundant) + some I/O TBD…**
  - **Limited space between filters (lots safety PLC of are too big to fit)**

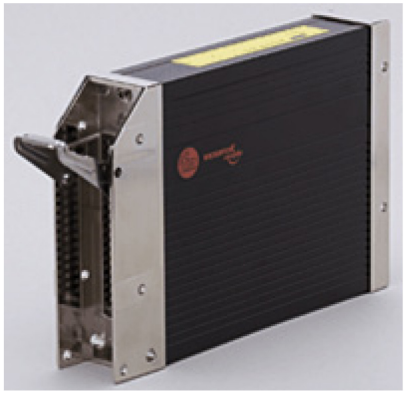
- **Rotation of the carousel**
  - **Need reliable link between moving and static part for signal (error check…)**
  - **Need power supply on the carousel (sensors, I/O, …)**
  - **Encumbrance of electrical contacts depends on the number (and the current)**
  - ➢ **One digital link (differential) + one power supply**

- **Encumbrance in the back flange**
  - **Need (3 temperature inputs +) 6 digital outputs + 3 relay outputs + some I/O TBD…**
  - **Space limited by flange-cells (lots safety PLC of are too big to fit)**
  - **Cabling : point to point wiring is space consuming**
    - Fieldbus will be preferred

- **Power consumption in the camera body**

Safety contoller…

- Safety controller in the utility trunk
- Connect with the safety I/O with a safety fieldbus



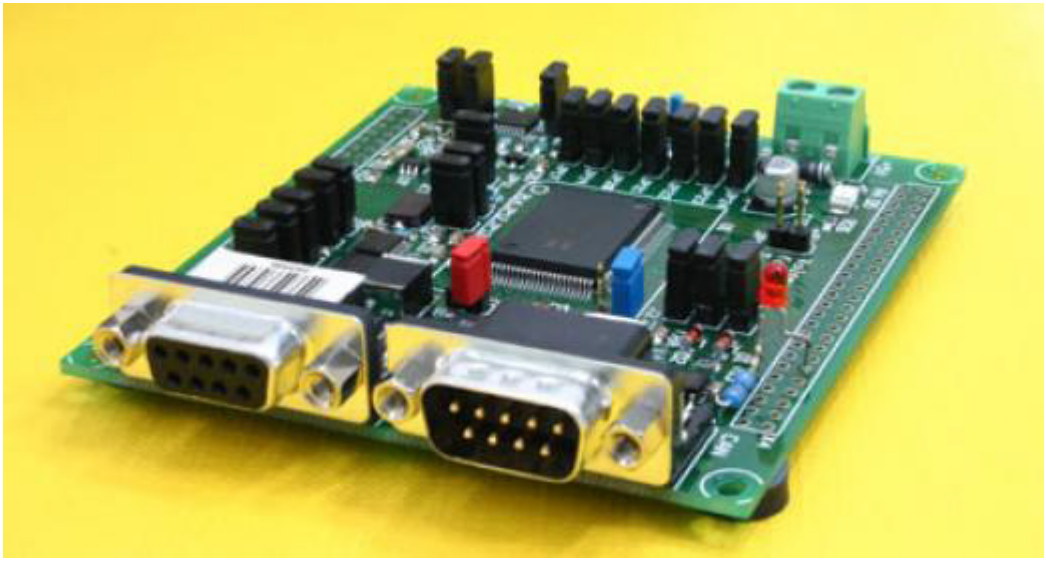
- Ifm: CR7021
  - R360/SafetyController/13849

