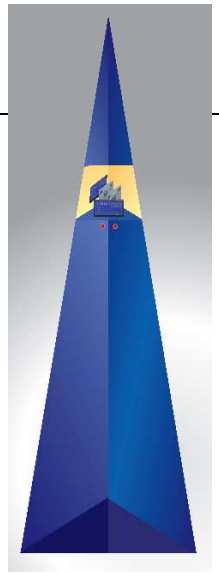
Dependable and Embedded Systems @ Fraunhofer FIRST

Sergio Montenegro

sergio@first.fhg.de

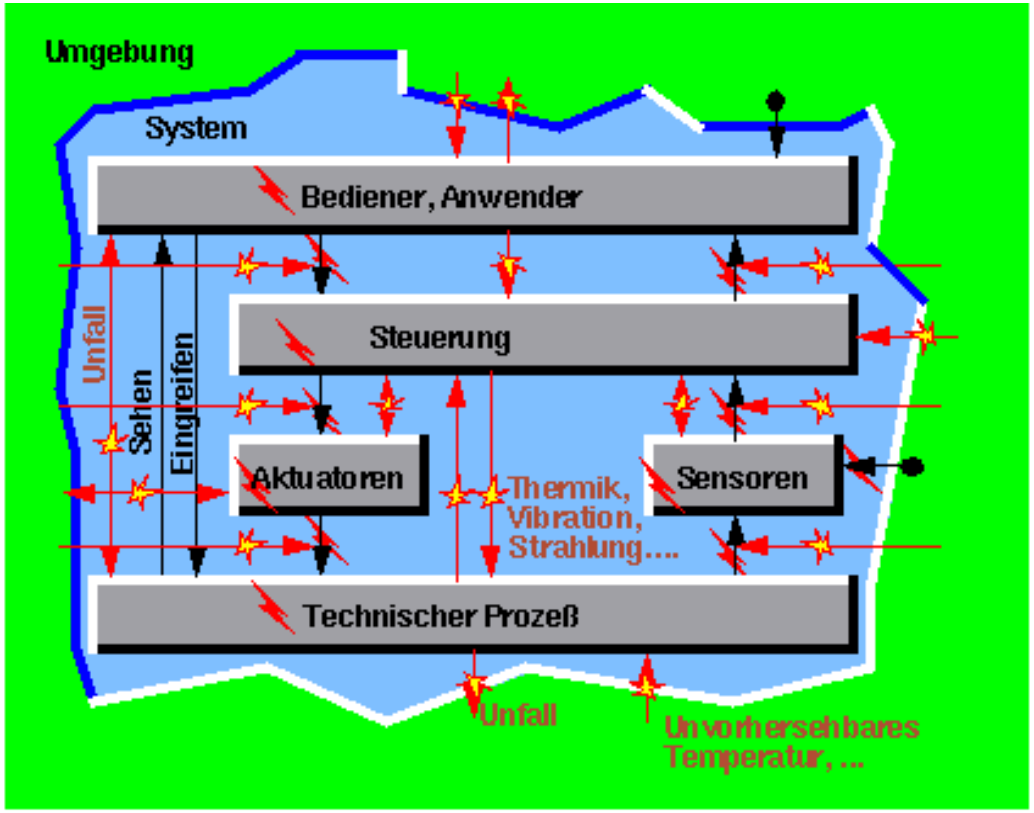
Fehlertoleranz

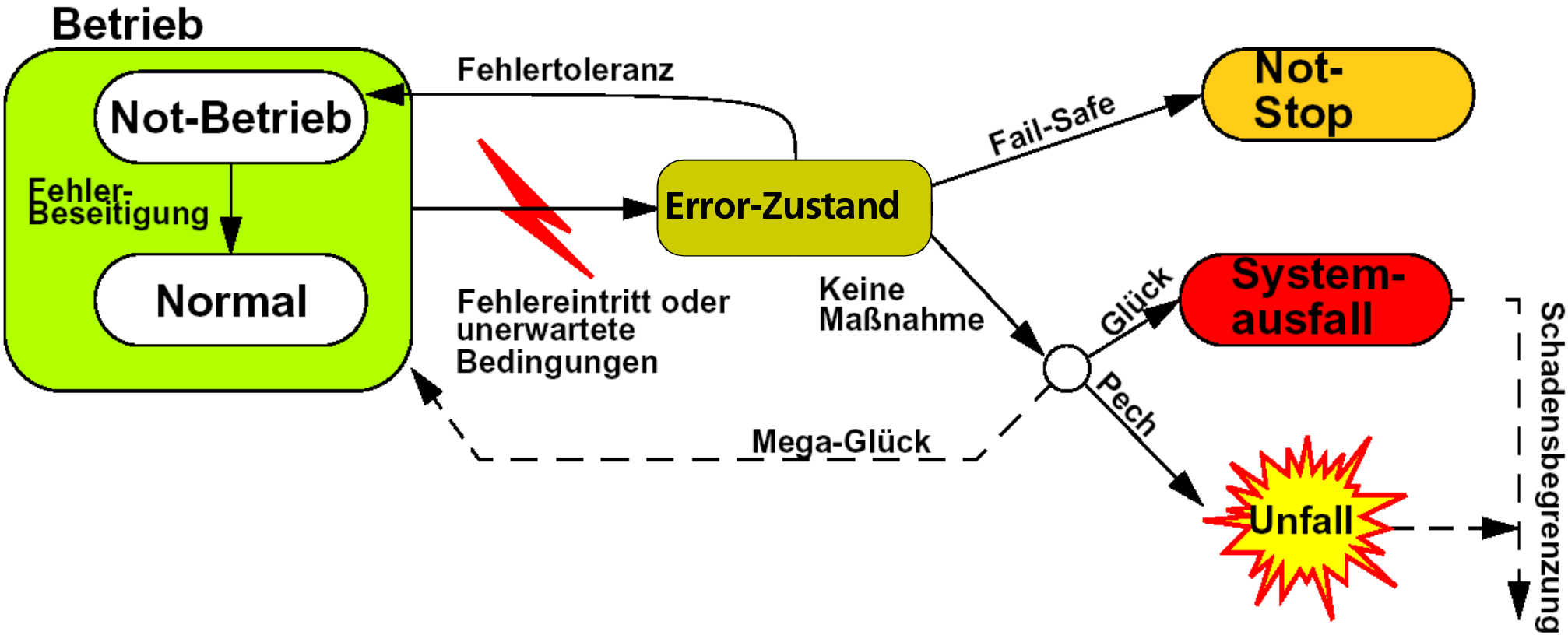


FIRST

Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

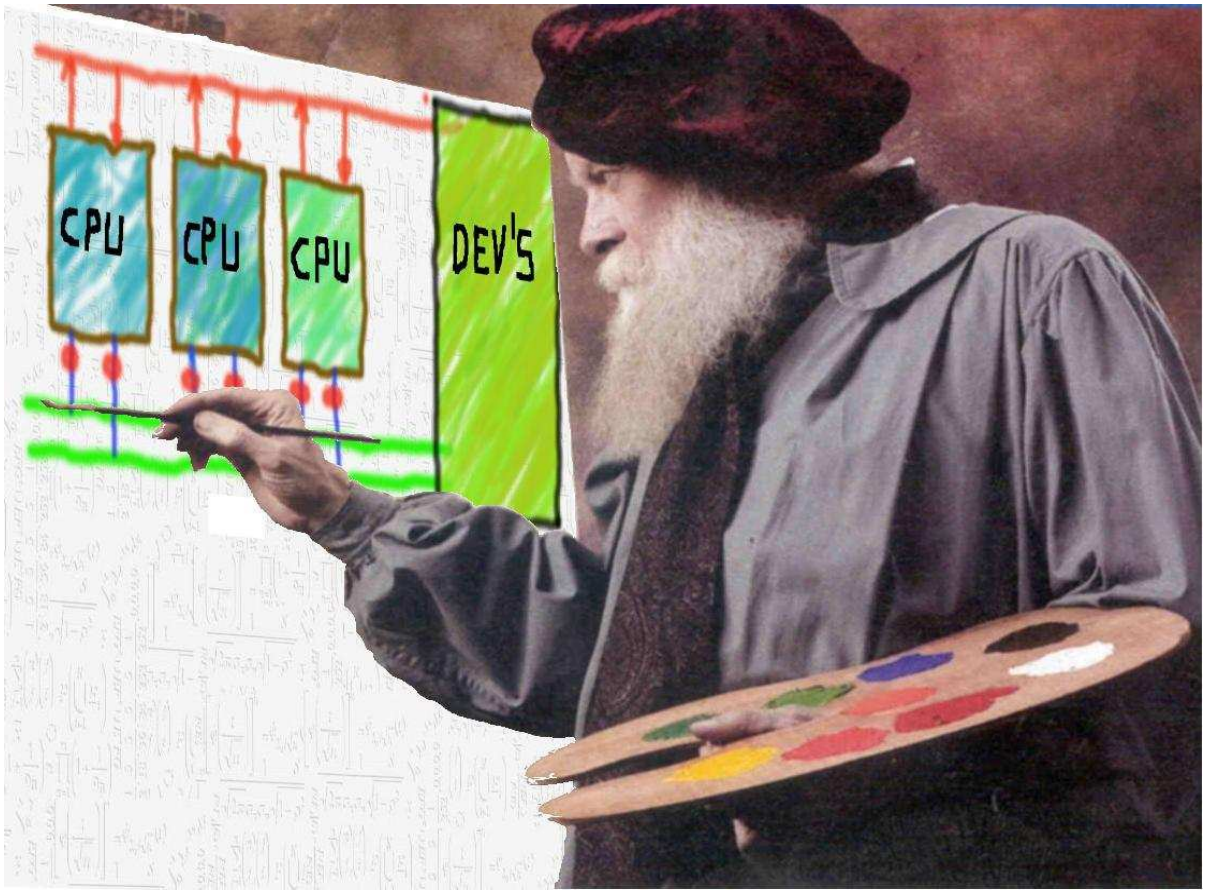
Warum Fehlertoleranz?





Der direkte Weg vom Fehler zum Unfall

The art of fault tolerance



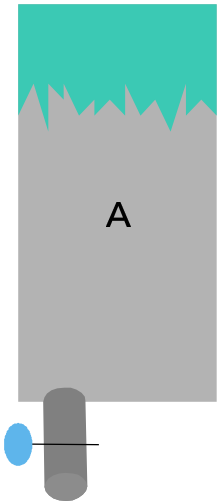
The art of fault tolerance

Gemeinsam ein Beispiel...

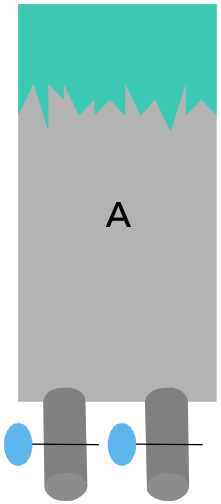
Was soll man duplizieren?

Die Tanks einer Rakete?

Was soll man duplizieren?

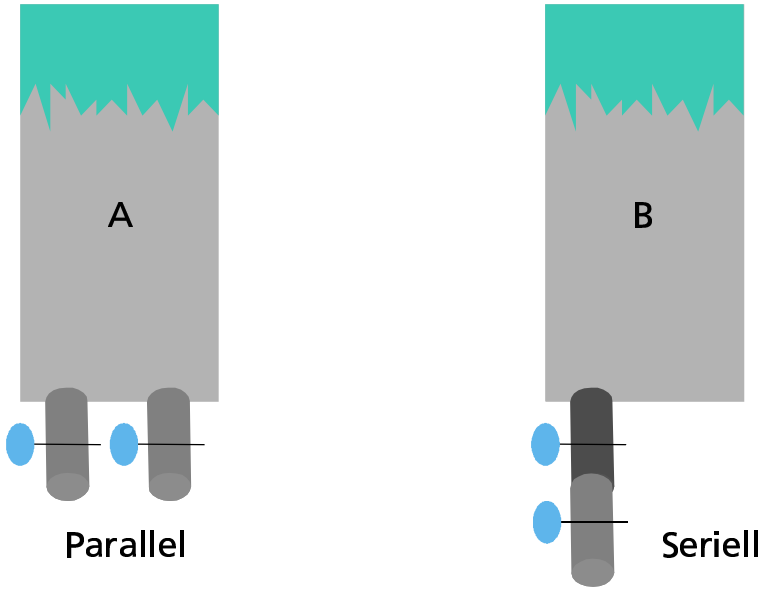


Was soll man duplizieren?

