A Systematic Approach to Developing Safe Tele-operated Robots

Diego Alonso, Pedro Sánchez, Bárbara Álvarez and Juan A. Pastor

UPCT. Grupo DSIE

Table of contents

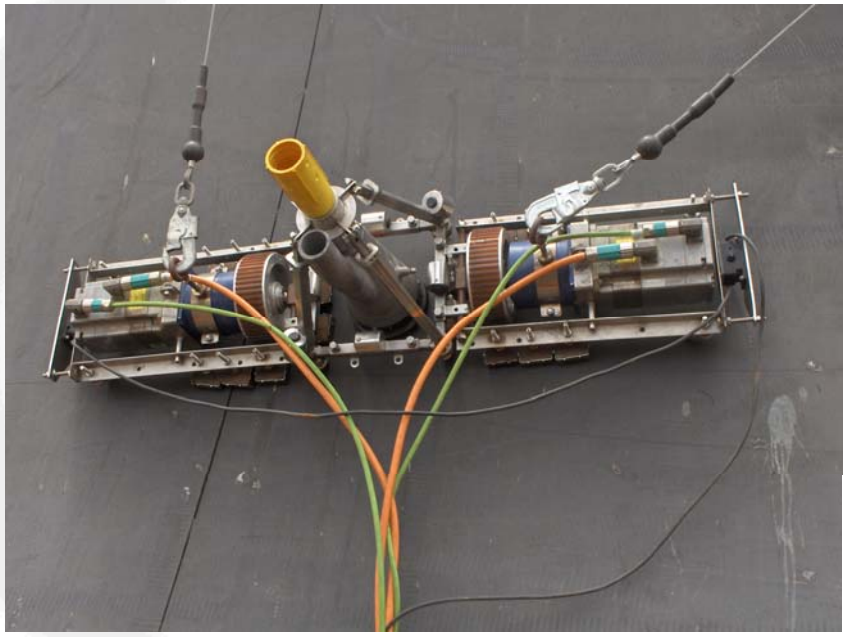
The EFTCoR Project

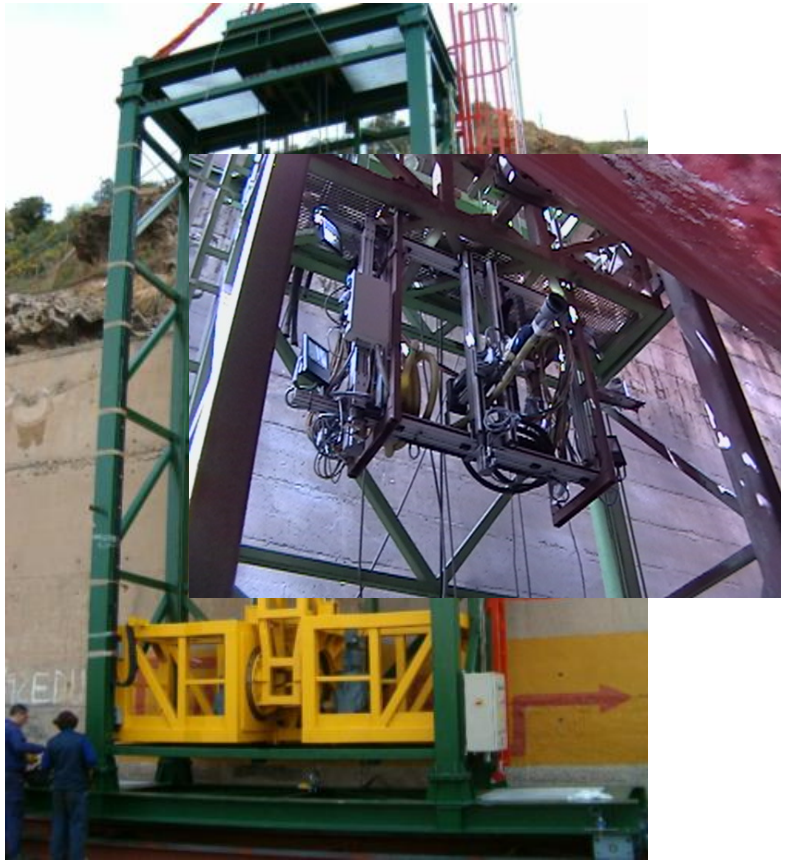
EFTCoR
Environmental Friendly and Cost-effective Technology for Coating Removal

Environmental friendly and cost-effective technology for coating removal. (GROWTH-V UE) + Special Action from spanish MCyT 2002/2005

Our solution

- Two product lines:
  - Climbing vehicles for spotting (discrete cleaning)
  - Cranes for full blasting (big area)





But ...