- Intercontrol: digsy® compact-S
  - redundant safety control system

- STW: ESX-3XM
  - designed for safety-related applications

Safety I/O…

- **Board using CSC02 safety chip**

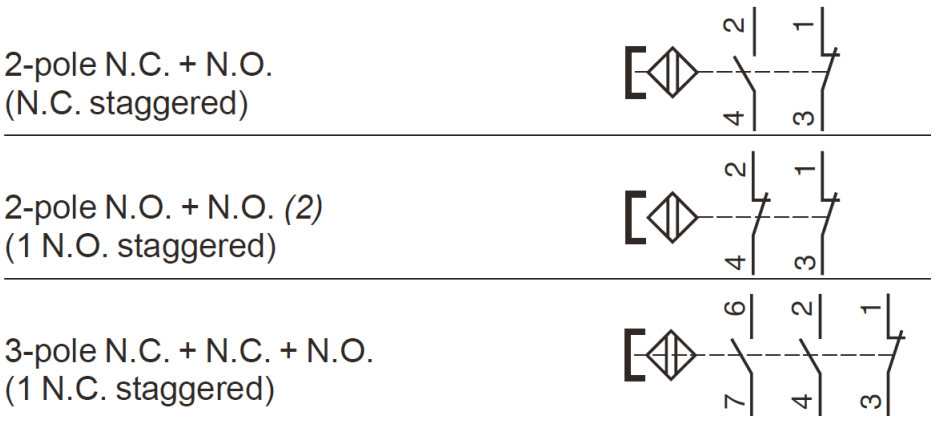


Safety Relay…

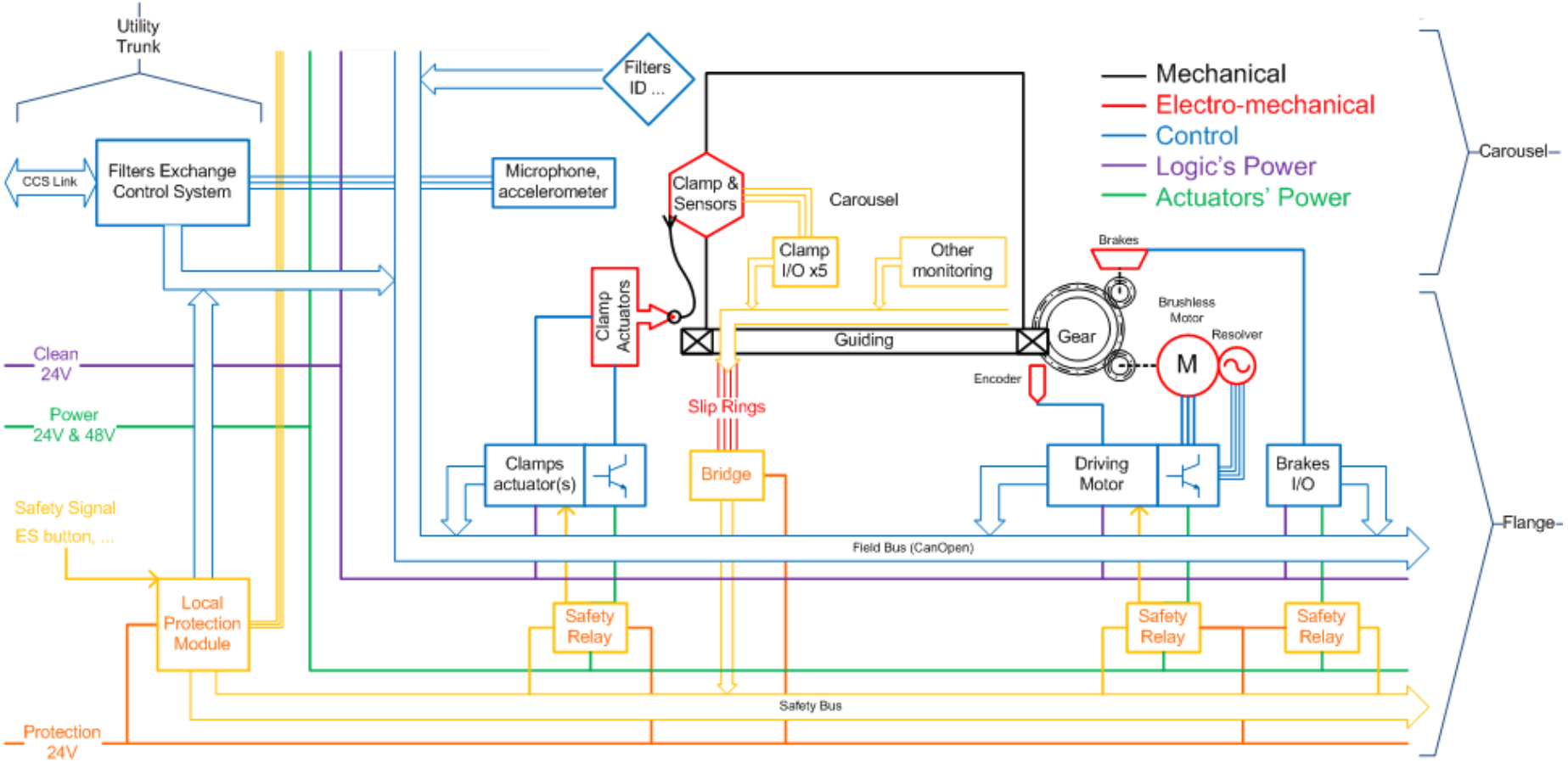
- **Safety relay for emergency stop with adjustable delay time**
  - **Ex: PSR-SCP- 24DC/ESD/4X1/30**

