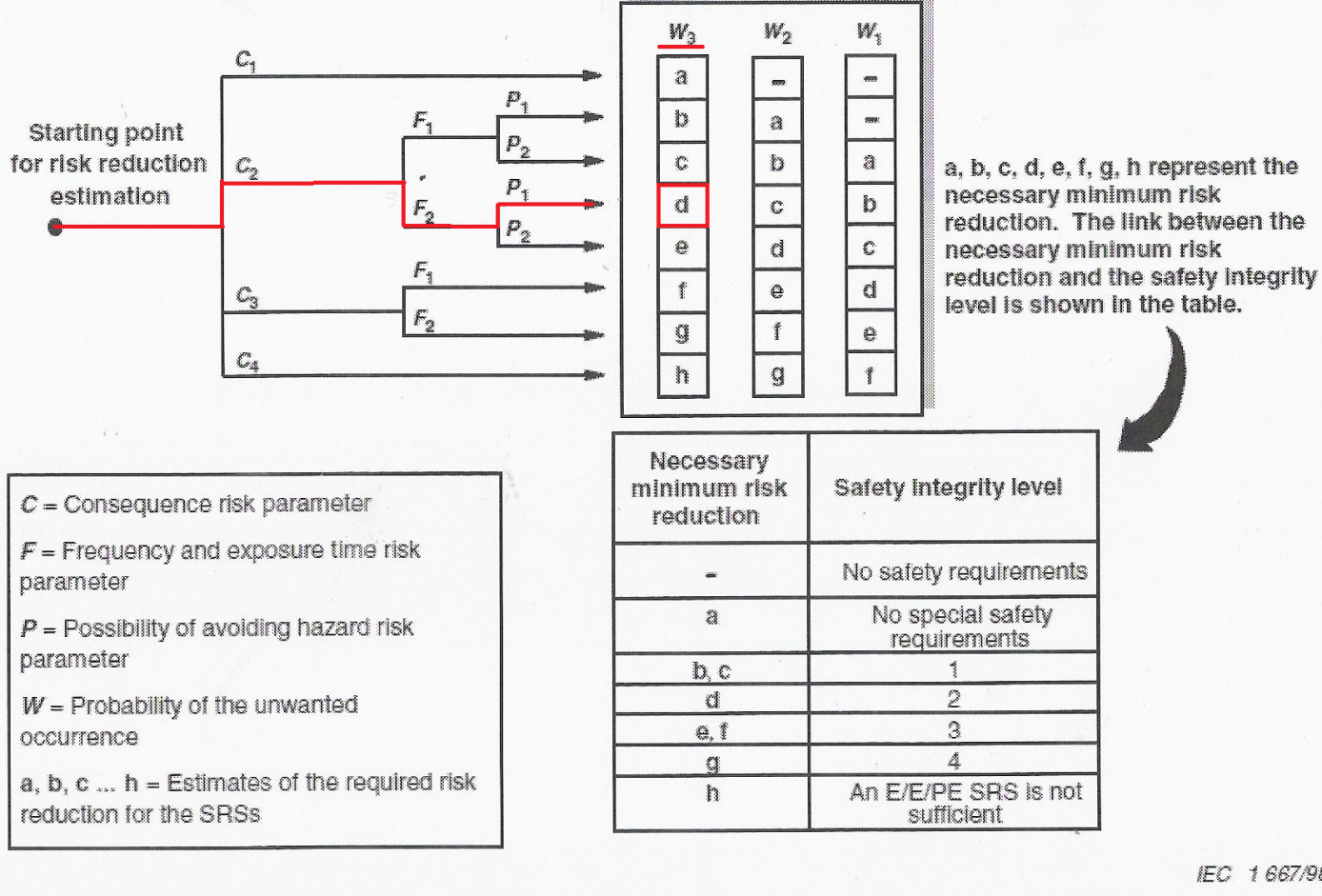
Risk graph

For this robot we used the IEC-51608 standard. By following the schematic in picture? We discovered that the Security Integrity Level of the robot is 2.

* C2: the robot could cause serious permanent injury to one or more persons and death to one.
* F2: frequent to permanent exposure in the hazardous zone.
* P1: The hazard risk is easy to avoid
* W3: A relative high possibility that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely.



Normal operation

In normal operation the robot will not cause any harm to human beings or damage its environment. The ultrasonic sensor will detect objects from a distance, when an object is to low it and will not be detected by the ultrasonic sensor then the bumper will detect the object (see Bumper collision).

Bumper collision

If the front bumper is pressed the robot will go backwards (include warning sound) after 5 seconds, When the back bumper gets pressed within the going back period( 3 seconds) the robot will go in to a fail state, else the robot will turn and go in a random direction( after 5 seconds).

Nearly empty battery

If the battery is getting low (10%) the robot will signal the user by sound signals, if the battery gets critical (5%) the robot will go to fail state.

Failing sensors

The bumpers, ultrasonic and light sensors can be tested while the robot is running; the robot will go in a testing mode and test those sensors. If one of the sensors does not operate like it should the robot will go in to the fail state mode.

Fallen robot

If the gyro sensor detects that the robot is fallen the robot will go to fail state.(This will not be implemented in this prototype)

Fail state mode

In the fail state mode the robot will go in to in to a frozen state and make an alarm sound; while the mode is activated the robot will show an error message. RESET