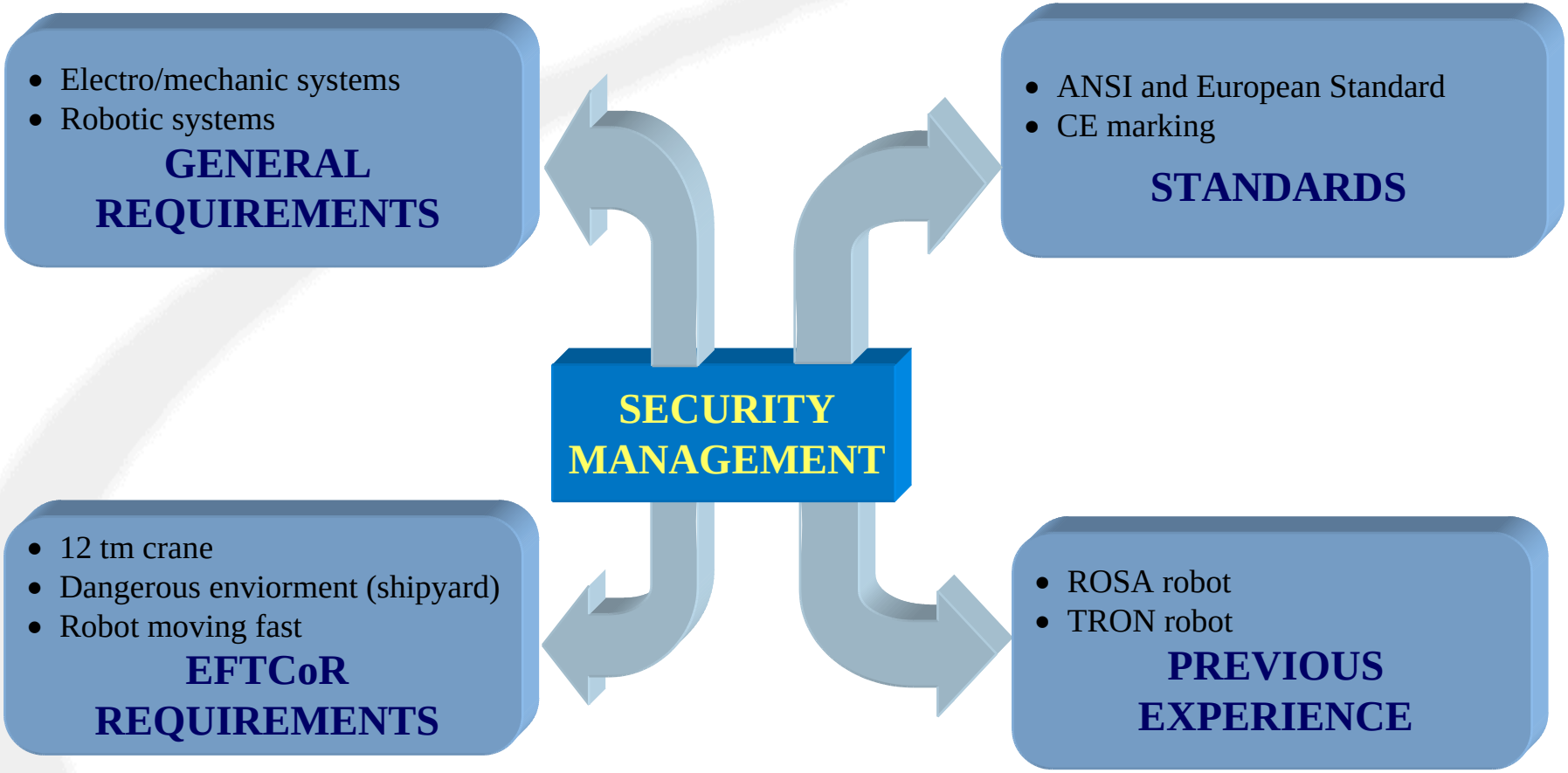
- The shipyard is the working place! (noise, water, heavy cargo moving, ...)

- Outdoors (wind, rain, dust)
- Use of abrasive material at high pressure
- Heavy robots moving
- and more ...

Thus ...