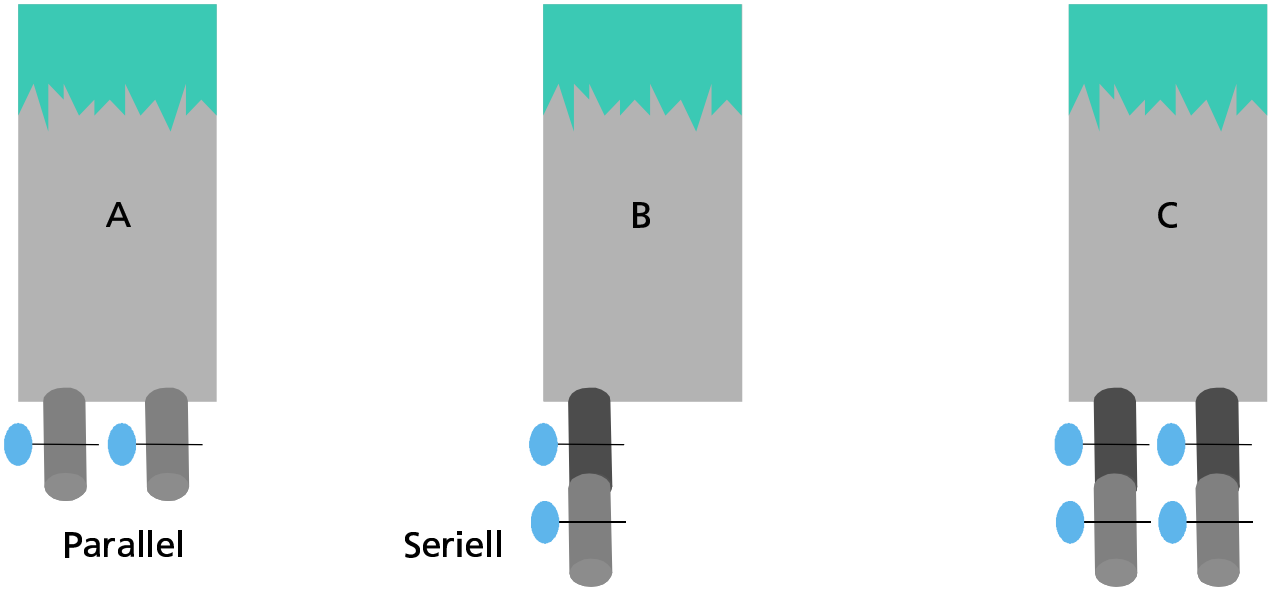


Parallel

Was soll man duplizieren?



Was soll man duplizieren?

