An overview of the Embedded Systems unit at Fondazione Bruno Kessler

Alessandro Cimatti

Fondazione Bruno Kessler

Center for Information Technology – IRST

Head of Embedded Systems Unit

cimatti@fbk.eu

Overview

- Fondazione Bruno Kessler
  - Non-profit private research foundation in Trento
  - Formerly Istituto Trentino di Cultura/IRST
  - Two hubs: humanities and technologies
- Center for Information and Communication Technology
  - Director: Paolo Traverso
  - Research units, coordinated in research lines
  - RL: Adaptive, Reliable and Secure Systems
- The Embedded Systems Unit
  - About 25 people
  - 7 research staff, 7 postdocs, 8 programmers, 6 ph.d. students

Mixing Research and TT

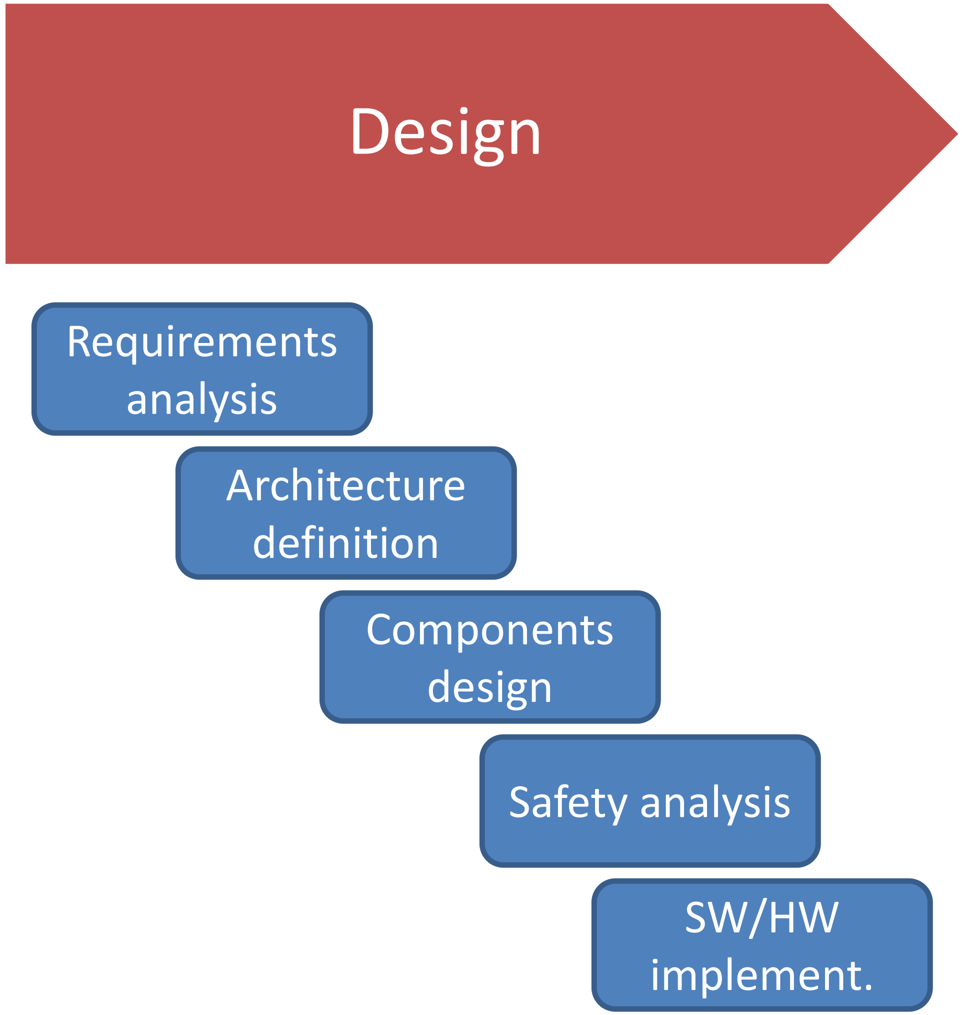
- Strategy: tight integration of
  - Basic research
  - Tool development
  - Technology transfer
- Funding sources
  - H2020
  - European Railway Agency, European Space Agency
  - NASA NextGen
  - Industrial players
    - Aerospace
    - Railways
    - energy
    - oil and gas
- Since 2008, between 60% and 80% self funding

Our activities

- Support Model-based design with formal methods
  - Find more bugs, earlier in design flow, certify correctness
  - Areas
    - Functional verification (traditional)
    - Dependability (FTA, FMEA) assessment
    - Requirements analysis

- Model based autonomous reasoning
  - Planning and scheduling
  - Execution monitoring
  - Fault detection, identification and recovery (FDIR)