- The safety requirements for these kind of systems need a thorough study.
- The influence of these requirements in the development of the system is crucial.
- So it is needed:
  - A method to discover the safety requirements.
  - A set of specific patterns to allow their representation in a way orthogonal to the rest of the requirement
- What will be the impact of safety in the architecture of the system?

Starting point



Standards and Techniques

- EN 61508:2001
  - European Standard. For electric/electronic/programmable devices.
  - Serve as basis for other specific standards (hopefully robotics).
- ANSI/RIA R15.06-1999:
  - American National Standard for Industrial Robots and Robot systems: Safety Requirements.
  - More specific than EN 61598.
- ROPES. Bruce Powell Douglass
  - Rapid Object-Oriented Process for Embedded Systems.
  - Includes an 8-steps methodology for safety.

Step 1 → ANSI/RIA

Description and classification of the tasks of the robot

Task #	Type	Description
T1	Operator	Move primary system (rail)
T2	Operator	Move primary system (vertical axis)
T4	Operator	Cordinate the movement of the primary to position the secondary
T5	Operator	Move the secondary (XYZ table)
T9-10	Operator	Turn on/off the blasting tool
T12-14	Operator	Stop the movement of the primary/secondary
T16	Operator	Change movement parameters
T17	Operator	Change mode
T20	Maintenance	Calibration of the primary system
T21	Maintenance	Calibration of the secondary system
T24-25	Maintenance	Manually mount or dismount a tool
T27	Maintenance	Repair blasting infrastructure
T28	Maintenance	Repair communication infrastructure

Step 1 ➡ ANSI/RIA

Task identification helps hazard discovery:

- The movement of mechanical components, especially those which can cause trapping or crushing.
- Stored energy in moving parts, electrical or fluid components.
- Power sources: electrical, hydraulic, pneumatic.
- Acoustic noise, vibrations, EMI, etc.
- Human failures in design, construction, installation, and operation, whether deliberate or not.
- Hazardous atmospheres, material or conditions: explosive or combustible, radioactive, high temperature and/or pressure, etc.

Step 1 → ANSI/RIA

Hazard	Task	Risk level	Source	Prob	Reaction
H1. The tool hits the hull	T5-7, T21	Severe	Breakage or control error of the tool axis. Comm failure (logic or physic)	Low	Raise alarm. Stop the tool and move apart the tool. Interrupt power source
H3. Person in the rail	T1	Very severe	There's a person standing on the rail in the path of the primary	Med.	Raise alarm. Emergency stop
H6. Obstacle in the secundary	T5-8, T21	Very severe	There's an abstacle in the path of the secondary	Low	Raise alarm. Emergency stop
H7. The limit switch of the primary is passed	T3-4, T20	Very severe	Sensor breakage or software error. Comm failure (logic or physic)	Low	Raise alarm. Emergency stop
H10. The secondary hits the hull or falls down.	T1-3, T4,T8, T20	Severe	Error in the trajectory calculation of the secondary. Operator error moving the tool. Aproximation sensor or limit switch error or breakage. Power source interruption	High	Raise alarm. Interrupt power source
H13. The primary does not stop	T1-4, T8, T12, T13, T20	Very severe	Control software error. Comm failure (logic or physic). Power source interruption	Low	Raise alarm. Emergency stop. Interrupt power source
H14. The sequence of the secundary does not end	T7, T21	Slight	Sequence software control error. Comm failure (logic or physic)	Low	Raise alarm. Stop secondary and tool
H15. The sequence of the primary does not end	T8, T12-T13, T20	Very severe	Sequence software control error. Comm failure (logic or physic)	Low	Raise alarm. Stop primary
H31. Temperature above the operating range	All	Severe	Extreme environmental conditions: heat or cold	Med.	Emergency stop. Note down the incidence

Step 2 ➡ ANSI/RIA + safety patterns

Identify risks + severity and probability

Hazard	Risk	Severity	Exp	Avoidance	Risk Red. Cat.	Solution	Exposure	Avoidance	Severity	Risk Reduction Cat.
H1. The tool hits the hull	Tool or secondary mechanism breakage	S1	E2	A1	R3A	Add contact sensors to the head of the tool. Limit the torque in Z axis	E1	A1	S1	R4
H3. Person in the rail	Run over a person	S2	E2	A1	R2A	Add presence detectors along the rail to detect obstacles or persons. Activate a siren when the primary moves along the rail	E1	A1	S2	R3B
H6. Obstacle in the secundary	Damage to the secondary or tool	S2	E1	A1	R2B	Torque monitoring to detect that the secondary is not moving	E1	A1	S1	R4
H7. The limit switch of the primary is passed	Damage to equipment or primary or persons	S2	E1	A2	R2B	Add mechanical limits	E1	A1	S1	R4
H10. The secondary hits the hull or falls down.	Damage to equipment or secondary or persons	S2	E2	A2	R1	Definition of a precise procedure of approximation to the hull. Add proximity sensors to the secondary	E1	A1	S2	R3B