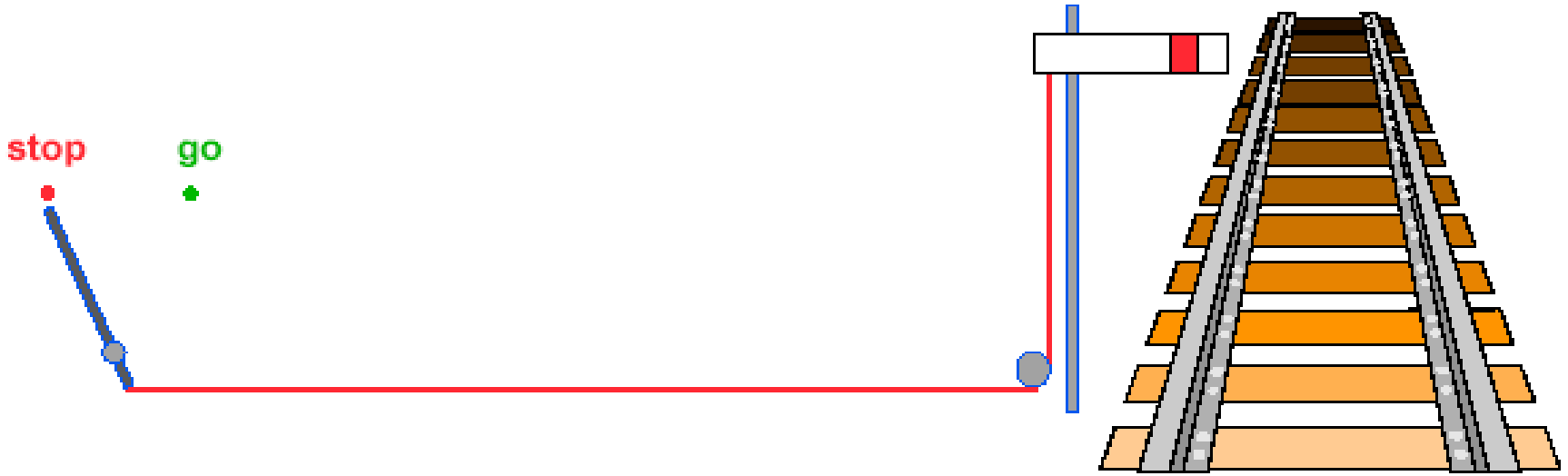


Ventile
Ausfall: Zu

Ventile
Ausfall: Auf

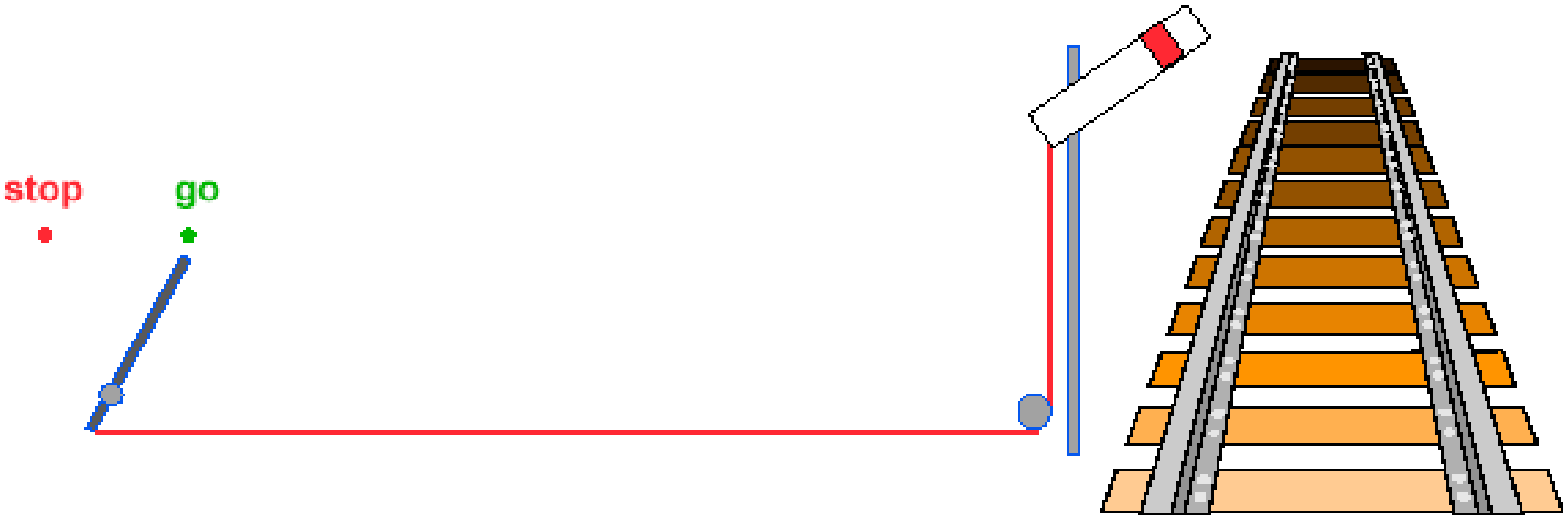
An Early Example of Fail-Safe Design

David Powel



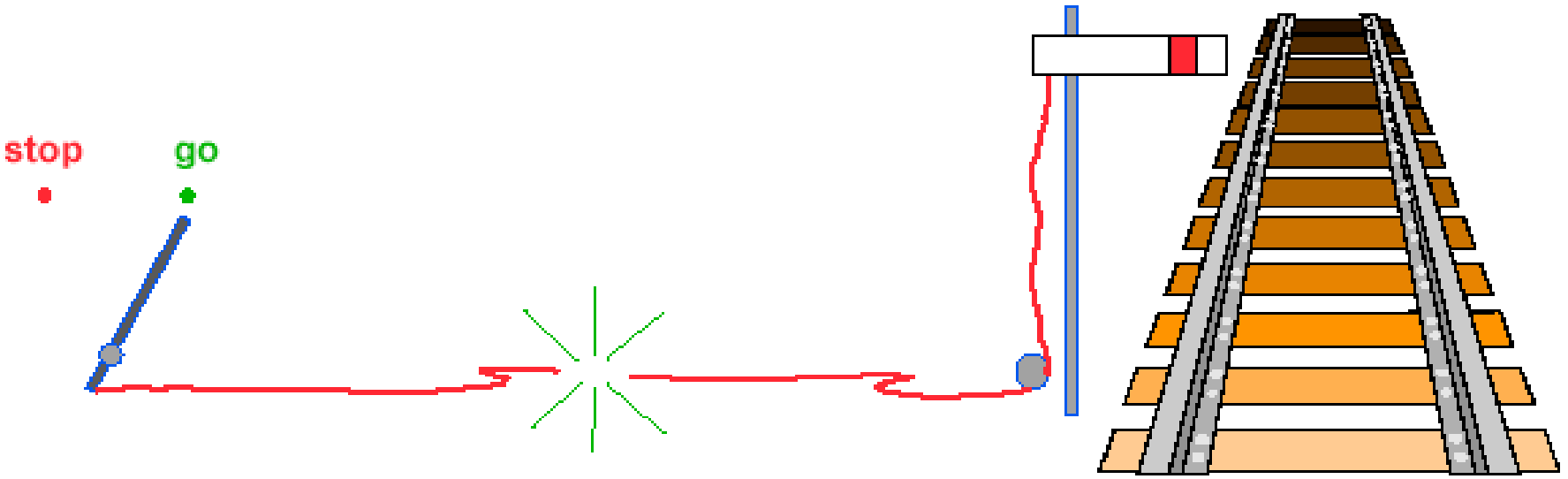
An Early Example of Fail-Safe Design

David Powel



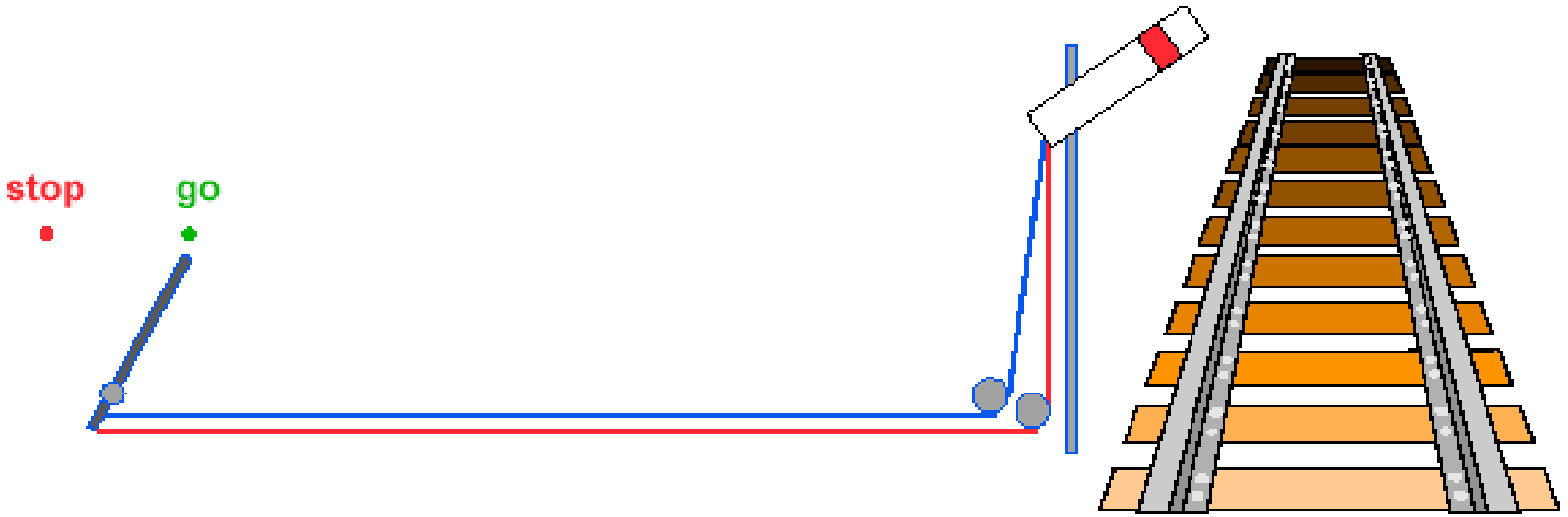
An Early Example of Fail-Safe Design

David Powel



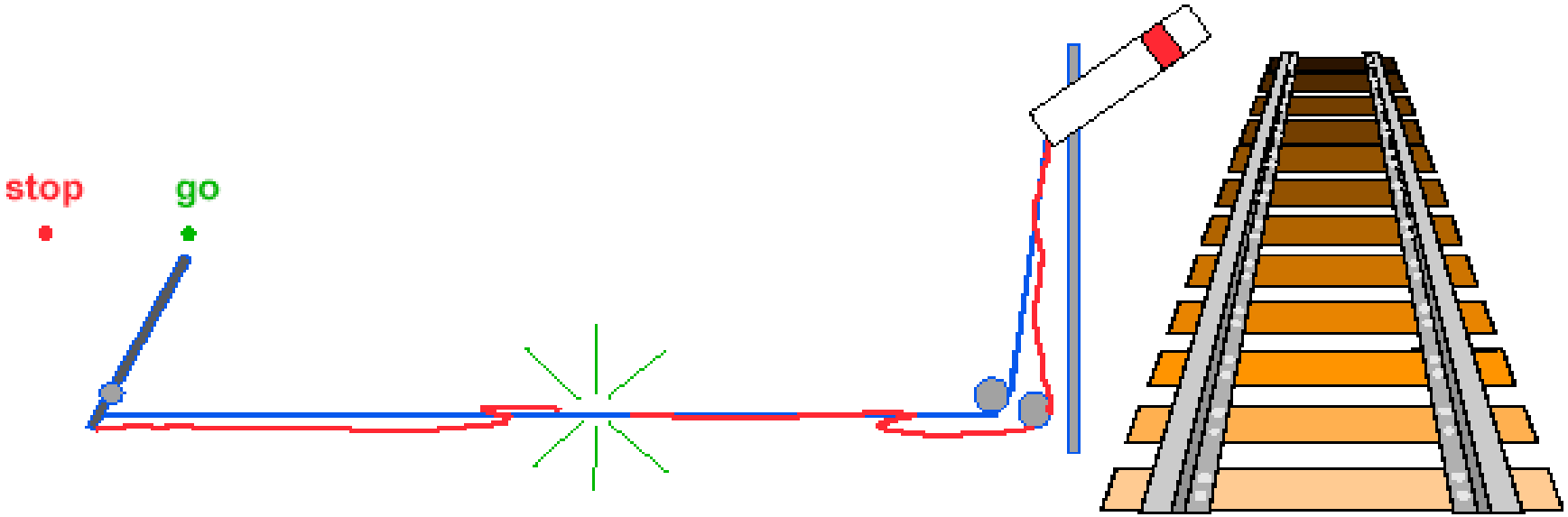
Fault-Tolerant Fail-Safe Design?

David Powel



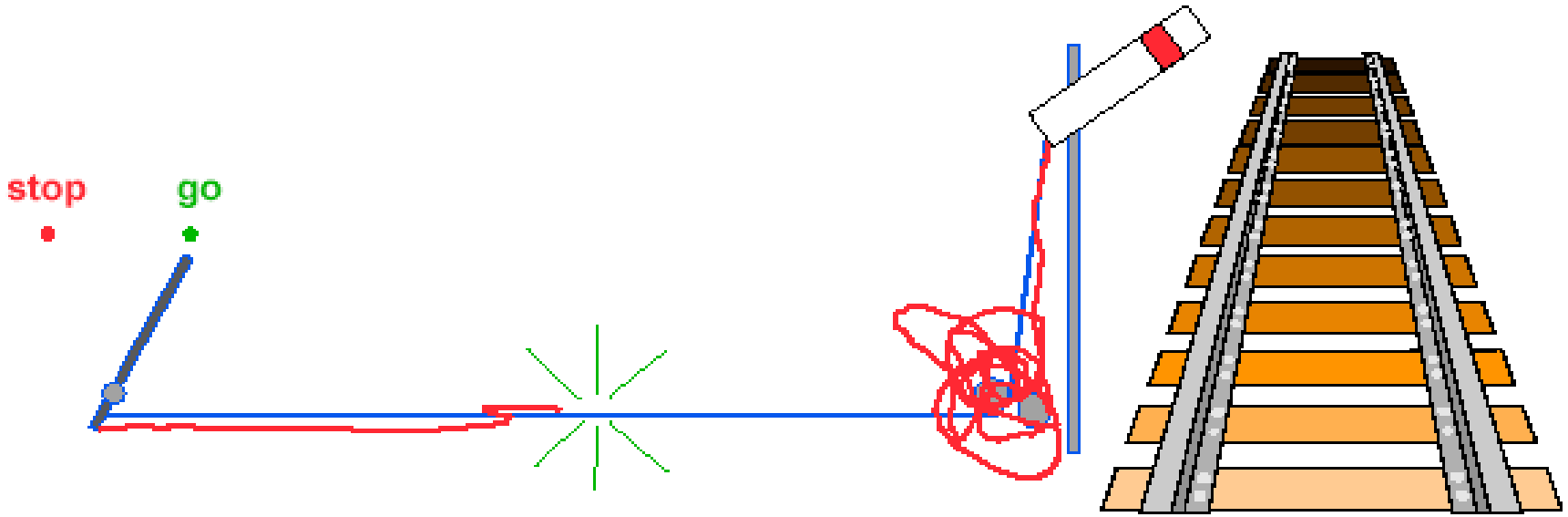
Fault-Tolerant Fail-Safe Design?

David Powel



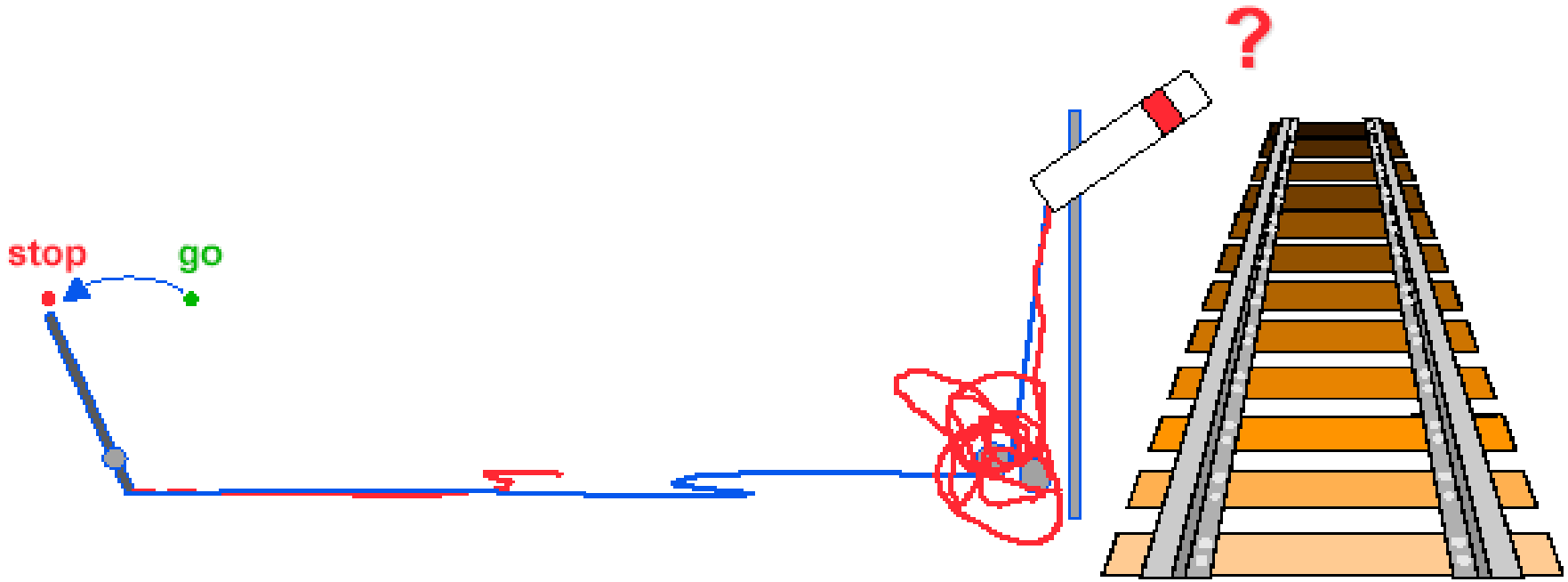
Fault-Tolerant Fail-Safe Design?

David Powel



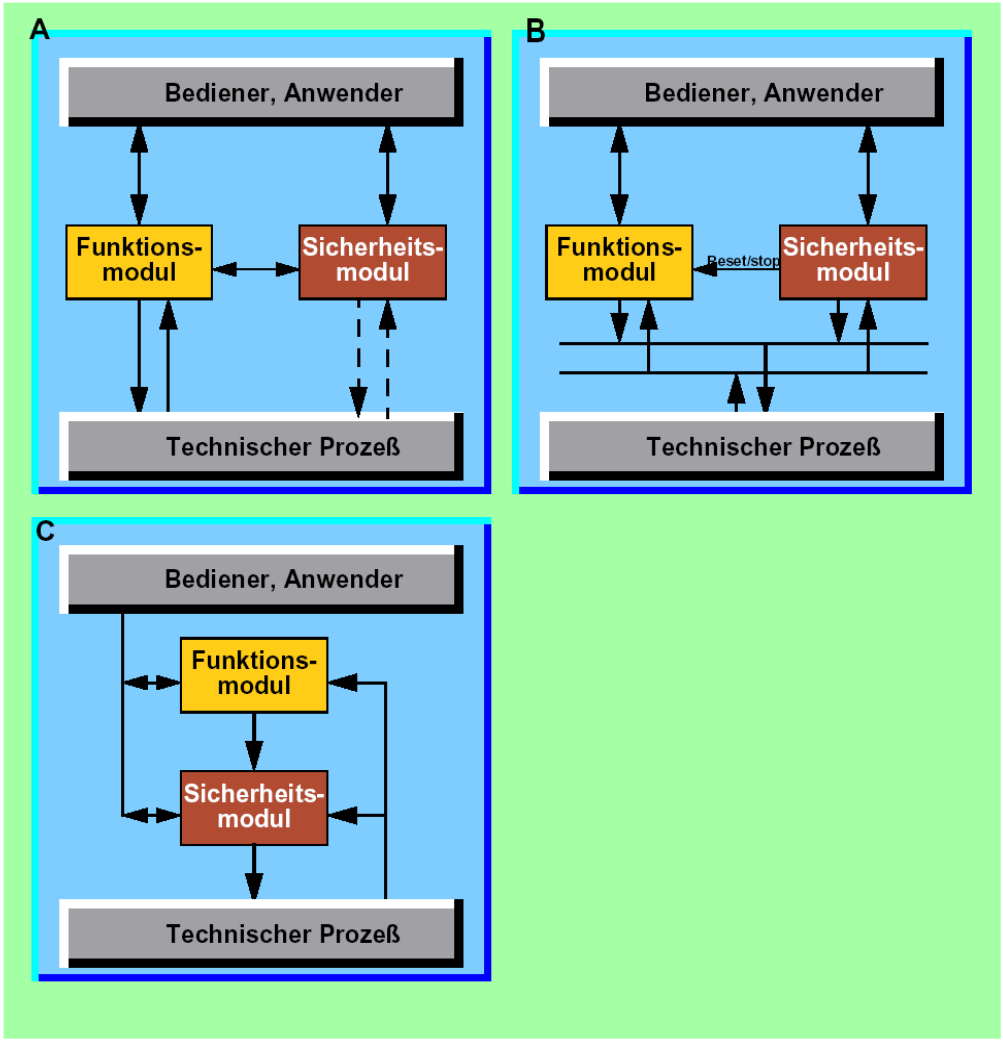
Fault-Tolerant Fail-Safe Design?