Life Cycle of Complex Systems

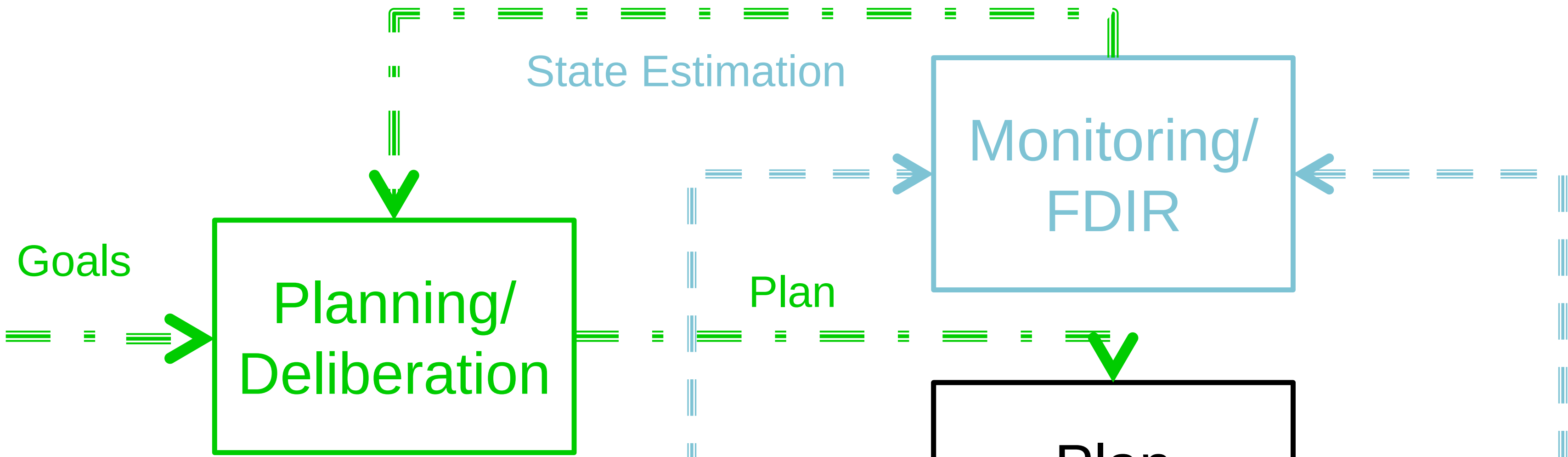


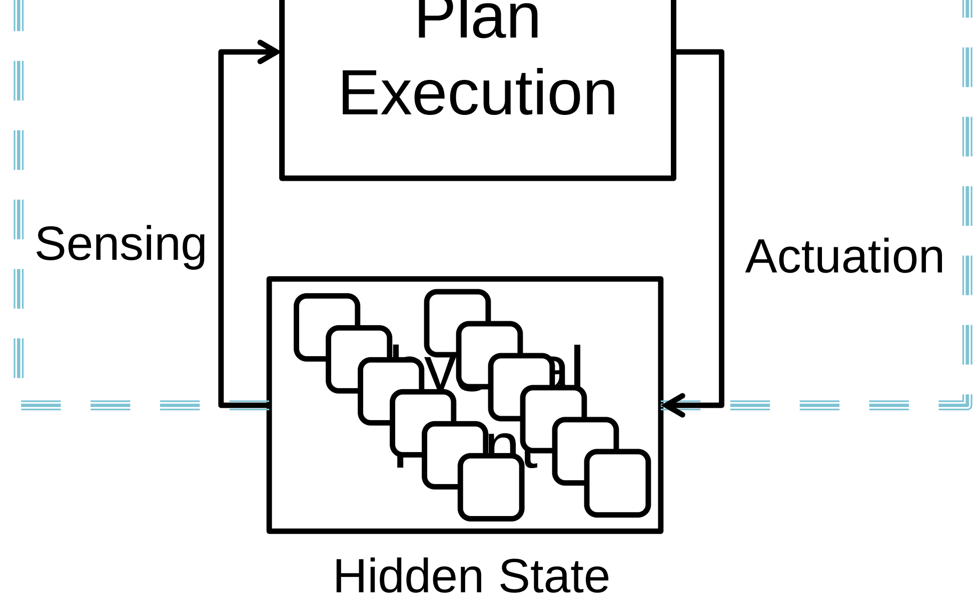
- How do we support the design?
- Requirements validation:
  - Are the requirements flawed?
- Functional correctness
  - Does the system satisfy the requirements?
- Safety assessment
  - Is the system able to deal with faults?

From design to operation…

- Planning
  - plan how to achieve desired “firing” sequence
  - retrieve pipes from holds, pre-weld, send to firing line, final weld
- Execution Monitoring
  - welding may fail, activities can take more time than expected
  - plant may fail
- Fault Detection, Fault Identification/Isolation
  - is there a problem? where is it?
- Fault Recovery
  - put off-line problematic equipment
- Replanning
  - identify alternative course of actions, e.g. reroute pipes