Analisys of a hazard: an example

Hazard. H13: the primary system does not stop

Involved tasks. T1-4, T8, T12, T13, T20

Risk level. Very severe

Hazard source. Error in the control software of the primary.Error Communication failure (either logical or physical). Power failure

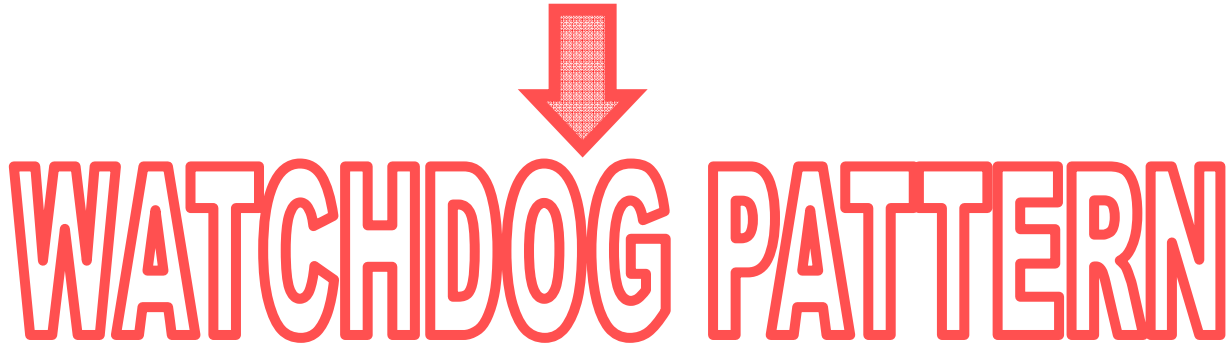
Probability. Low

Reaction. Raise alarm. Interrupt power souce. Emergency stop

Risk. Damage to the primary or persons or equipment. The severity is serious (S2), the exposition level is not frequent (E1) and the possibility of avoidance is low (A2)

Risk reduction category. R2B

Solution. Add mechanisms to make an emergency stop and movement detectors independent and outside the control loop (compliant with 6.4 ANSI)