David Powel

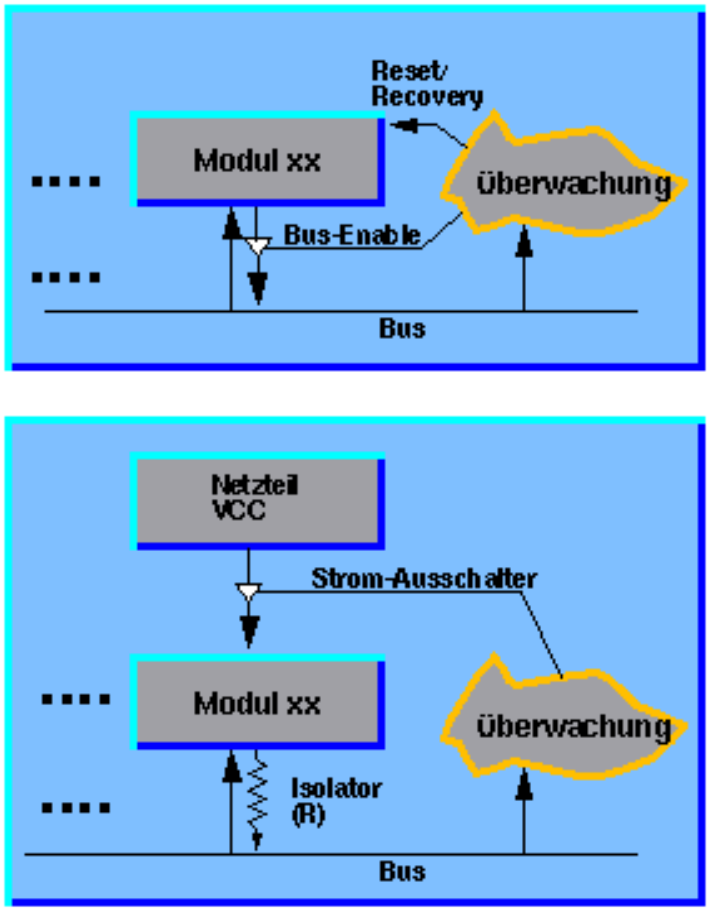


Fraunhofer FIRST Institut
Rechnerarchitektur
und Softwaretechnik

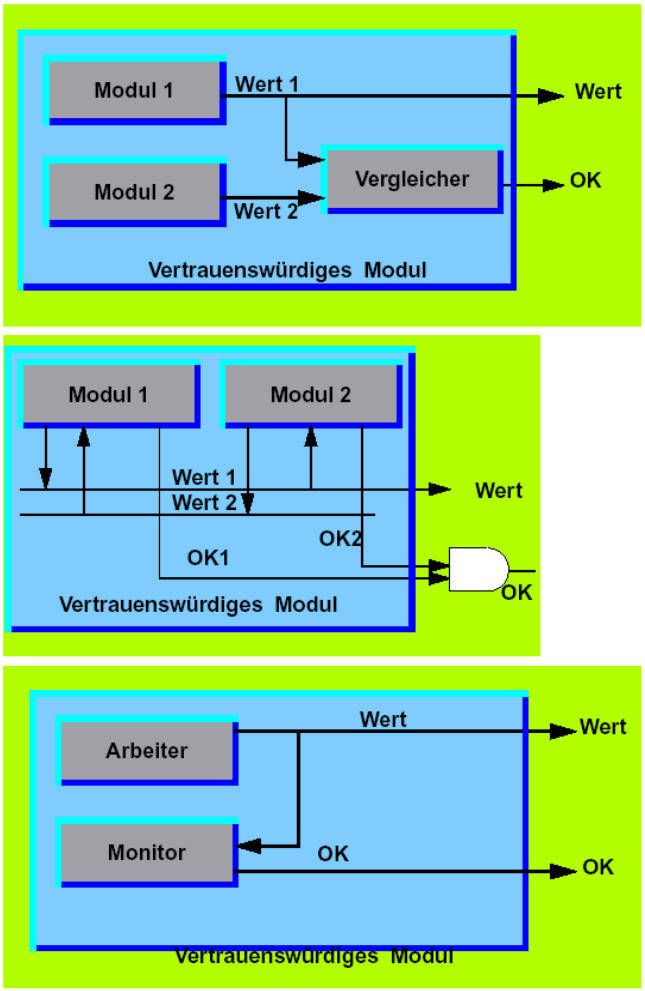
Überwachung / Prüfung



Überwachung -> Fehlertoleranz Modelle

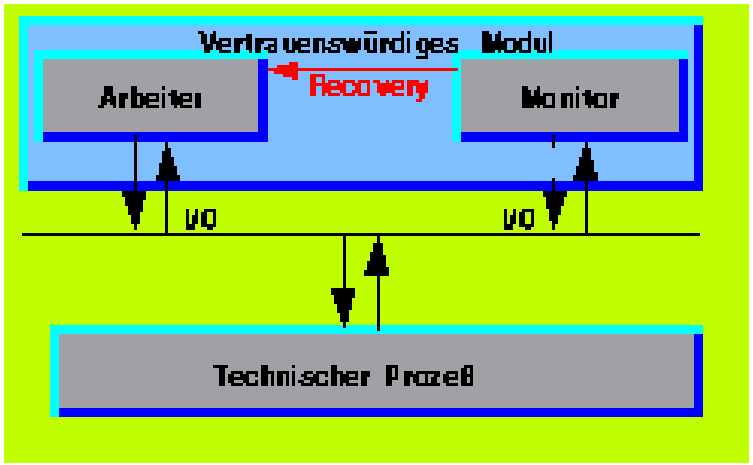


Fehlertoleranz Modelle.. Self checking par

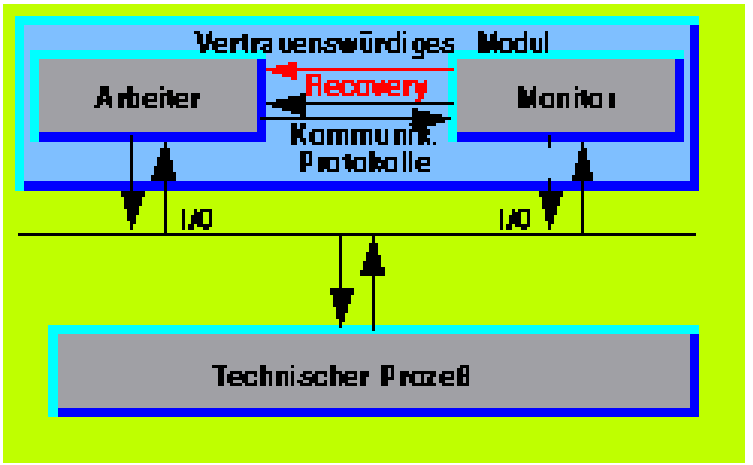


Vertrauenswürdige Module

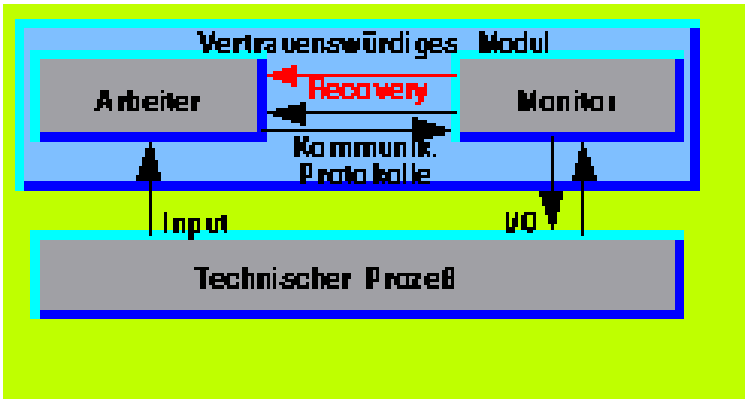
Fehlertolernaz Modelle... Und nach dem Fehler?



