**PhD in Information Engineering**

**XXX Cycle**

**Guidelines for software development in safety-critical domains: the examples of railway signalling and avionics domains**

**Course description**

Modern transport systems more and more rely on computer-based control and automation equipment. A fault in such equipment is potentially able to cause serious accidents. However, notwithstanding the popularly known frequency of software bugs, such systems are widely used without any significant problem: in the avionic domain it is reported that no serious accident have been directly caused by software errors in the last thirty+ years. These positive results have been achieved thanks to the adoption of precise and rigid guidelines for software development, which however have exhibited the side effects of delaying innovation and increasing development costs. This course will give a survey of the concepts on which such guidelines are based, using the two most significant examples, namely the railway signaling EN50128 and the avionic DO178.