Socket sensors…

- **Non contact coded safety switch**
- **Read by the safety I/O**



Control and protection system schematic



Filter Exchange Operations

- **Carousel rotation**
  - **Changer stopped in ON-LINE or Hand-Off position**
    - ➢ Changer configs = TBD

- **Unclamping**
  - **Carousel rotation stopped in a socket**
  - **If filter engaged in standby socket:**
    - Changer in stand-by position
    - Truck Filter Engaged
    - Latch Lock
    - ➢ Changer config = TBD
  - ➢ **Hazard 5**

Protection System Logic

Filter Exchange Operations

03-sept-10

Sensor Status Required for Operation

Definitions: LS = limit switch HE = Hall effect sensor An = analog Bin = binary 1 = switch closed F = filter I.D. code S = carousel socket I.D. code

Actuator:					Carousel Rotary Drive			Clamp Release					Linear Actuator								Truck Latch						On-Line Latches						Slide					Clamp	MPS						
Component:		Protection System			Carousel Sensors								Auto Changer Sensors																				Manual Changer Sensors											
Sensor type:					An	An	S=0-5	An	An	An	An	An	F=0-7	An	An	Bin	Bin	Bin	Bin	F=0-7	F=0-7	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin	Bin
Operation		Carousel Configuration	Auto changer Configuration	Loader Configuration	Carousel motor current monitor	Carousel rotary position sensor	Carousel socket identification H-E sensors (3)	Carousel brake shoe current monitor	Lock clamp status: UNLOCKED (1 x 2 clamps)	Lock clamp status: LOCKED (1 x 2 clamps)	Filter Clamp Presence Status : LOCKABLE (1 x 2 clamps)	Filter Clamp Presence Status : NO FILTER (1 x 2 clamps)	Filter identification H-E sensors (3)	Changer motor current monitor	Changer linear actuator absolute position encoder	Linear rail ON-LINE LS (1 x 2 rails)	Linear rail STAND-BY LS (1 x 2 rails)	Filter position Online x2 (HE)	Filter position Hand-Off x2 (HE)	Filter position Stand By x2 (HE)	Filter identification H-E sensors (3) On-Line	Filter identification H-E sensors (3) - Hand Off	X+ truck Filter ENGAGED HE	X- truck Filter ENGAGED HE	X+ Latch Lock H-E sensor	X+ Latch UnLock H-E sensor	X- Latch Lock H-E sensor	X- Latch UnLock H-E sensor	X+ Online clamp ENGAGED LS	X+ Online clamp DISENGAGED LS	X- Online clamp ENGAGED LS	X- Online clamp DISENGAGED LS	Y- Online clamp ENGAGED LS	Y- Online clamp DISENGAGED LS	Loader Mounted on the camera - sensor	Loader master enable switch	Video camera mounted on slide	Filter slide INSERTED into autochanger LS	Filter slide RETRACTED LS	Filter latch clamp UN-CLAMPED H-E sw	Filter latch clamp CLAMPED ON FILTER H-F sw	Filter latch clamp solenoid current monitor	Master Permit	RotZ digital level - Permit from MPS	RotX digital level - Permit from MPS	Hatch sensors for camera acces	Latches Relay	On-Line clamps relay	Linear rail Relay
Protection System	Hazard ID																																										
Standard Operations With the Loader																																											
Latches Relay ON																																											
Open Latches Hand Off position	5 - (8-95)		A1	L1														1				1	1												1		1		1		1	1	1	0	
Close Latches Hand Off position	5 -(8-95)		A1	L1														1				1	1												1		1		1		1	1	1	0	
Linear Motor Relay On																																											
With Filter																																											
Any displacement Carousel socket empty	4 - 29 - (8-95)	C1	A2	L2		1				1		1										1	1	1		1		1	1	1				1			1				1	1	1	0	
Any displacement Carousel socket with filter	4 - 29 - (8-95)	C2	A2	L2		1			1													1	1	1		1		1	1	1				1			1				1	1	1	0	
Without Filter																																											
Any displacement	4 - (8-95)		A3	L2																					1		1								1			1				1	1	1	0	
Standard Operations Without the Loader																																											
Latches Relay ON																																											
Open Latches Stand By position	5 - (8-95)	C3	A4							1	1								1			1	1																			1		1	0	
Close Latches Stand by position	5 - (8-95)	C3	A4							1	1								1			1	1																			1		1	0	
Linear Rail motor																																											
With Filter																																											
From On-Line to Stand-by	4 - 29 - (8-95)	C1	A2			1				1		1										1	1	1		1		1	1	1											1		1	0	
From On-Line to an other position	4 - 29 - (8-95)	C1	A2			1				1		1										1	1	1		1		1	1	1											1		1	0	
From Stand by to Online	4 - 29 - (8-95)	C2	A2			1			1													1	1	1		1		1	1	1											1		1	0	
From Stand by to an other position	4 - 29 - (8-95)	C2	A2			1			1													1	1	1		1		1	1	1													1	0	
From an other position to Stand By	4 - 29 - (8-95)	C1	A2			1				1		1										1	1	1		1		1	1	1											1		1	0	
From an other position to On Line	4 - 29 - (8-95)	C2	A2			1			1													1	1	1		1		1	1	1											1		1	0	
Without Filter																																											
Any displacement	4 - (8-95)		A3			1																			1		1															1		1	0	
Clamp Online Relay On																																											
Close OnLine Clamps	4 - (8-95)		A5														1					1	1	1		1															1		1	0	
Open Online Clamps	4 - (8-95)		A5														1					1	1	1		1															1		1	0	

Check specs for the carousel

C-EXCH-151	The local HPU and LPM shall have a power source separate from that powering local HCU's and non-protection elements	~ OK (~ 151 ?) *
C-EXCH-152	Local HPU power shall be unswitched ("always on")	OK (≠ 156 ?)
C-EXCH-153	Local HPU power feeds shall be independent of other power feeds supplying the subsystem	~ OK (~ 151 ?) *
C-EXCH-154	The LPM logic shall include a master inhibit to all loads for a full "off" state of the hardware.	~ OK
C-EXCH-155	The master inhibit signal shall be the default state of the LPM so when power is lost or the LPM ceases to function, all hardware will be inhibited from functioning	OK
C-EXCH-156	The local HPU and LPM shall either be always on when voltage is applied, or turn on independent of the control system HCU.	~ OK (≠ 152 ?)
C-EXCH-157	The LPM shall provide a master status signal and status of all permit/inhibit signals to the local HCU for monitoring and communication to the CCS. This can either be done with direct wiring or through a network.	OK
C-EXCH-158	Sensors and switches shall not be shared by control and protection systems.. Splitting of the unamplified signal, cross-strapping of the conditioned signal to both the HPU and HCU, and using the HCU or other non-protection system hardware is expressly prohibited	? **
C-EXCH-159	Protection system signals that are needed as part of the control system functionality shall be read out and conditioned within the HPU/LPM only, then sent to the HCU as telemetry.	~OK (delay !?!)
C-EXCH-160	LPM protection logic shall rely solely on binary switching logic and/or locally-coded programming logic only. Control by remotely-loadable software or software hosted on the local HCU is expressely prohibited.	~ OK Safety controller ?
C-EXCH-161	Communication among local protection system elements (e.g.: from sensors to the HPU) shall not use publish/subscribe protocols nor any system. network shared by elements that are not part of the protection system. By definition, hardware and protocols used for communication between protection system elements are themselves part of the protection	? **
C-EXCH-162	Only positive signals shall be used in protection system logic. Thus, a zero-voltage or zero-current condition can never be confused with a loss of signal or damaged sensor.	OK (analog ?) (short circuit ?)
C-EXCH-163	Local protection system hardware components that operate through "action-on-demand," shall be safety-rated components per Ref. [XXX] with a safety integrity level (SIL) of TBD.	?
C-EXCH-164	Local protection system hardware components, including wiring, connectors, and boards, shall be fail-safe from loss of function. Thus, failure of a component shall result in the dropping of a permit signal and never result in a bypassing or lack of protection functionality.	~ OK
C-EXCH-165	Local protection system hardware components and assemblies shall have the same reliability as other single-failure point components in the subsystem. Since the subsystem can only be operated when the protection system is functioning properly, it must exhibit the same reliability as other key components in the subsystem, to reduce the likelihood of downtimes.	~ OK
C-EXCH-002	All powered latches and actuators or release mechanisms shall be fail-safe from sudden loss of power	OK
C-EXCH-005	Protection from mechanical and electrical failure shall be handled locally in the Filter Exchange hardware	OK
C-EXCH-166	The filter exchange subsystem shall comply with the ICD to the Master Protection Module (LCA-293)	?

Some Issues…

- **Sequence management (interne LSST FRANCE)**
  - **Exchange of the filter is a tricky point for the protection system**
- **Sensor telemetry send to the FCS**
  - **FCS is not independent from the protection system (read input)**
  - **Delay…**
- **Power consumption of the protection system…**
- **Mass of the protection system hardware…**
- **Diagnostic LED on ‘all’ hardware…**