A

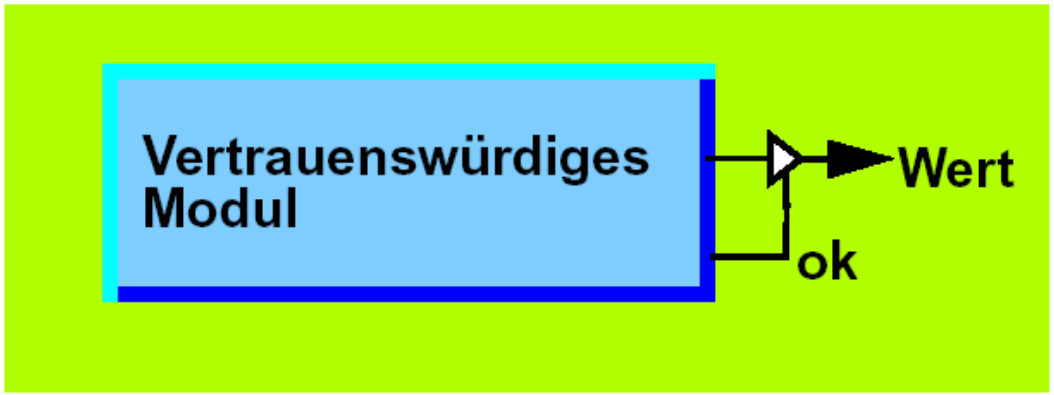


B



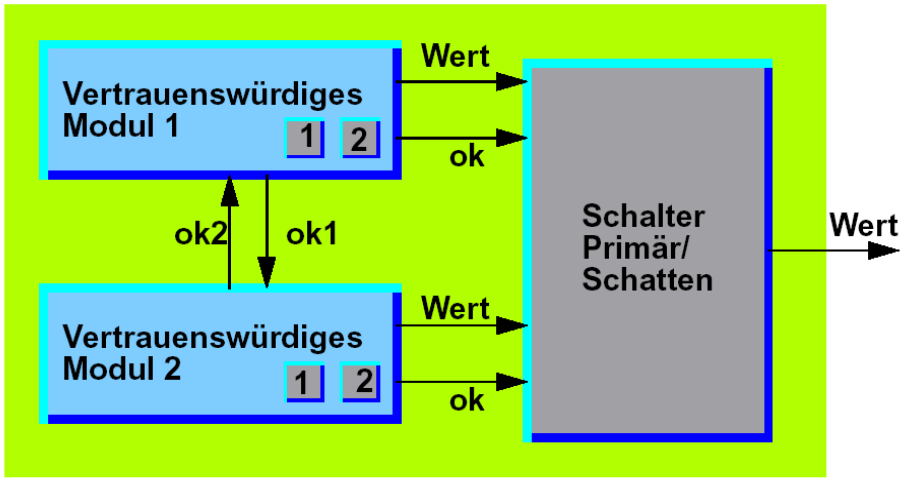
C

Fehlertoleranz Modelle.. Self checking par : Fail silent

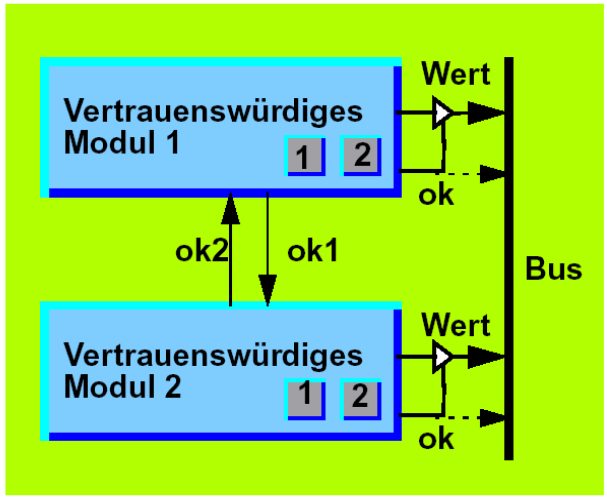


Autoisolation bei Fehlern

Fehlertoleranz Modelle.. Self checking par : Fail silent



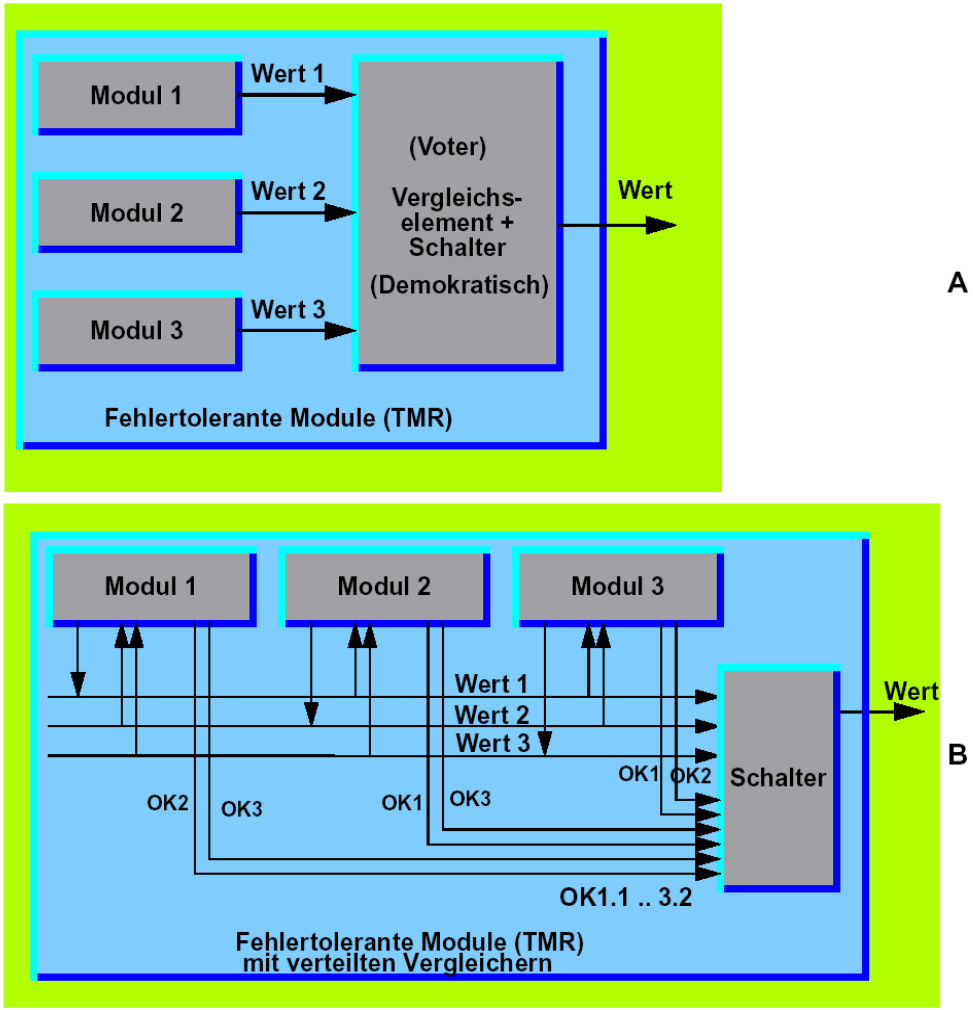
A



B

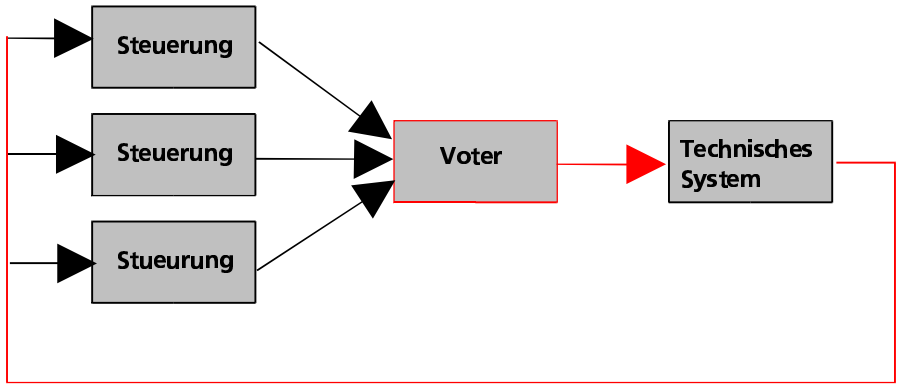
Fehlertolerante Module mit vetrauenswürdigen Modulen

Fehlertoleranz Modelle.. TMR

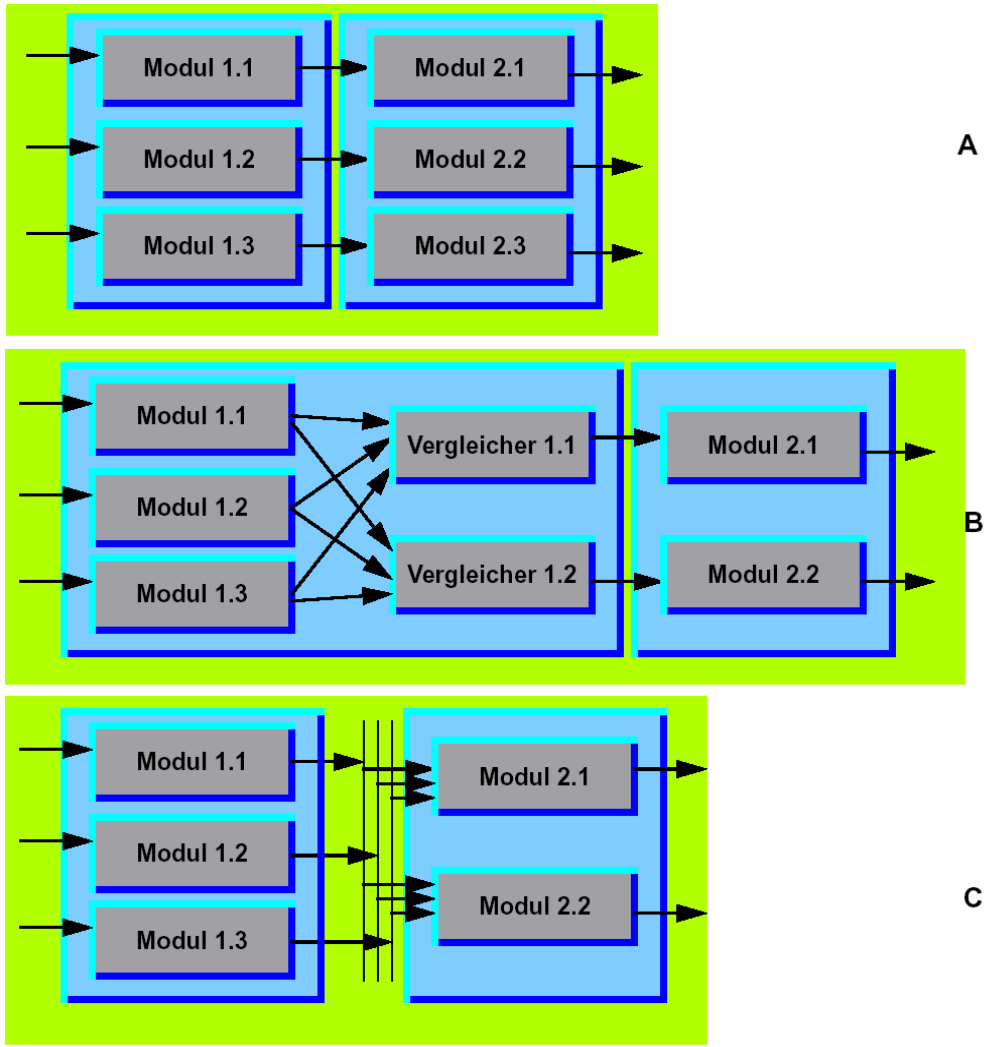


TMR: Dreifache Modulredundanz

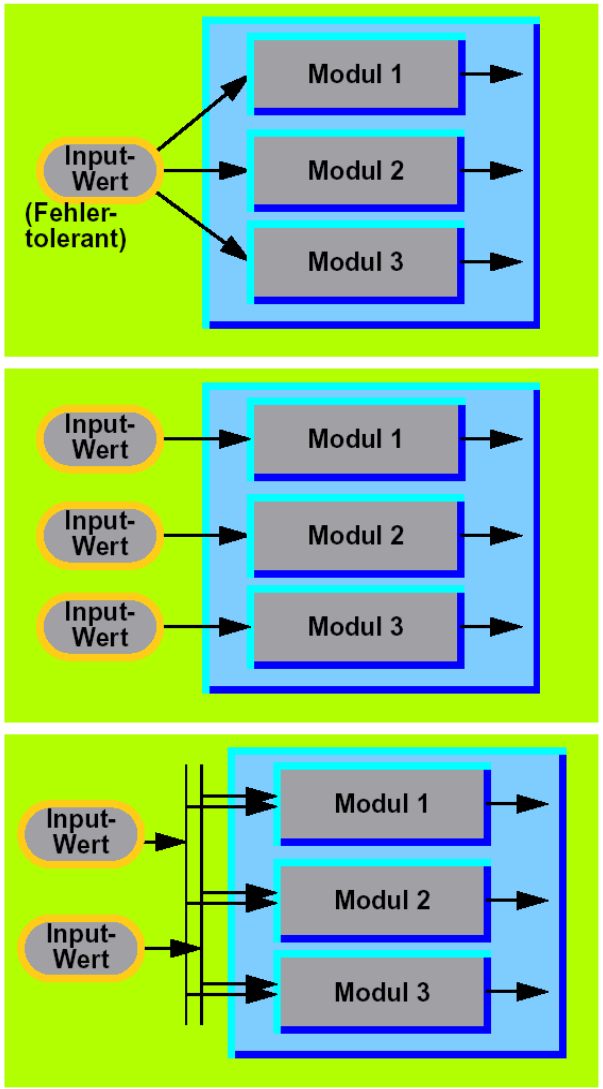
Fehlertoleranz Modelle.. TMR: Ist es sicher?



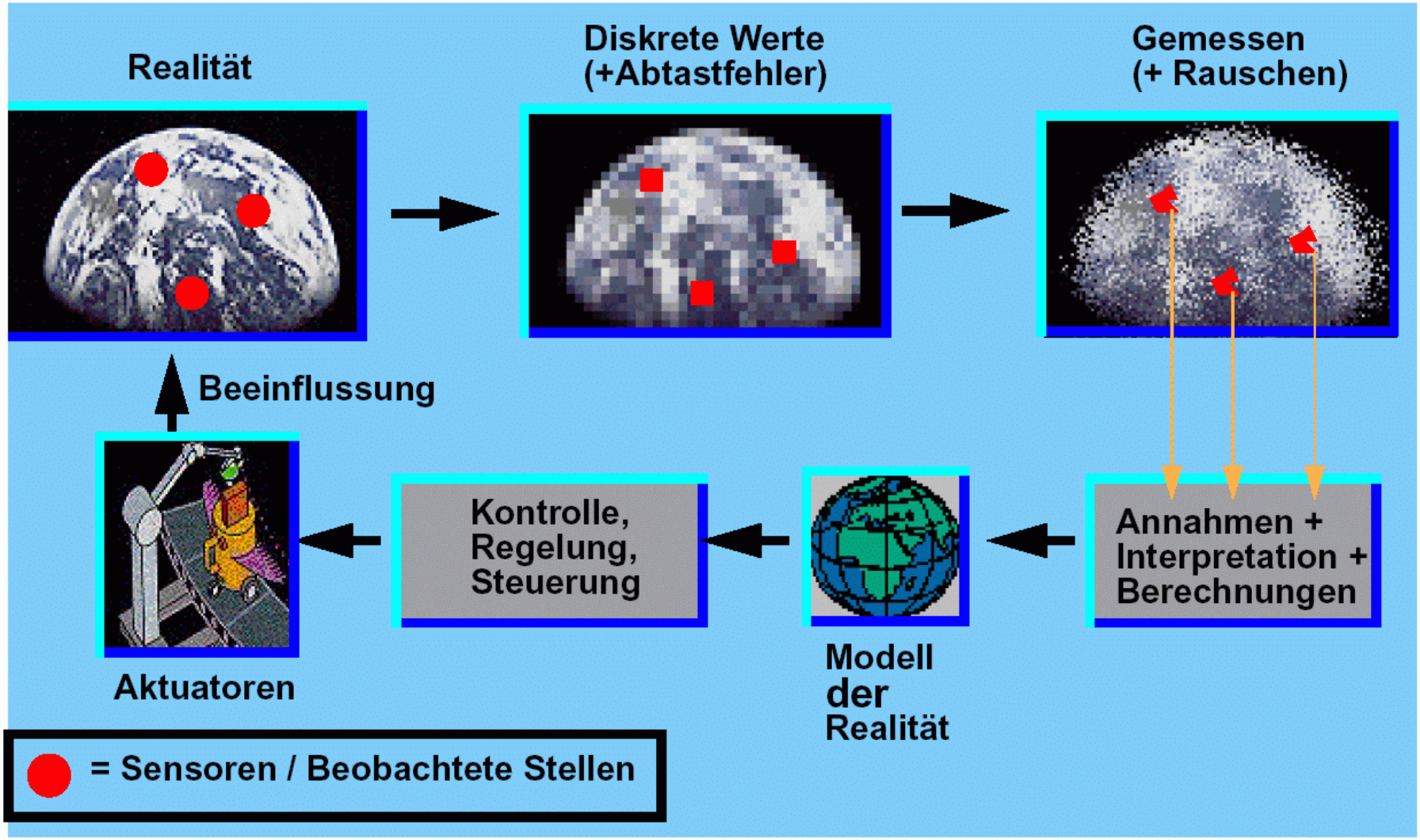
Fehlertoleranz Modelle.. TMR: Ist es sicher?



Fehlertoleranz Modelle.. TMR: Und die Inputs?