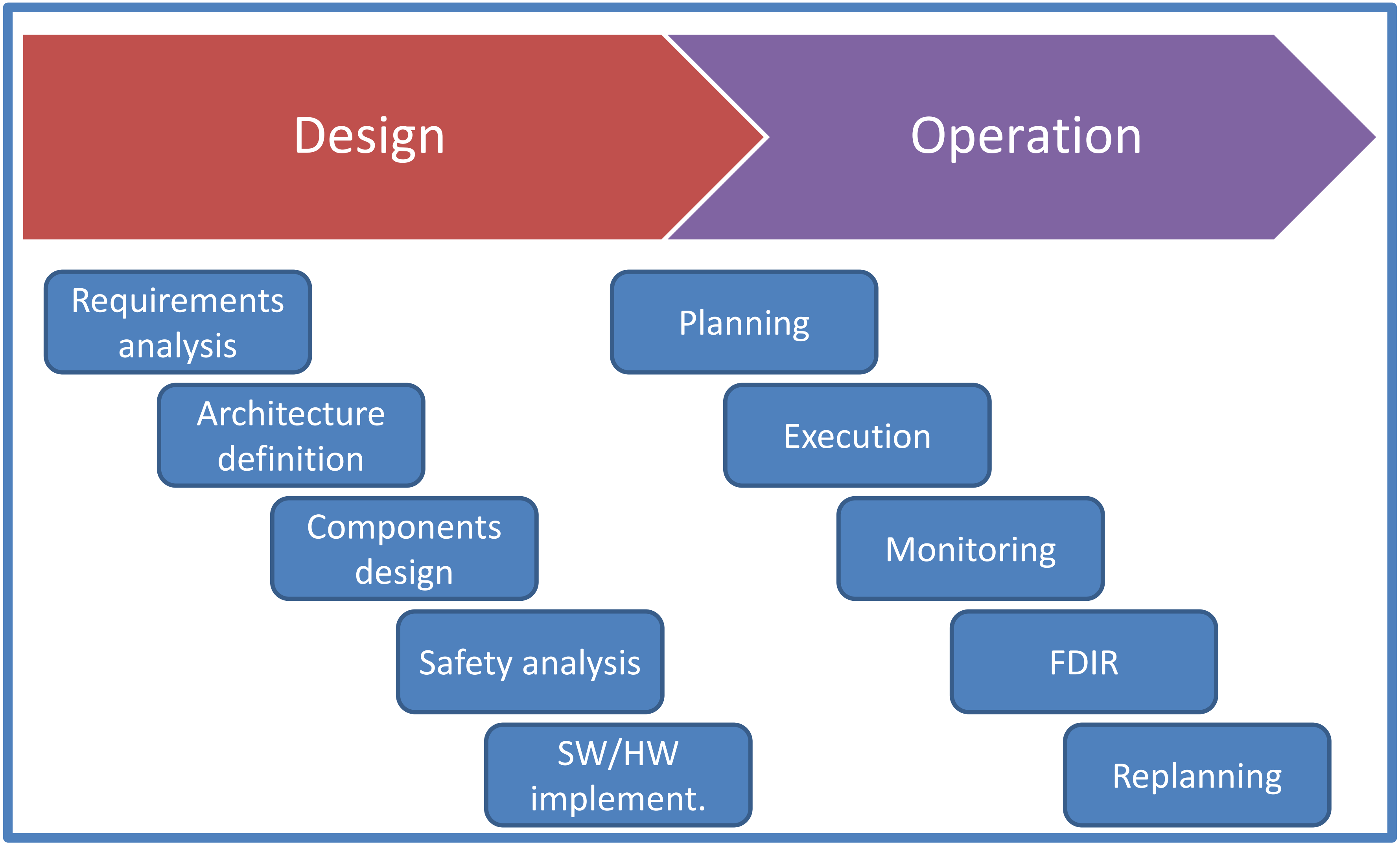
Complex systems operation





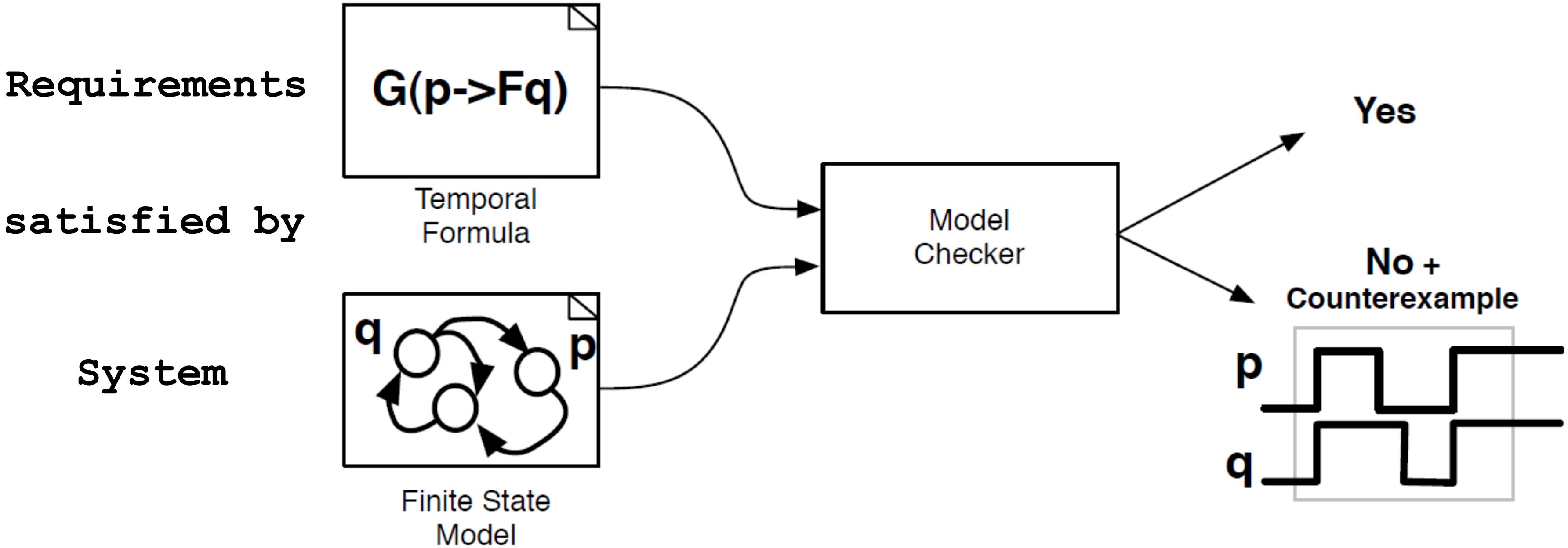
- How do we support operation?
  - Planning, Monitoring, FDIR, replanning
  - they all require reasoning about the behaviour of a dynamic system

Life Cycle of Complex Systems



The workhorse: Model Checking

- Does system satisfy requirements?
- System as finite state model
- Requirements as temporal properties



