The protection system serves dual purposes. Firstly, to verify that safety constraints identified during hazard analysis have been implemented appropriately. Secondly, as a high-level safety enforcer governing the actions of the robot, preventing the control system from performing unsafe operations.

Separating safety processes from control is a relatively new technique and not one which is generally done in commercial systems.

The design of the safety policies are such that they are not tied to any specific hardware. This gives more flexibility to the construction of the robot and allows identical policies to be used on different types of robotic system.

An example safety policy is shown below. This policy is based on an ISO 10218-1 safety requirement. The requirement states that while operating in reduced speed mode, the maximum speed of the robot must not exceed 250 mm/s.

This example shows that it is possible to explicitly represent safety standard requirements, opening up the possibility that standards could not only be used as guidelines, but also as specifications for actual safety constraint implementation.