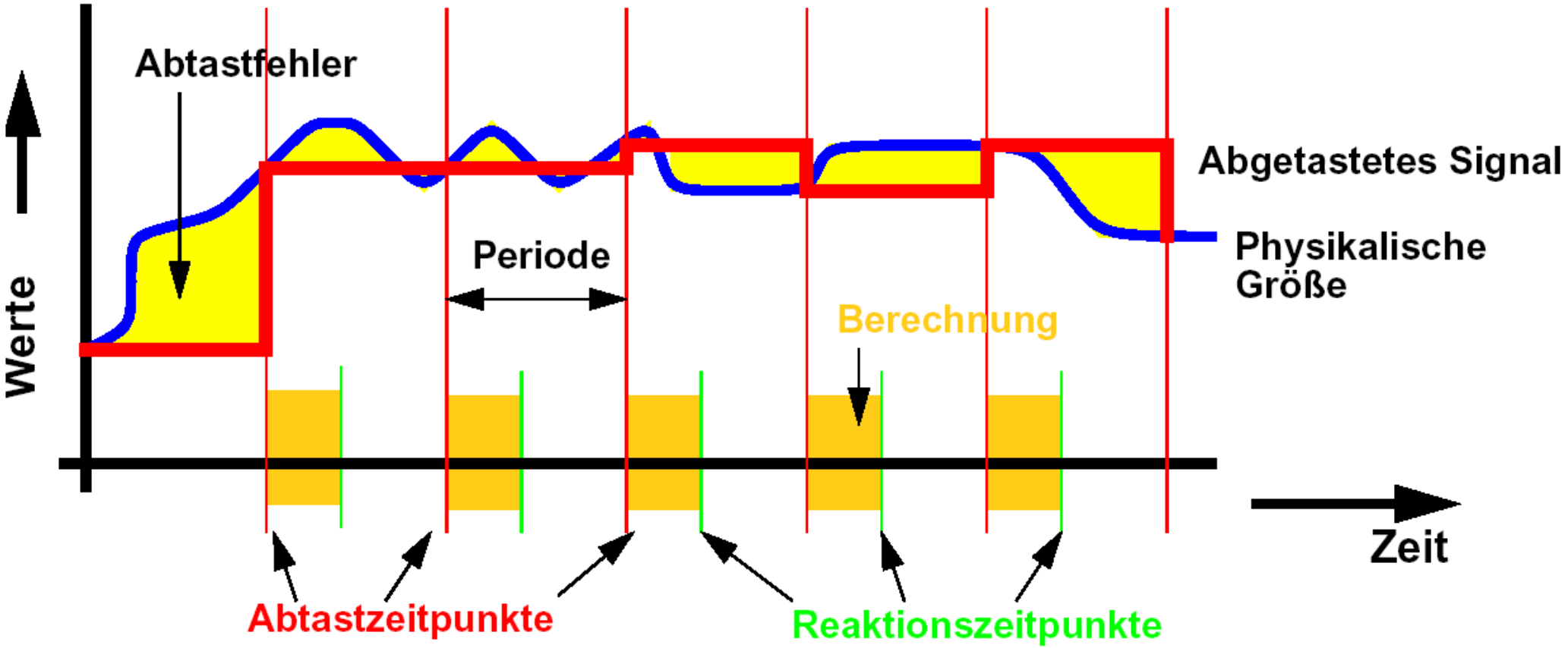


Was kann der Computer sehen? (dies ist noch kein Fehler, aber falsch)

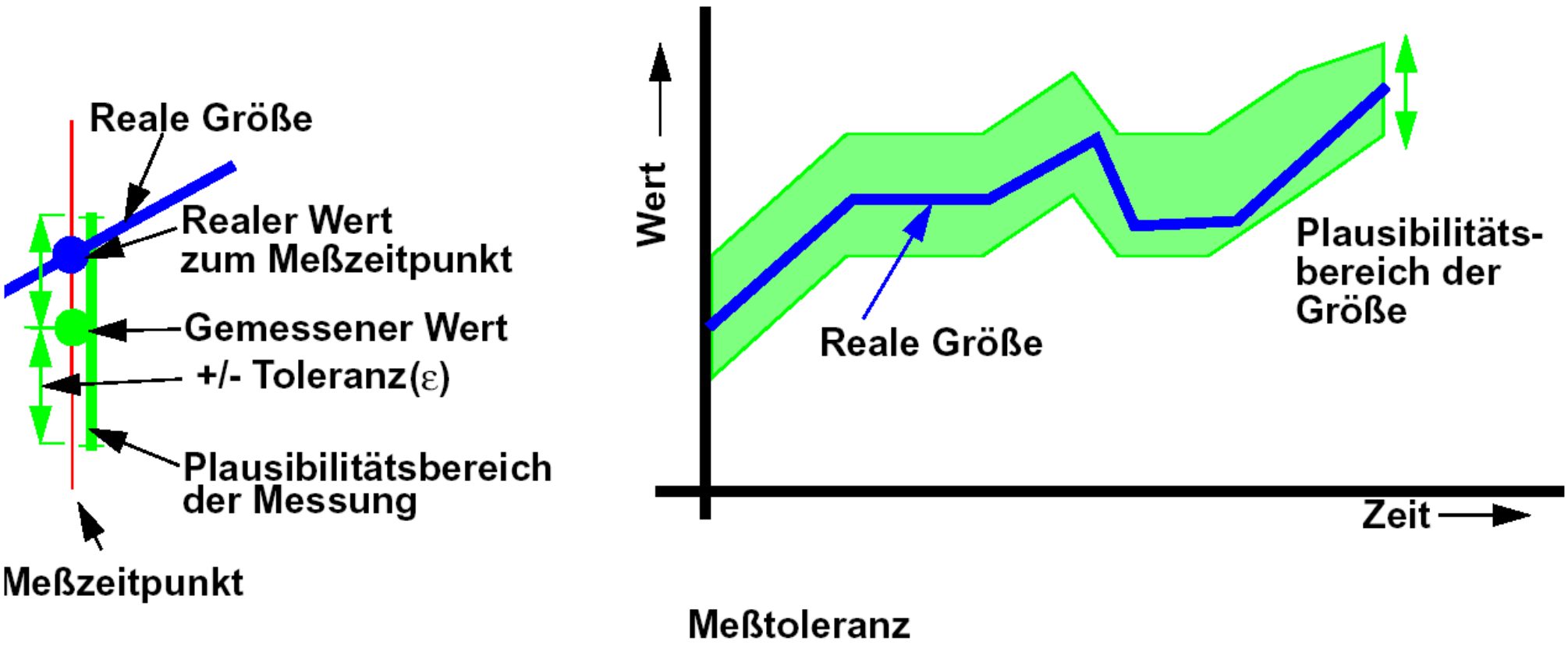


FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

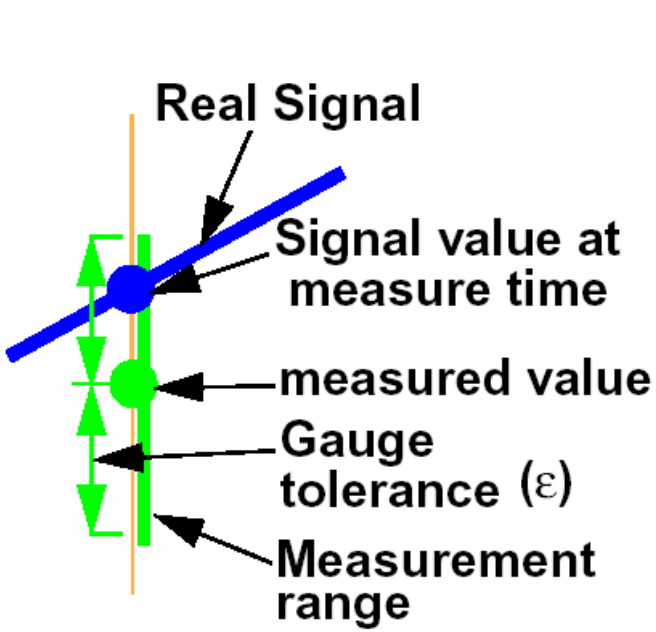
Was kann der Computer sehen? (Dies ist noch kein Fehler, aber falsch)

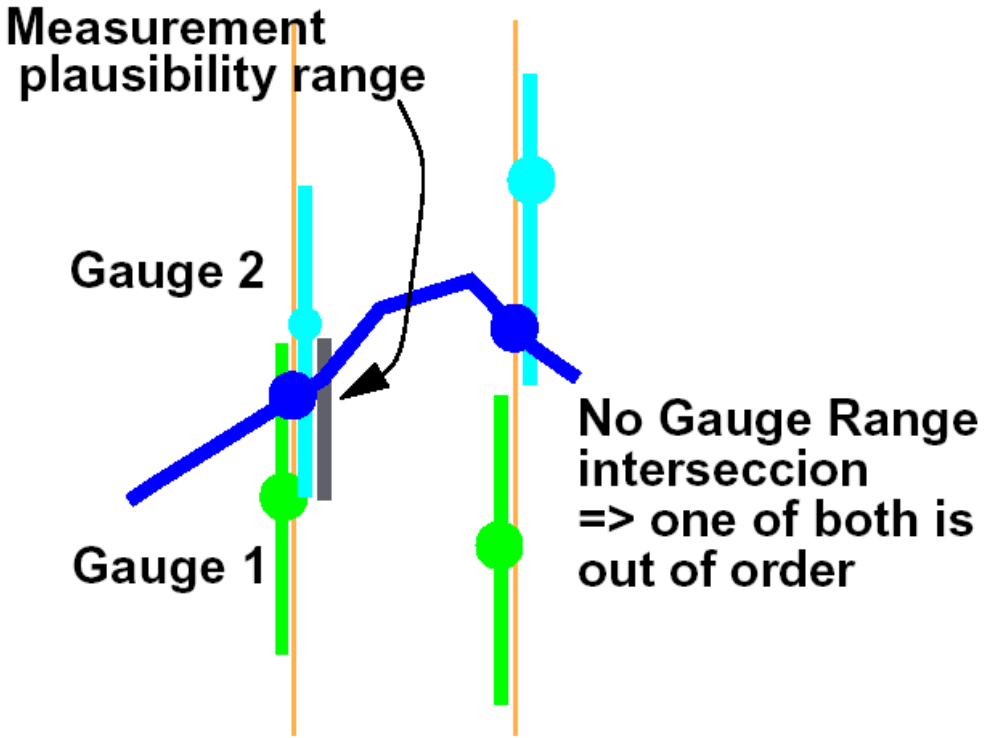


Sensor Toleranz..



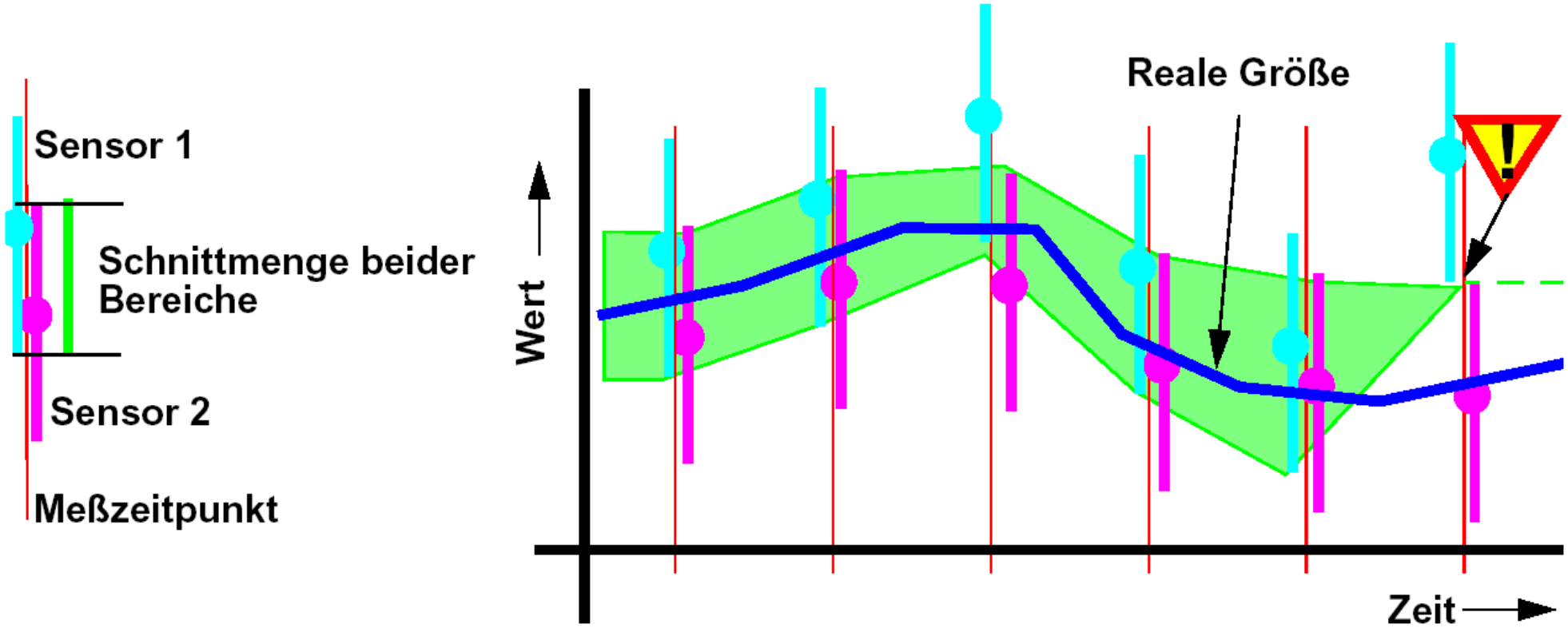
Sensor Toleranz..





