



# Spi2Java

## From Security Protocol Models To Java Application Generation



Politecnico di Torino

### What is this about?

Spi2Java is a model driven development (MDD) framework to semi-automatically generate Java security protocol implementations from verified Spi Calculus formal specifications of such protocols. The aim of the framework is to provide high correctness confidence on the generated code, thus making a step towards bridging the gap between the verified abstract formal models, and their concrete implementations.

### How To Use It

The methodology implied by the Spi2Java framework is simple, see Fig. 1. The user starts from a formally verified model of a security protocol. Then, supported by automatic tools, she fills some implementation details that are not captured by the formal model. When these data are ready, an automatic tool generates the Java code implementing the protocol logic. Finally the user provides a manually written marshalling layer. And the final application is ready.

### The Type System

Since Spi Calculus is an untyped language, while Java is statically typed, a type system for Spi Calculus has been designed (see Fig. 2), so that well typed Spi Calculus processes can be translated into Java programs.

### The Generated Code

Each Spi Calculus statement is translated into a sequence of Java statements, see Fig. 3. Thanks to formal translation rules and a formal simulation relation, the Java generated code can be proven to correctly refine the Spi Calculus process from which it was generated.

### I'd like to know more...

Great! For more information, or if you have any comment or suggestion, you can contact us by e-mail. Also, you can contact us if you wish to get a copy of the Spi2Java framework. The Spi2Java framework is released under the GPL.