Research Topics

- Satisfiability Modulo Theory
  - Boolean SAT + Constraint solving
- Abstraction to deal with infinite-state systems
  - Timed and hybrid systems
  - Software model checking
  - IC3 + implicit abstraction
- Contract-based design
  - correct-by-construction hierarchical decomposition
- Link to design languages
  - Simulink/SF, C, Altarica, AADL, SysML, BIP, Verilog, …
- Formal safety analysis
  - From nominal to non-nominal behaviours
  - Automated Fault Tree construction
- Analysis of redundancy architectures
  - Automated reliability for TMR-based systems
- Diagnosability and FDIR specification and verification

Projects w/ European Space Agency

- Since 2007, a number of competitive projects awarded to FBK in cooperation with various industrial partners
- Topics:
  - Model-based safety analysis
  - Contract-based analysis
  - On-board model checking

- An AADL-based modeling language
- The OCRA, nuXmv, xSAP tool chain at the core
- Fault Tree generation, FDIR specification and V&V

Activities with Boeing RnT

- 2014: five-year collaboration agreement
  - Substantial amount of funding
  - Level of commitment
- Activities
  - Formal analysis of complex subsystems
  - Trasfer of verification tools
  - Training
  - Process improvement
- Examples of analyzed subsystems
  - Primary flight computer
    - Fly by wire – signals from pilot and sensors to actuations
    - Triple-triple redundancy – nine computers in parallel, mutually checking each other
  - Wheel brake system
    - Ground braking control

Case from AIR 6110 Wheel Brake System

- Aerospace Information Report
  - Informal description of development process
- Two-engine aircraft
  - 300-350 passengers
  - Up to 5hrs flights
- Focus on WBS
  - Two landing gear
    - 4-wheel per LG
    - Independent control

AIR 6110 WBS: main features

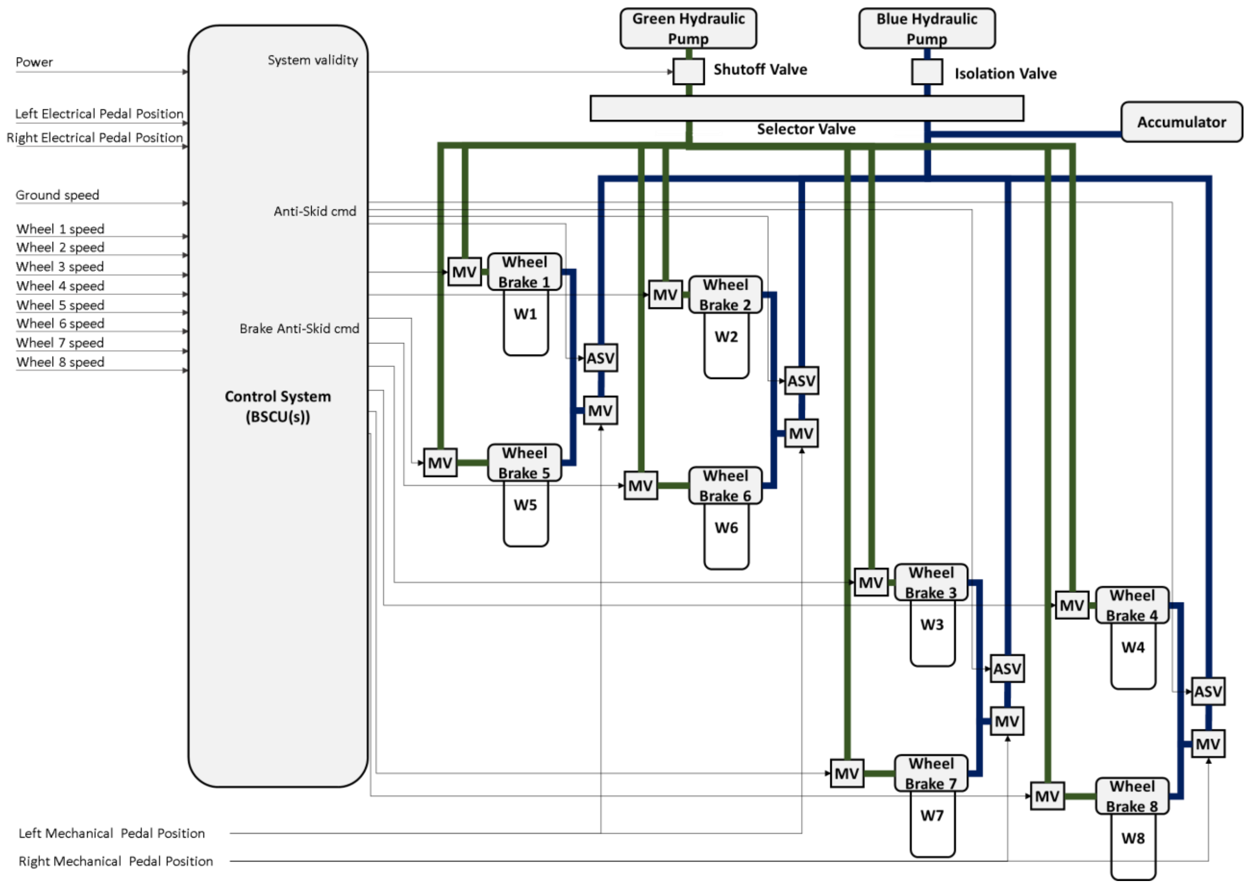
- Hydraulic braking
- Mixed computer-based/mechanical control
- Antiskid
- Redundancy in hydraulic plant and in computer-based control system

		Wheel Brake System		
		Normal Mode *(Primary pressure source)*	**Alternate Mode** *(Secondary pressure source)*	**Emergency Mode** *(Finite-reserve accumulator)*
Control system	**Valid**	• $\text{Brake}_{\text{Elec}}$ • Individual AntiSkid	• $\text{Brake}_{\text{Mech}}$ • Paired-AntiSkid	• $\text{Brake}_{\text{Mech}}$ • Paired-AntiSkid
	Invalid	N/A	$\text{Brake}_{\text{Mech}}$	$\text{Brake}_{\text{Mech}}$

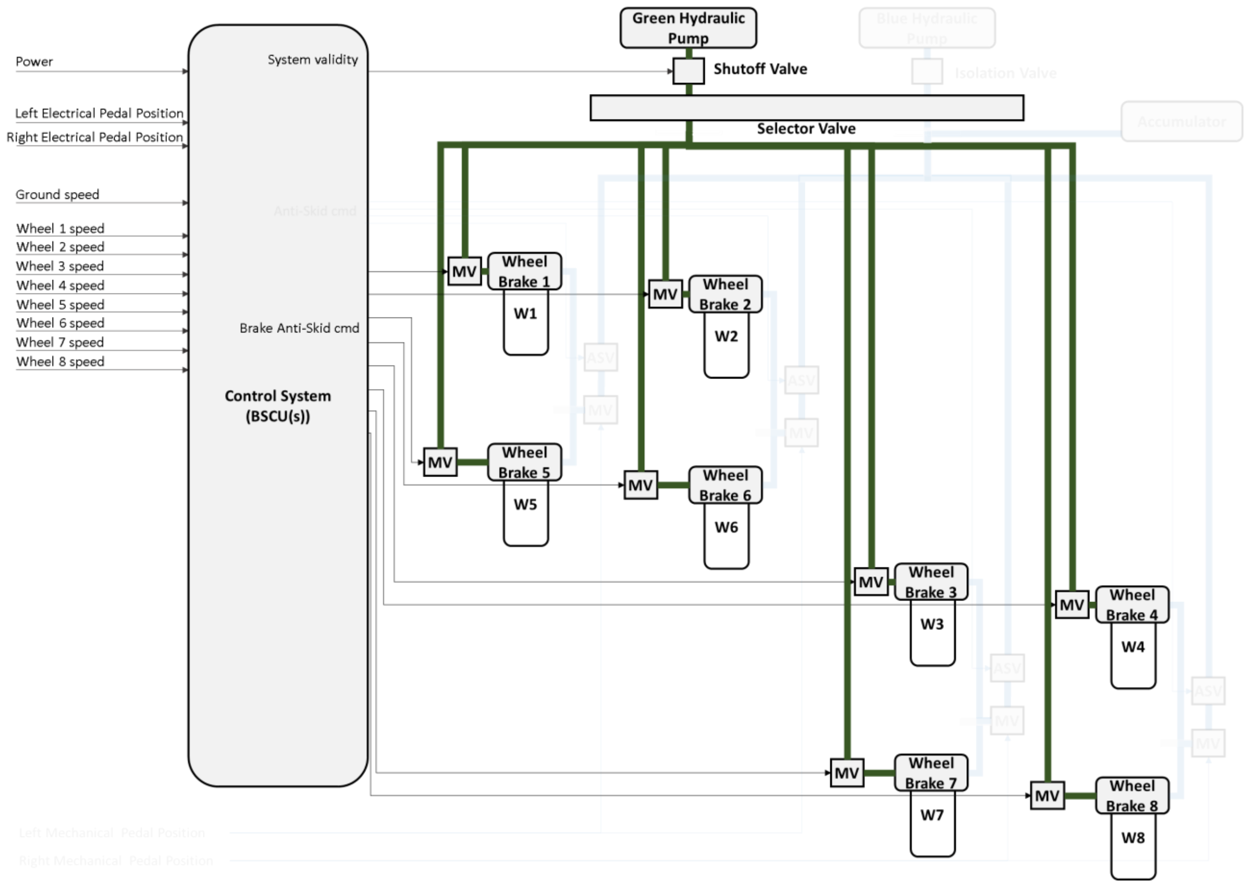
AIR 6110 WBS: examples of requirements

- **S18-WBS-R-0321**: Loss of all wheel braking (unannunciated or annunciated) during landing or RTO shall be extremely remote
- **S18-WBS-R-0322**: Asymmetrical loss of wheel braking coupled with loss of rudder or nose wheel steering during landing or RTO shall be extremely remote
- **S18-WBS-0323**: Inadvertent wheel braking with all wheels locked during takeoff roll before V1 shall be extremely remote
- **S18-WBS-R-0324**: Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be extremely improbable
- **S18-WBS-R-0325**: Undetected inadvertent wheel braking on one wheel w/o locking during takeoff shall be extremely improbable

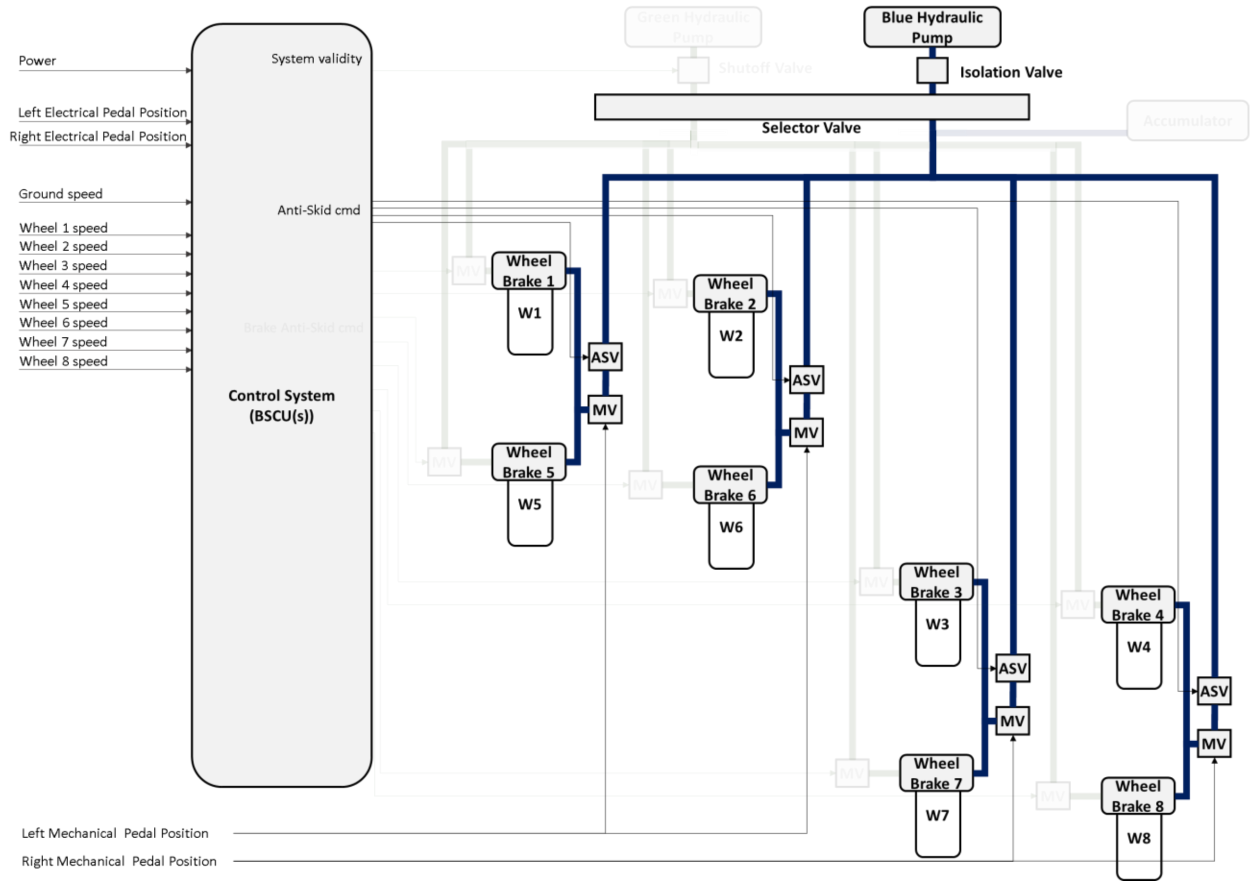
AIR 6110 WBS: general schema



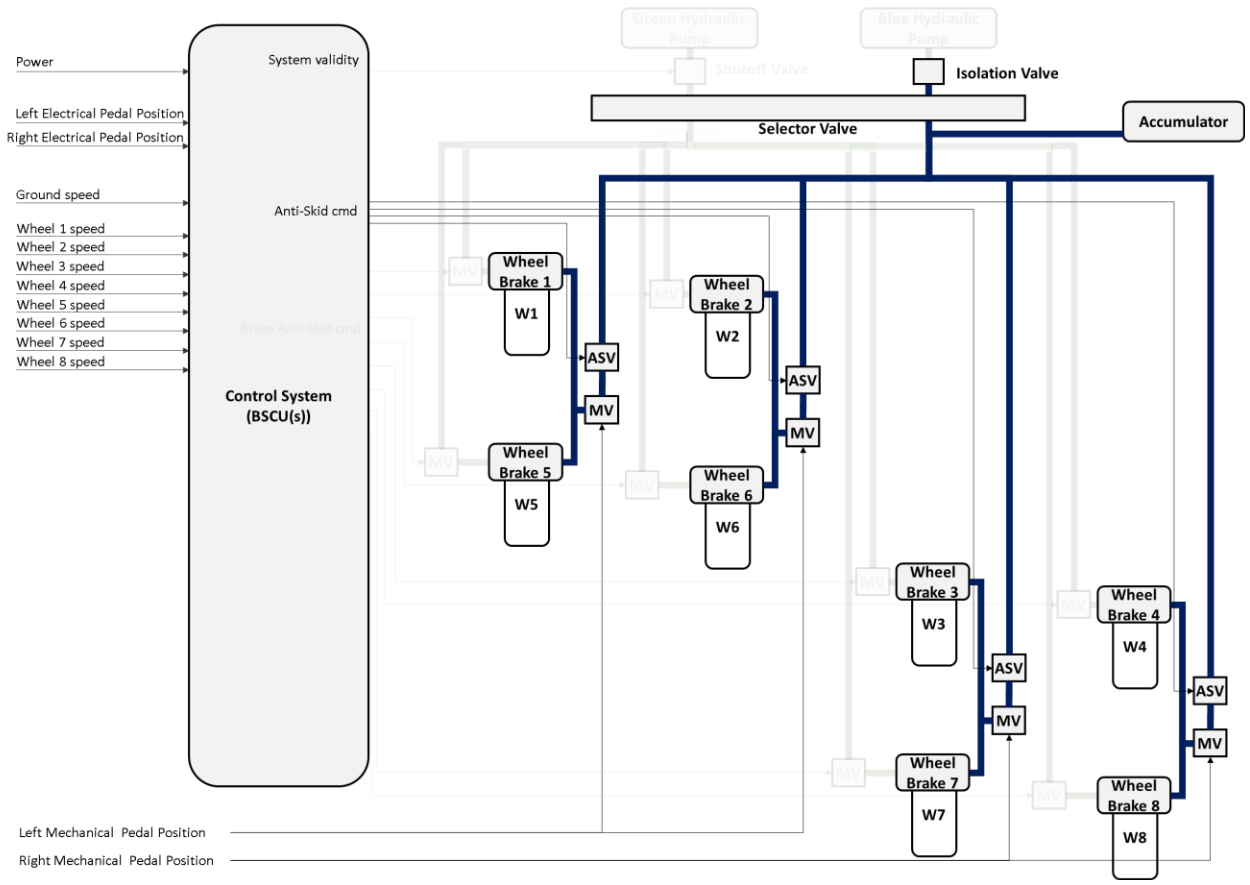
AIR 6110 WBS: main



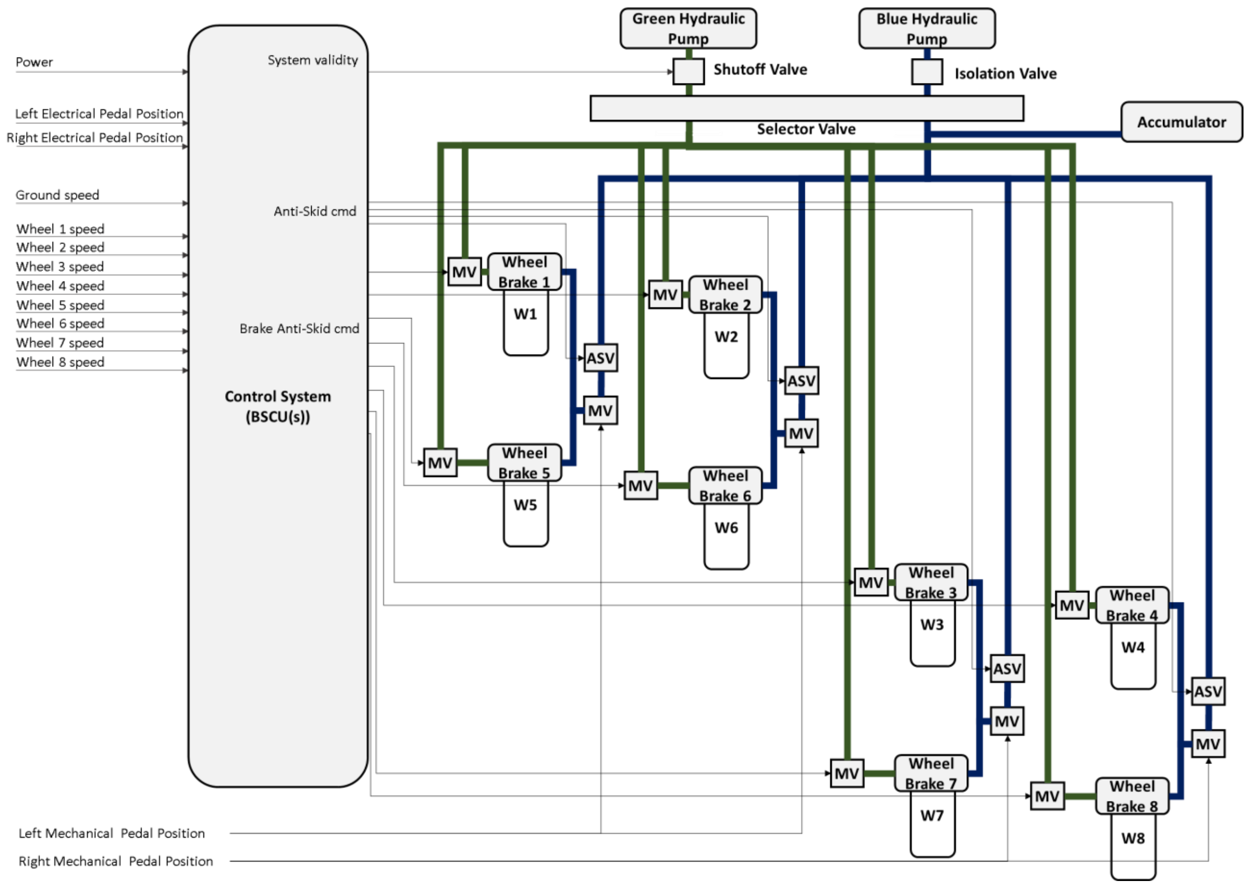
AIR 6110 WBS: backup



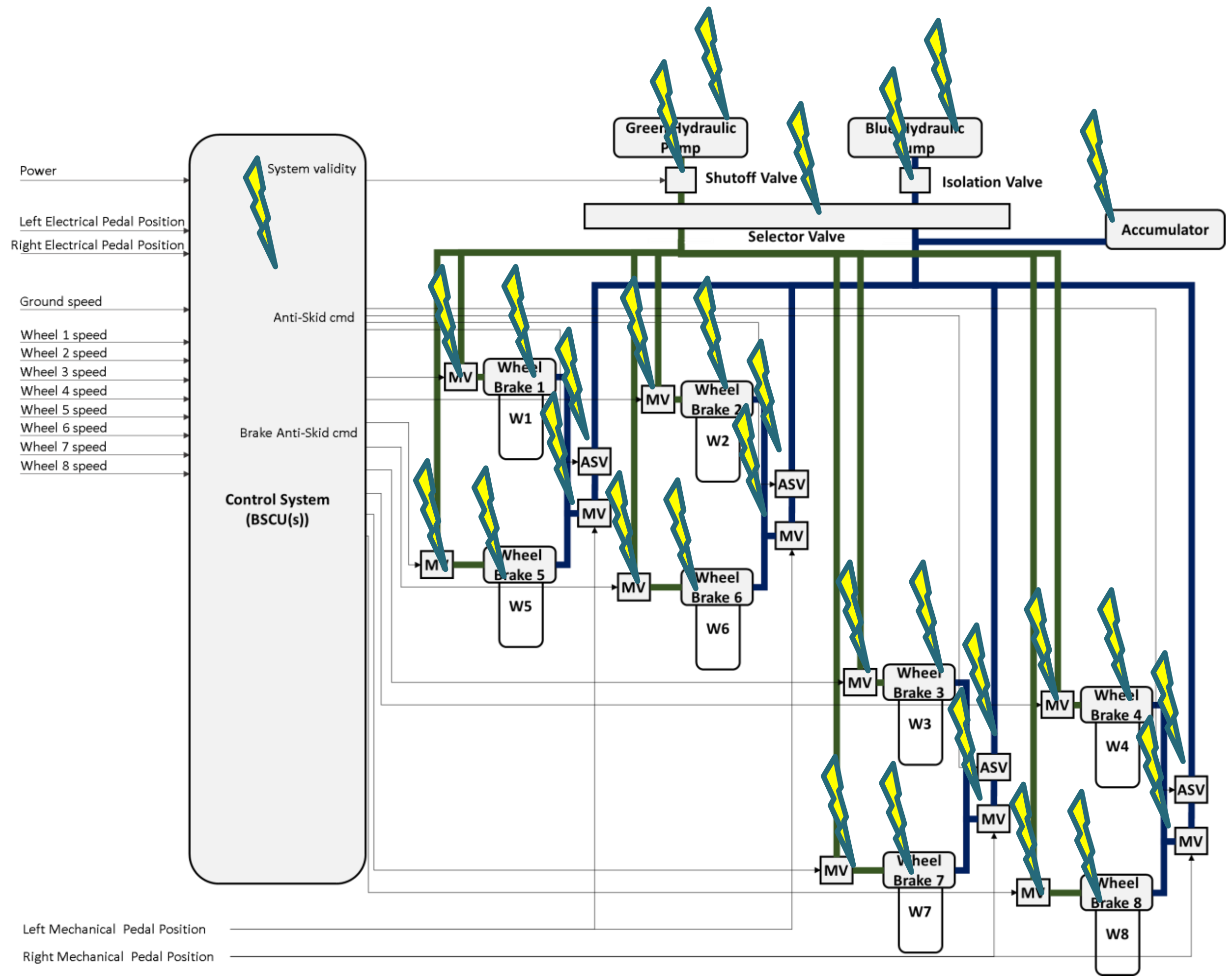
AIR 6110 WBS: emergency



AIR 6110 WBS: nominal

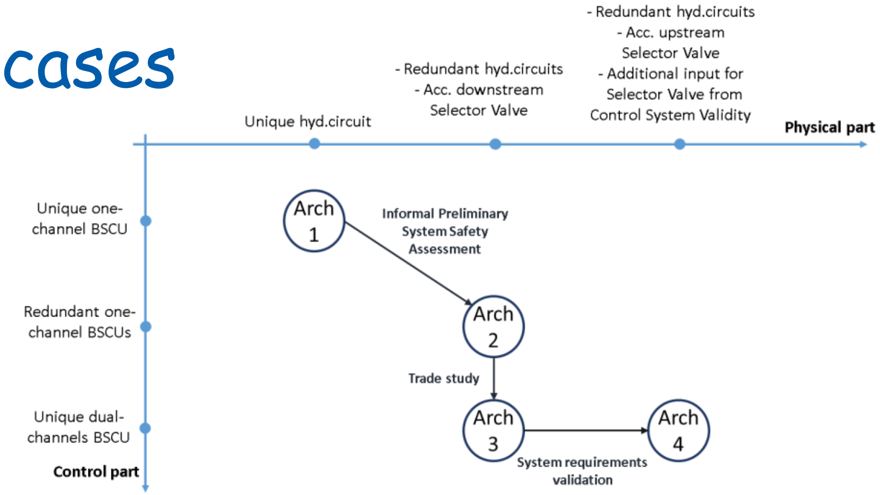


AIR 6110 WBS: extended



AIR6110 WBS: architecture variants

- Various architectures automatically analyzed
- All minimal cut sets (fault combinations) leading loss of function
- Generated Fault tree
- Generated FMEA tables
- Found some uncovered cases



FONDAZIONE BRUNO KESSLER

Thanks for your attention

Next year in Trento in September...

SEFM