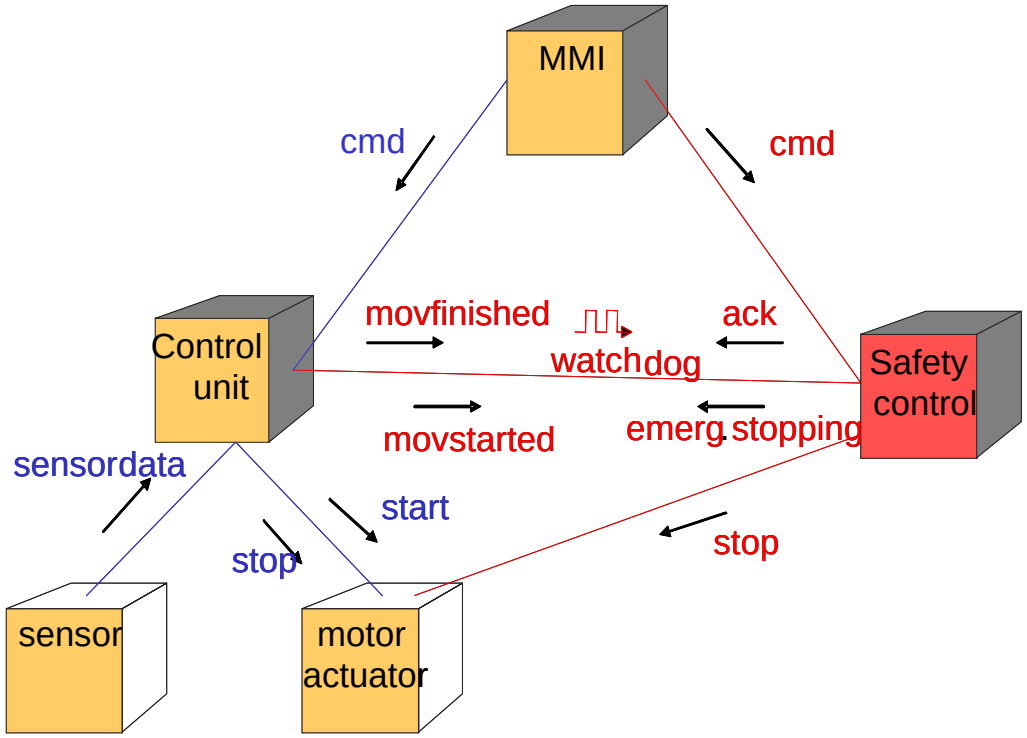


The primary system doesn't stop !

1. When a movement command is received, the *MMI* node forwards it simultaneously to the *Control Unit* (that will execute it) and to the redundant node (*Safety Control*).

2. The *Control Unit* reads periodically the current position of the joint from a sensor and controls the actuator. The *Safety* node is in charge of stopping the motor when it detects that the motor is not working properly.

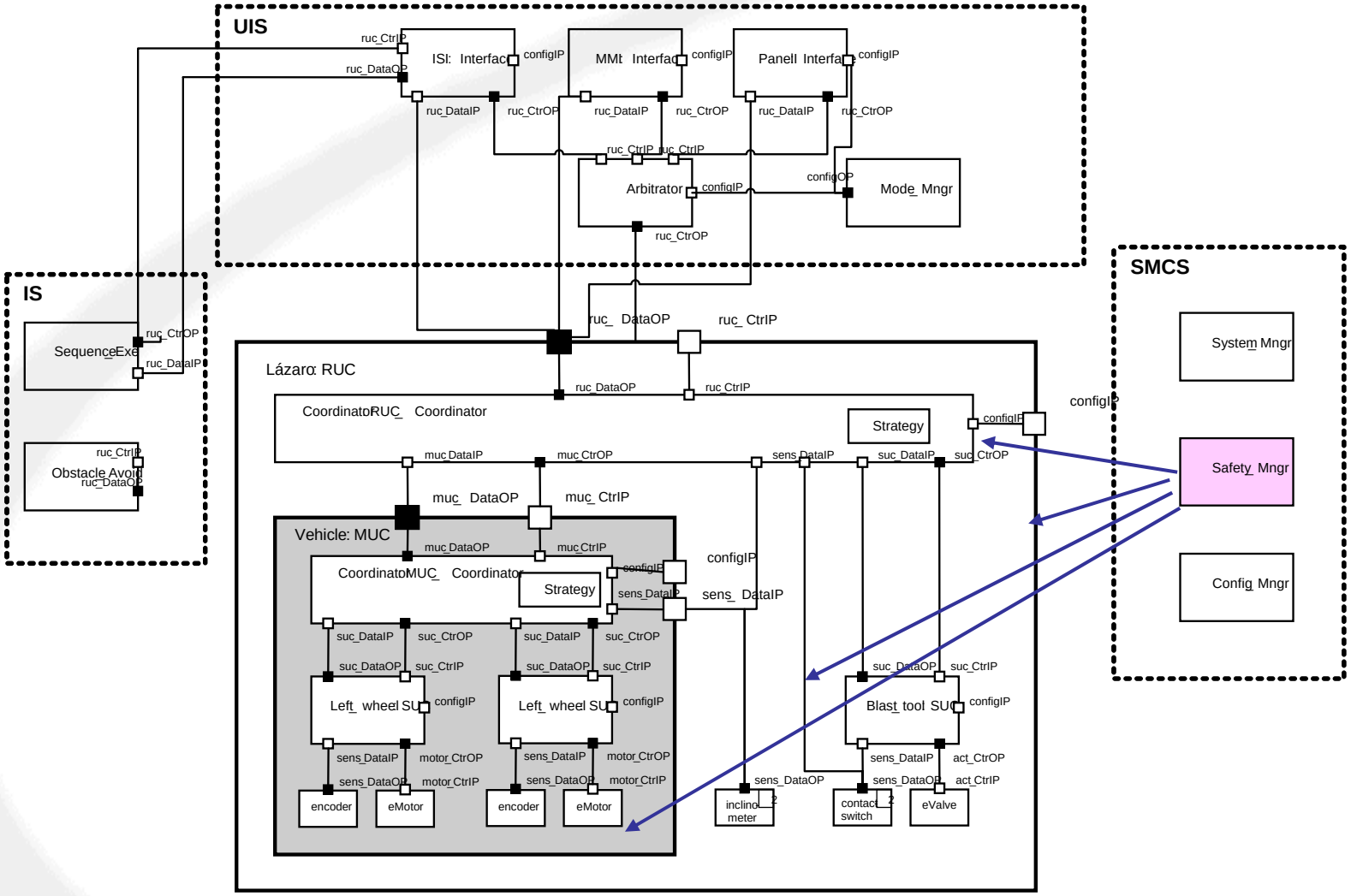
3. Just before any movement, the *Control* node sends a message to the *Safety* node, which will monitor the movement.