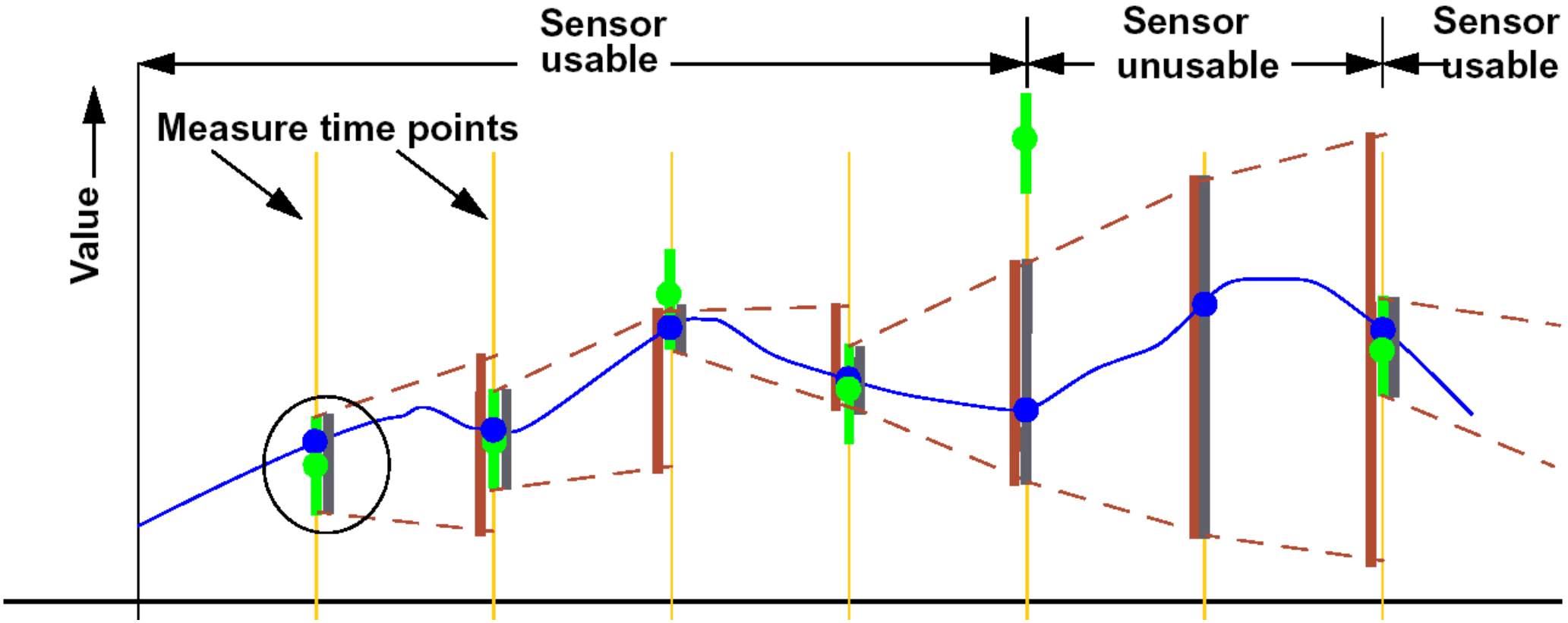
Gauge tolerance and the use of 2 or more Gauges

Sensor Toleranz..

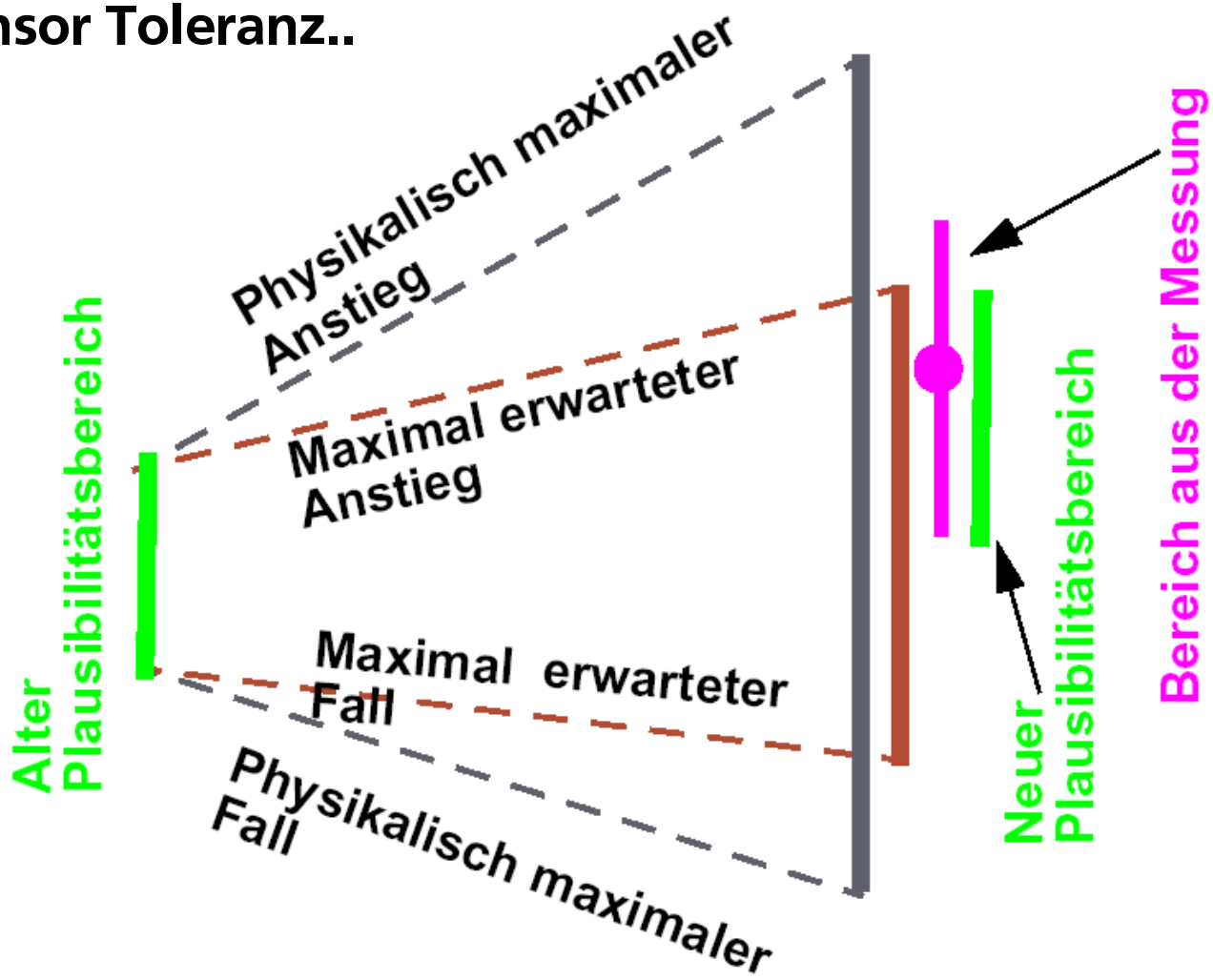


Direkte Redundanz engt den Plausibilitätsbereich ein

Sensor Toleranz..

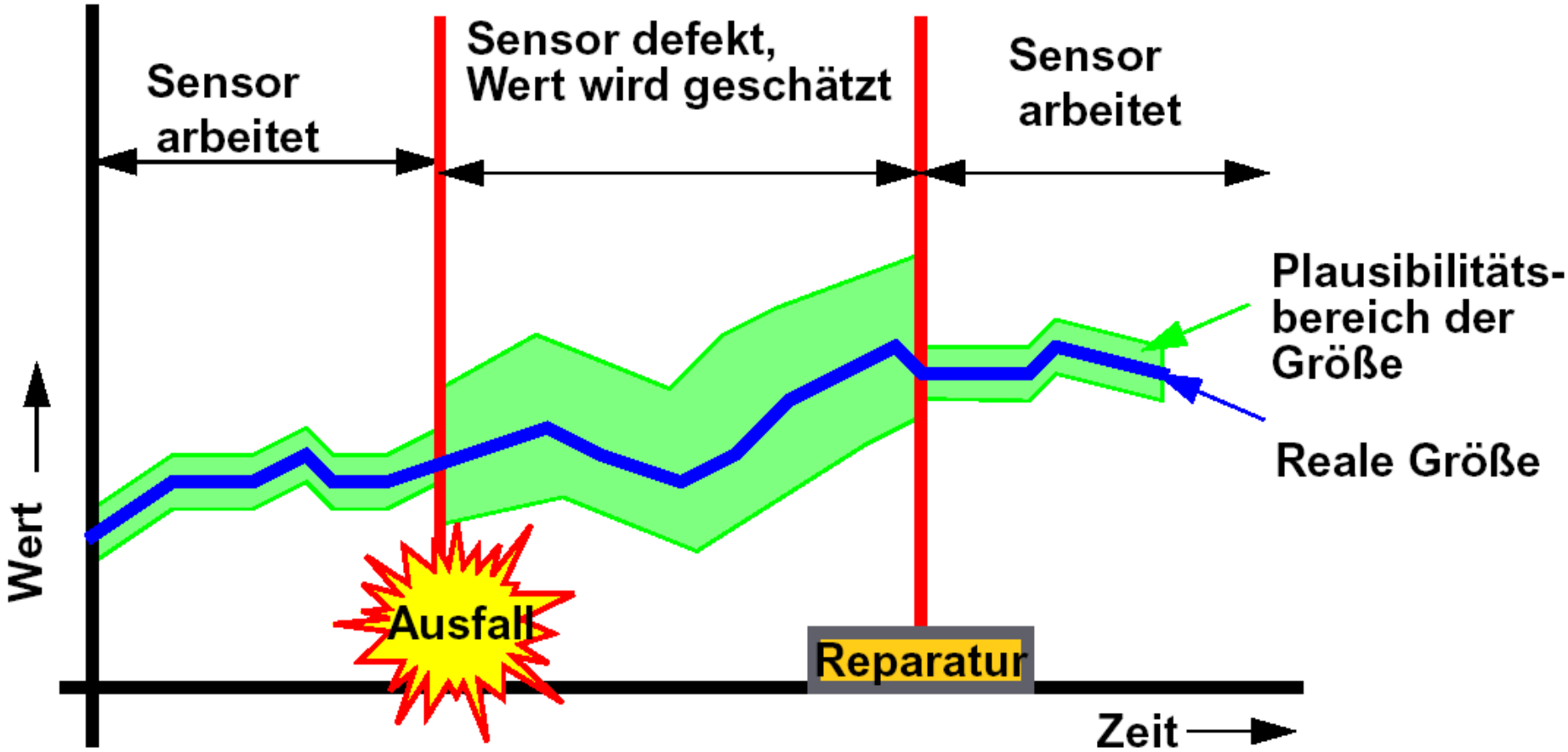


Sensor Toleranz..



Indirekte Redundanz engt den Plausibilitätsbereich ein

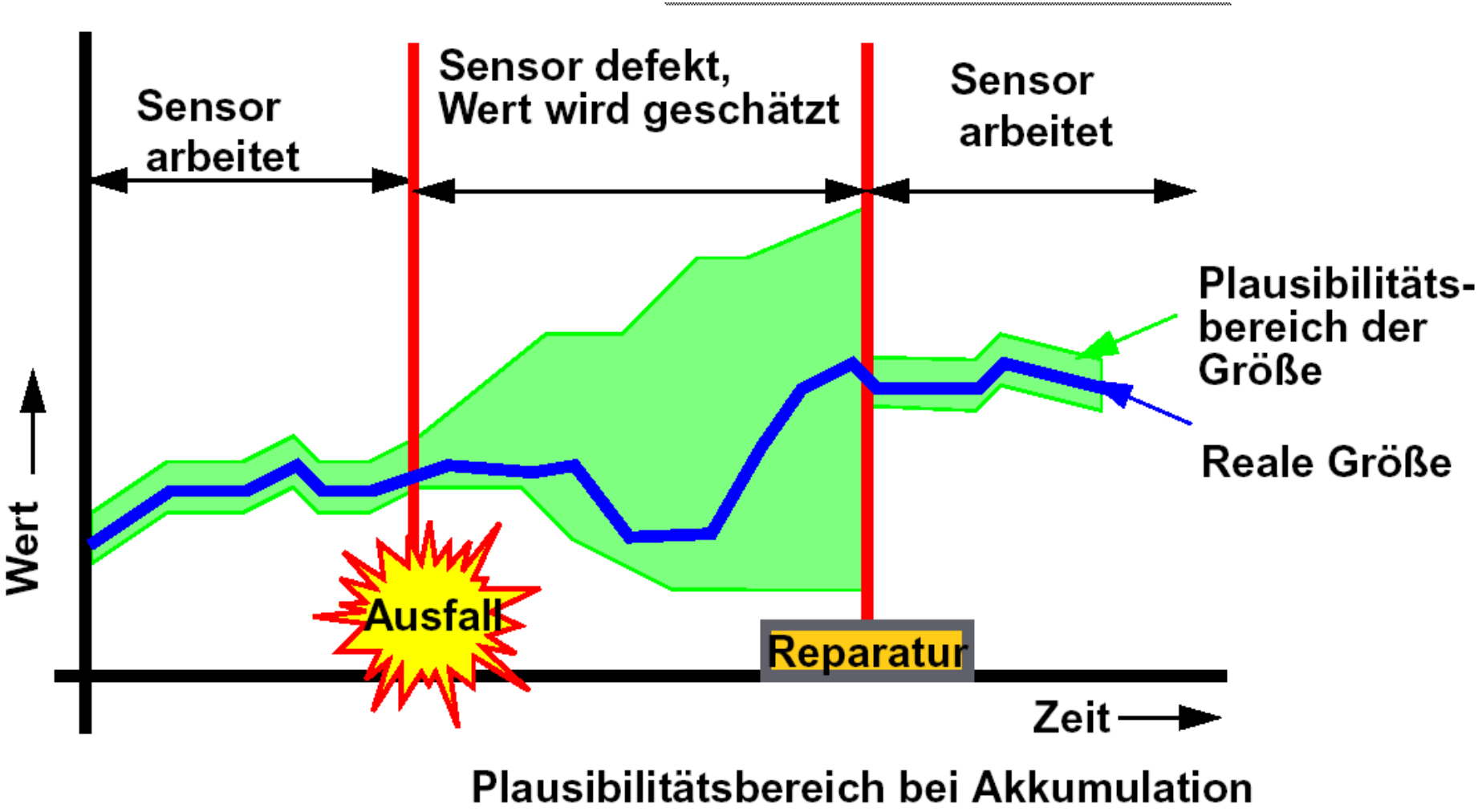
Sensor Toleranz..