IMBSA

Safecomp

PhD at FBK

The FBK-ICT PhD program involves more than 60 PhD Students allocated to the units of the three Research Lines and of the three High Impact Initiatives of the center. The PhD program is carried out in collaboration with prestigious national and international Affiliated universities.

- FBK-ICT has a special partnership with:
  - Department of Information Engineering and Computer Science, University of Trento
- FBK-ICT has a joint PhD school ("accreditamento congiunto") with:
  - University of Bologna ("scuola di dottorato UNIBO-DEI/FBK")
  - University of Genova (with UNIGE-DIBRIS, under approval)
  - University of Padova (with UNIPD-BMCS, under approval)
- FBK-ICT has joint PhD agreements with:
  - Queen Mary University, London, UK
  - University College London, UK
  - Imperial College London, UK
  - Massachusetts Institute of Technology, USA
  - DFKI, Germany
  - University of Haifa, Israel
- FBK-ICT has agreements for co-supervised PhD students with University of Siena, Perugia, Pavia, Brescia.

Ingredients for the formal view

- A formal language to specify contracts
  - Temporal logics
- A framework for correct contract refinement
  - Proof obligations
  - Logical consequence of temporal logic formulae
- A formal language to specify implementation
  - Finite state machines
- Checking implementation
  - Model checking