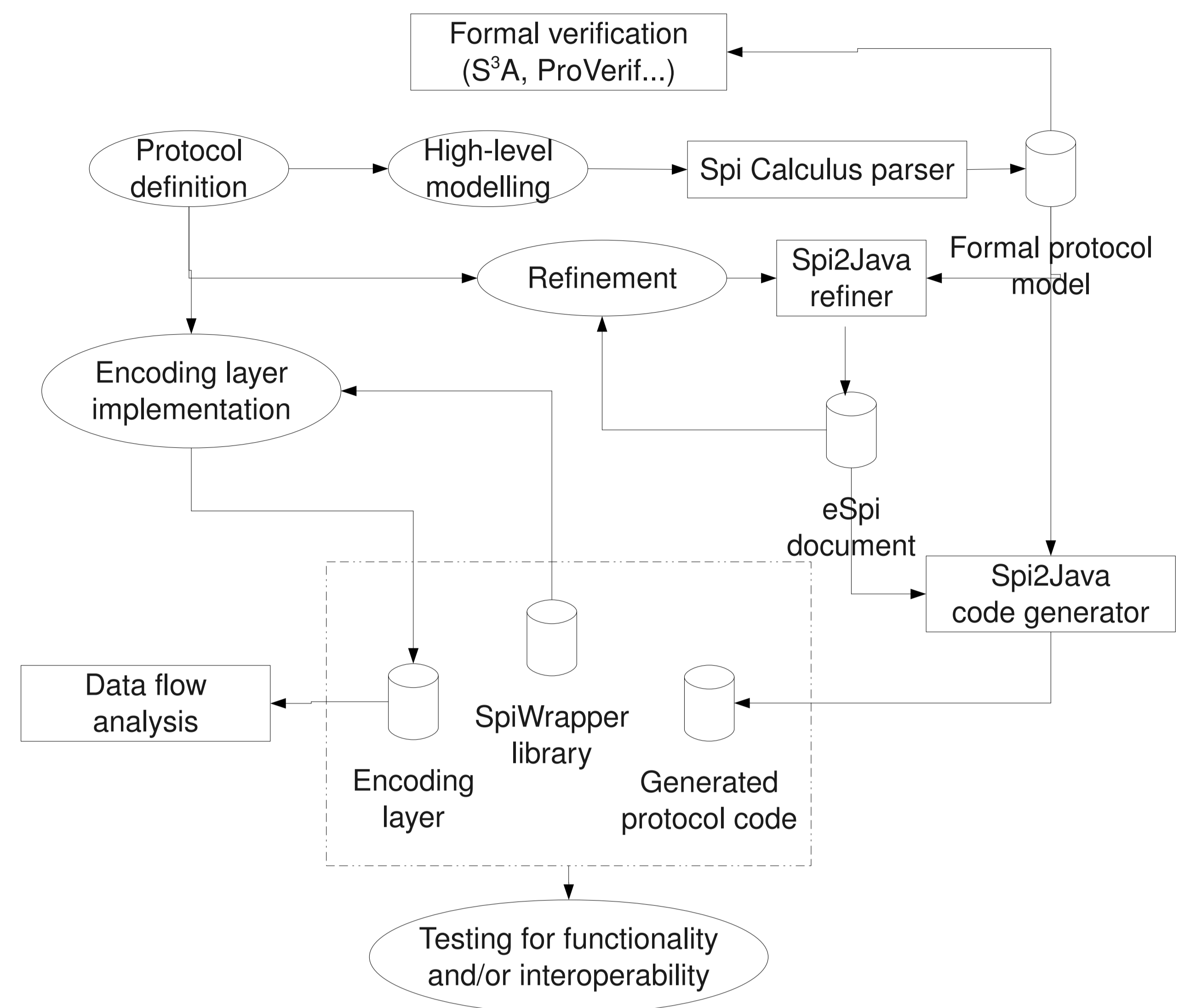


Fig 1: Typical Spi2Java workflow

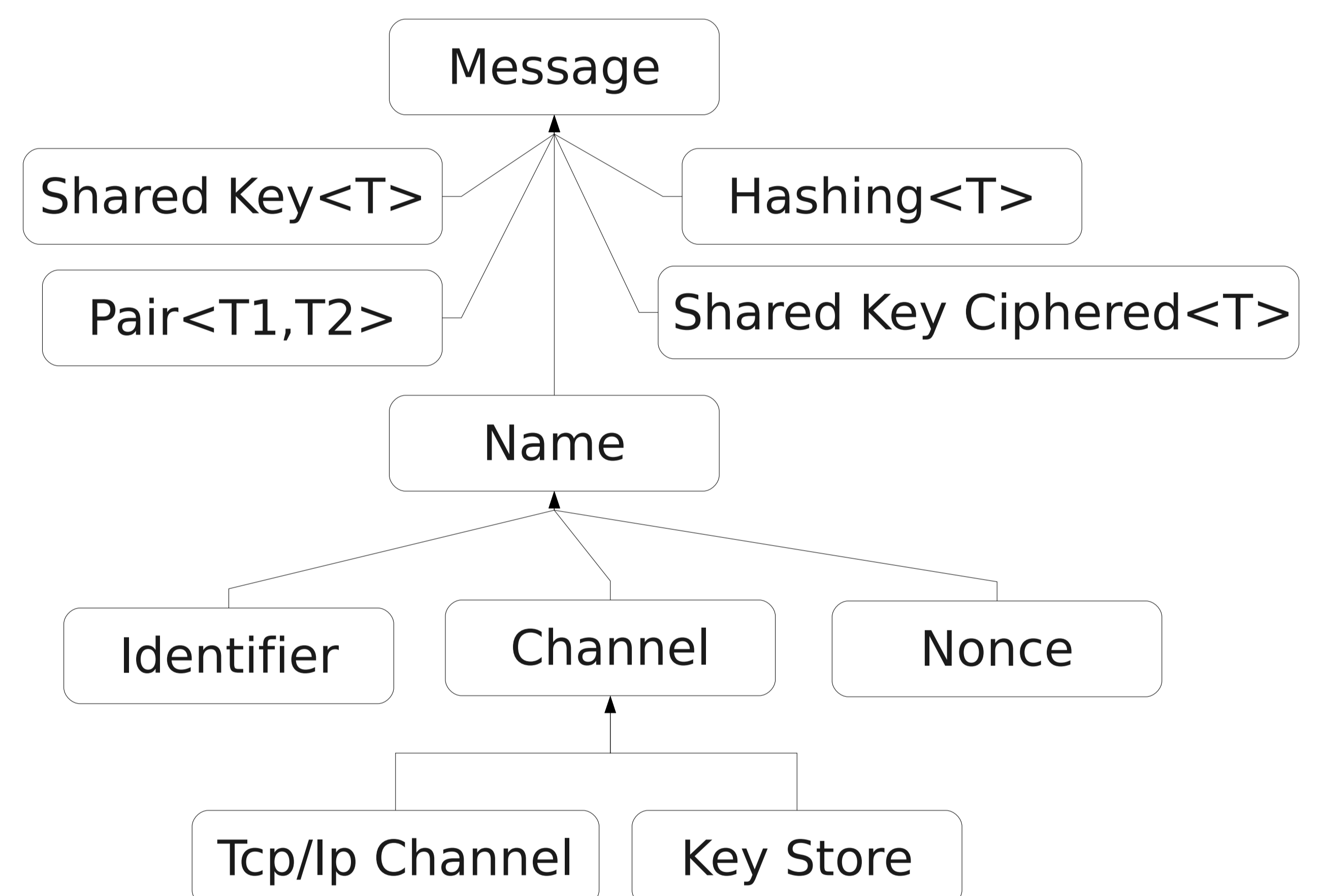


Fig 2: Type hierarchy

```
1 /* let (ID_5,M_5) = _w0_4 in */
2 Identifier ID_5 =
    (Identifier) _w0_4.getLeft();
3 Message M_5 = (Message) _w0_4.getRight();
```

Fig 3: Generated code snippet

### Who's working on it

Spi2Java has been designed and is currently developed at Politecnico di Torino. The research group is composed by

**Prof. Riccardo Sisto** <riccardo.sisto@polito.it>, **Project Leader**  
**Dr. Davide Pozza** <davide.pozza@polito.it>, **Fellowship Researcher**  
**Alfredo Pironti** <alfredo.pironti@polito.it>, **PhD Student**