Ada representation

Node	TASK	Does its main function
Watchdog	TASK	Synchronous rendezvous with timeout
Access to hardware	PROTECTED OBJECT	Periodically updated
Real time issues	-	Nodes and wathdog are periodic tasks.

How does safety affect the system architecture?



How does safety affect the soft. arch.?

	KIND OF SOLUTION	HAZARDS	%
The solution implies changes in the architecture of the system	Additional software control module in the Control Unit	H2, H14, H16, H17, H21	**8.33%**
	Added safety elements controlled by software, such as emergency stop, siren, presence detectors,...	H1, H2, H3, H3, H4, H4, H5, H10, H12, H12, H13, H13, H15, H15, H21, H22, H25, H25, H24, H26, H26, H28, H31, H27	**40%**
	Redundant elements, independent from the control loop, in the Control Unit	H10, H23, H5, H11	**6.66%**
			Sub-total 55%
The solution does not affect the architecture of the system	Inclusion of electric or mechanic limits	H1, H6, H7, H8, H9, H18, H18, H19	**13.33%**
	Develop of a procedure of use and signal	H10, H24, H24, H28, H31, H25, H26, H27, H28, H28	**16.66%**
	Use of certified material, according to safety standards (connectors, wires, ...)	H20, H20, H21, H21, H26, H29, H30, H30, H31	**15%**
			Sub-total 45%

This is more than “glued” standards

1. It gathers the methodologic experience of diverse authors, usually absent from standards

2. The application covers more than what a single standard/technique offers:
   - Requeriments specification
   - Architectural design

3. 66 safety requirements were added to the specification.

Conclusions

- The analysis of hazards is a complex procedure that needs a specific methodology.

- Although there's no single standard for robotics, we have shown how the **ANSI** can be complemented with the **ROPES** methodology.

- The system is rich and complex enough to be able to extract important conclusions:

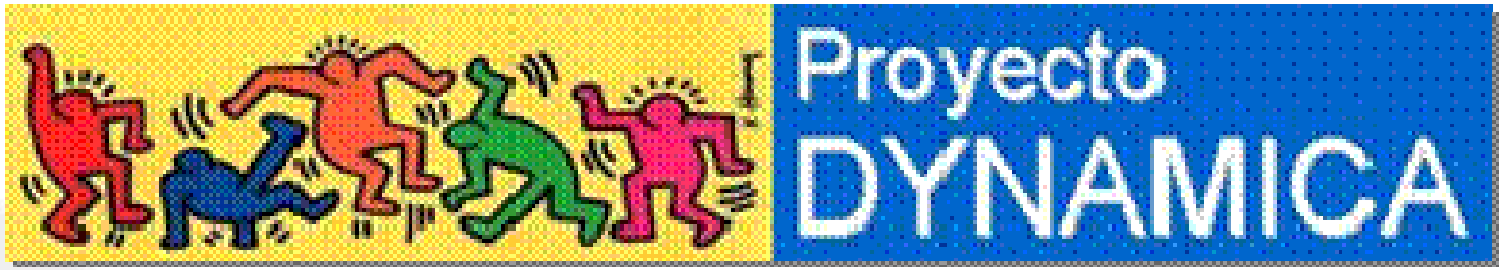
  55% of the identified safety requirements directly affect the software control architecture of the robot.

  7% need a reduntant, extern control loop with the strictest safety levels (deep modification).

Future work

Since safety requirements are, conceptually, independent of the functional ones, it would be more than desirable to have an architectural approach that allows:

- The conceptual separation of concerns.
- A catalogue of requirements and its dependencies
- The traceability of requirements, from specification to architecture.



Thank you for your attention