**Single point fault**A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working.   
This is a fault in an element which is not covered by a safety mechanism and where the fault leads directly to the violation of a safety goal  
  
ISO 26262 specific:

⎯ can lead directly to the violation of a safety goal; and

⎯ is a fault of a hardware element for which not one safety mechanism prevents some   
 of the faults of the hardware element from violating the safety goal.

*Example:*

*Systems can be made robust by adding*[*redundancy*](https://en.wikipedia.org/wiki/Redundancy_(engineering))*in all potential SPOFs. For instance, the owner of a small tree care company may only own one wood chipper. If the chipper breaks, he may be unable to complete his current job and may have to cancel future jobs until he can obtain a replacement.*

*Redundancy can be achieved at various levels. For instance, the owner of the tree care company may have spare parts ready for the repair of the wood chipper, in case it fails. At a higher level, he may have a second wood chipper that he can bring to the job site. Finally, at the highest level, he may have enough equipment available to completely replace everything at the work site in the case of multiple failures.*

*Example ALKA (my interpretation):*

*Unconnected wire that transmits the actuation signal to the steering wheel. With such a failure, a fault is detected.*

**Residual fault**portion of a fault which by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by existing safety mechanisms

⎯ can lead directly to the violation of the safety goal; and

⎯ is a fault of a hardware element for which at least one safety mechanism prevents   
 some of the faults of the hardware element from violating the safety goal.  
🡪 Difference with Single point fault; now safety mechanisms are added, but they will   
 not cover all the faults.

*Example:*

*If a Random Access Memory (RAM) module is only checked by a checkerboard RAM test safety mechanism, certain kinds of bridging faults are not detected. The violation of the safety goals due to these faults are not prevented by the safety mechanism. These faults are examples of residual faults.*

*Example ALKA (my interpretation):*

*Unconnected wire that transmits the actuation signal to the steering wheel. With such a failure, a fault is detected. However, a safety mechanism is able to detect this failure.*

**Detected dual-point fault**One fault of several independent faults that in combination, leads to a multiple point failure (either detected, perceived, or latent)

⎯ *contributes* to the violation of the safety goal;

⎯ can only lead to a safety goal violation in combination with one other independent   
 hardware fault that is related to the dual-point fault; and

⎯ is detected by a safety mechanism which prevents it from being latent.

*Example:*

*Flash memory that is protected by parity: a single bit fault which is detected and triggers a reaction according to the technical safety concept, like switching off the system and informing the driver via a warning lamp.*

*Example ALKA (my interpretation):*

*Camera sensor is over-illuminated and Kalman filter is unable to predict future positions   
 for some time. However, note that a safety mechanism is present to detect these faults   
 in some way. A warning signal is issued to the driver to take over control again.*

**Perceived dual-point fault**One fault of several independent faults that in combination, leads to a multiple point failure (either detected, perceived, or latent)

⎯ contributes to the violation of the safety goal but will only lead to a safety goal   
 violation in combination with one other independent hardware fault that is related to

the dual-point fault; and

⎯ is *perceived by the driver* with or without detection by a safety mechanism within a   
 prescribed time;

*Example:*

*A dual-point fault can be perceived by the driver if the functionality is significantly and unambiguously affected by the consequence of the fault..*

*Example ALKA (my interpretation):*

*Camera sensor is over illuminated and Kalman filter is unable to predict future positions   
 for some time. The driver can observe from the screen in the car that the lane detection   
 system is unable to detect the lane markings ahead. It takes over the control and   
 deactivates the system.*

**Latent dual-point fault**

Multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver

⎯ contributes to the violation of the safety goal but will only lead to the violation of the   
 safety goal in combination with one other independent fault; and

⎯ is neither detected by a safety mechanism nor perceived by the driver. Until the   
 occurrence of the second independent fault, the system is still operable and the driver   
 is not informed about the fault.

*Example:*

*In the case of a flash memory that is protected by EDC: a permanent single bit fault for which the value is corrected by the EDC when read but that is neither corrected in the flash memory nor signaled. In this case, the fault cannot lead to a safety goal violation (since the faulty bit is corrected), but it is neither detected (since the single bit fault is not signaled) nor perceived (since there is no impact on the functionality of the application). If an additional fault occurs in the EDC logic, it can lead to a loss of control of this single bit fault, leading to a potential violation of the safety goal.*

*Example ALKA (my interpretation):*

*Bit flip?*

**Safe fault**

Fault whose occurrence will not significantly increase the probability of violation of a safety goal.

Safe faults can be faults of one of two categories:

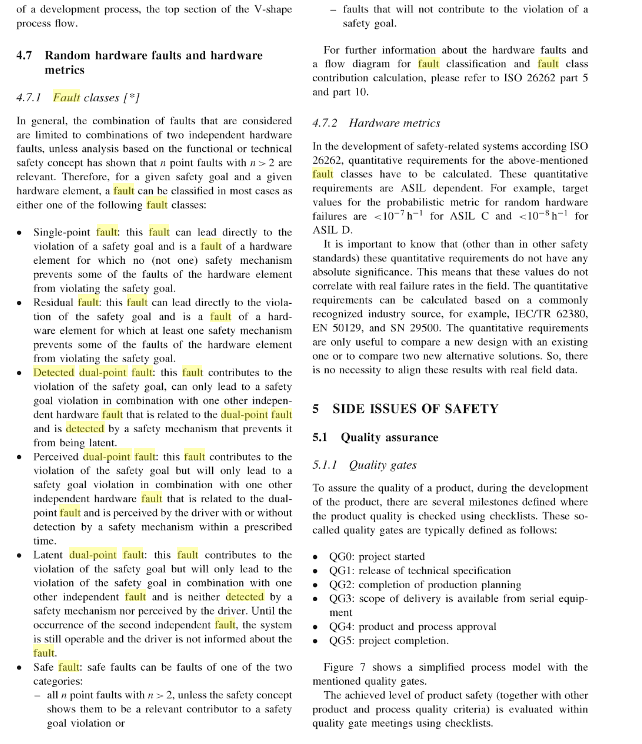
a) All n point faults with n > 2, unless the safety concept shows them to be a relevant contributor to a safety goal violation, or

b) Faults that will not contribute to the violation of a safety goal.

*Example:  
 In case three resistors are connected in series to overcome the problem of a single-point   
 fault in the case of a short circuit, the short circuit of each individual resistor can be   
 considered to be a safe fault as three independent short circuits are needed (n=3)*

*Example ALKA (my interpretation):   
 Suppose the single point fault example explained above. Now assume that there are   
 three wires (two as backup) to reduce the risk of a loose wire. This means that n>2 and   
 the fault of a single loose wire can be seen as a safe fault.   
  
 A second example is an extra-illuminated camera image. By means of using a filtering   
 method, a bad image/picture will not result in a violation of a safety goal.*

Interesting link:  
[**http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/58/workshop/08.Fuhrman.pdf**](http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/58/workshop/08.Fuhrman.pdf)

  
<https://books.google.nl/books?id=ANfdCgAAQBAJ&pg=PA2794-IA26&lpg=PA2794-IA26&dq=detected+dual-point+fault&source=bl&ots=gyygAbVfWl&sig=73-3yWeI7xTDDHuRdYbFe0otD-Y&hl=nl&sa=X&ved=0ahUKEwiG2qaQn9_QAhWL1hoKHW-2ArcQ6AEIIjAB#v=onepage&q=detected%20dual-point%20fault&f=false>