Meßtoleranz und Abschätzungstoleranz

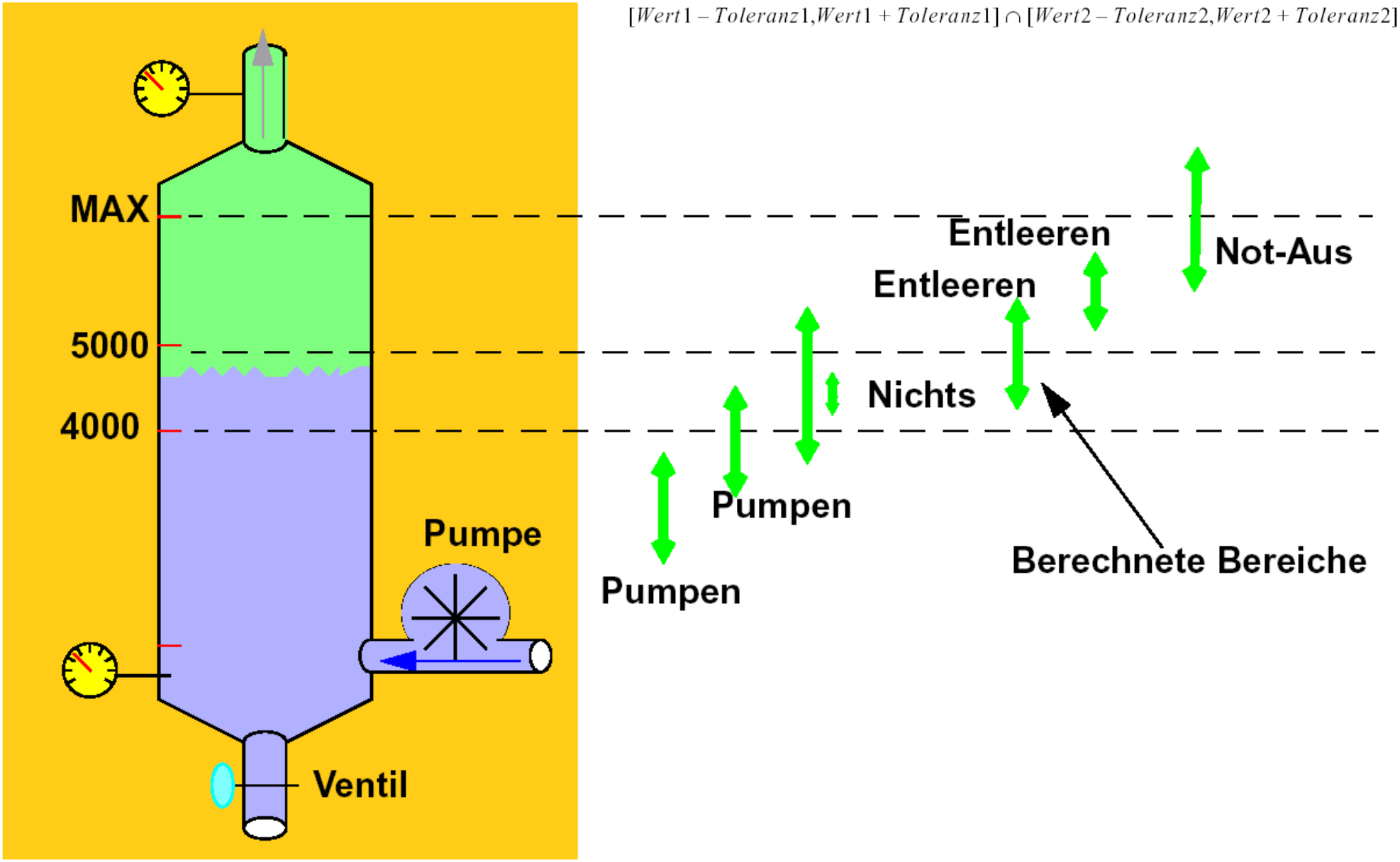
FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

Sensor Toleranz..



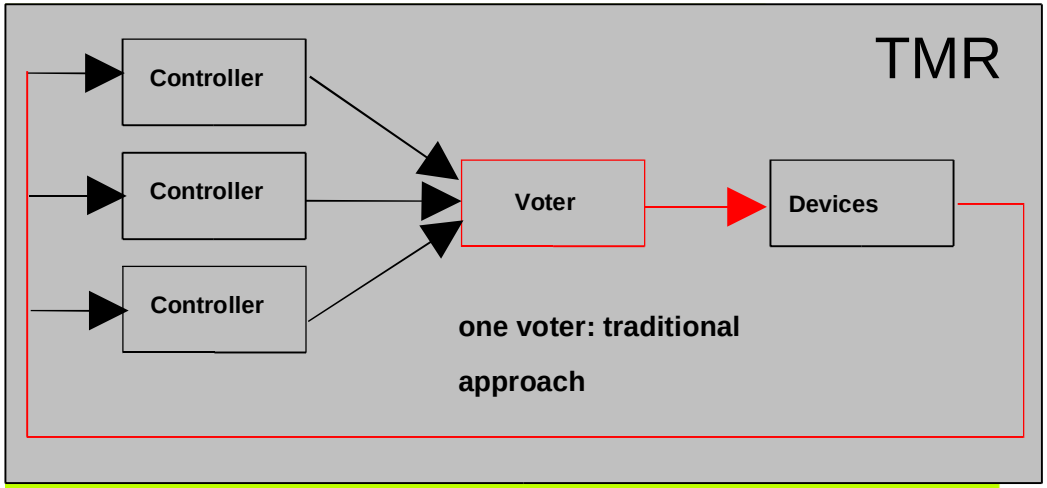
Plausibilitätsbereich bei Akkumulation

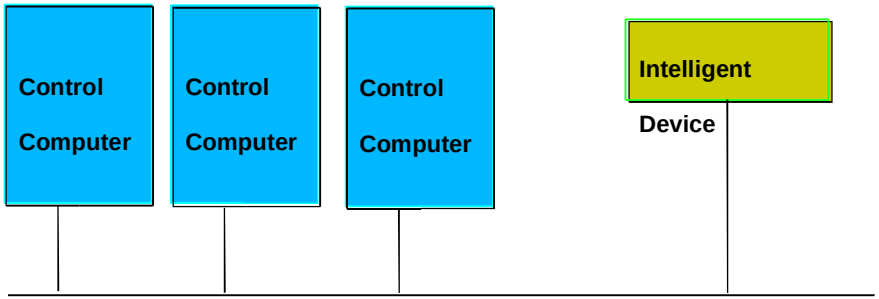
$$[Wert1 - Toleranz1, Wert1 + Toleranz1] \cap [Wert2 - Toleranz2, Wert2 + Toleranz2]$$



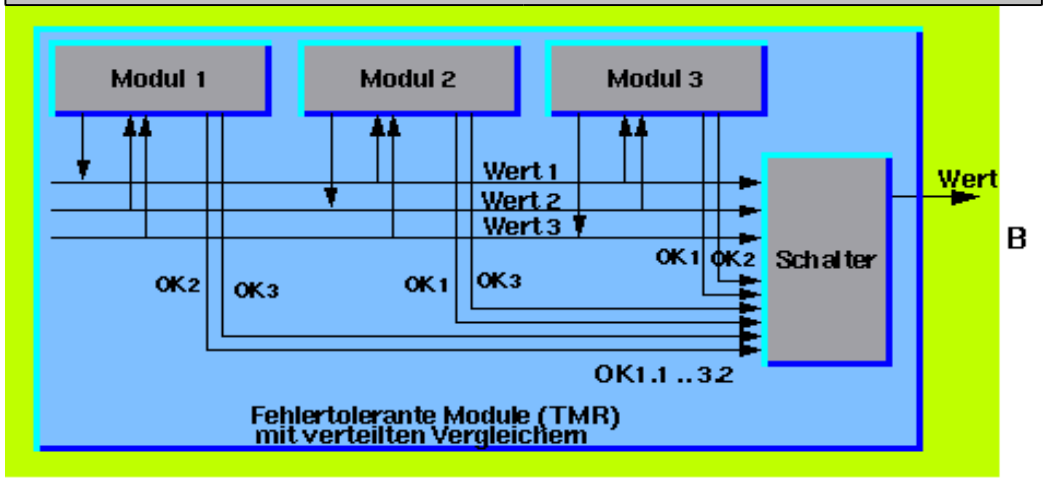
Steuerungsbeispiel

Alternativen





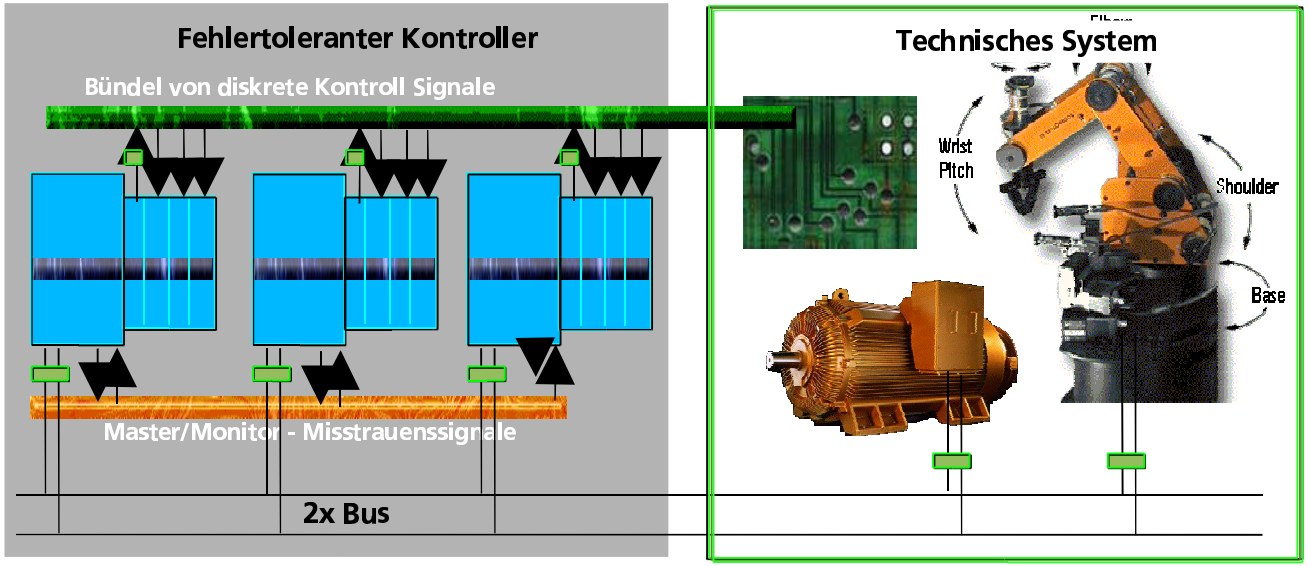
software voter, identification using
authentification

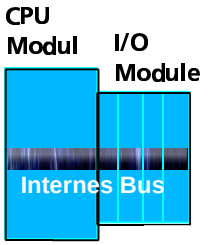


distributed voter, simple switch

Fraunhofer FIRST Institut Rechnerarchitektur und Softwaretechnik

EverControl: demonstrator for fault tolerance in real time





FIRST
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik