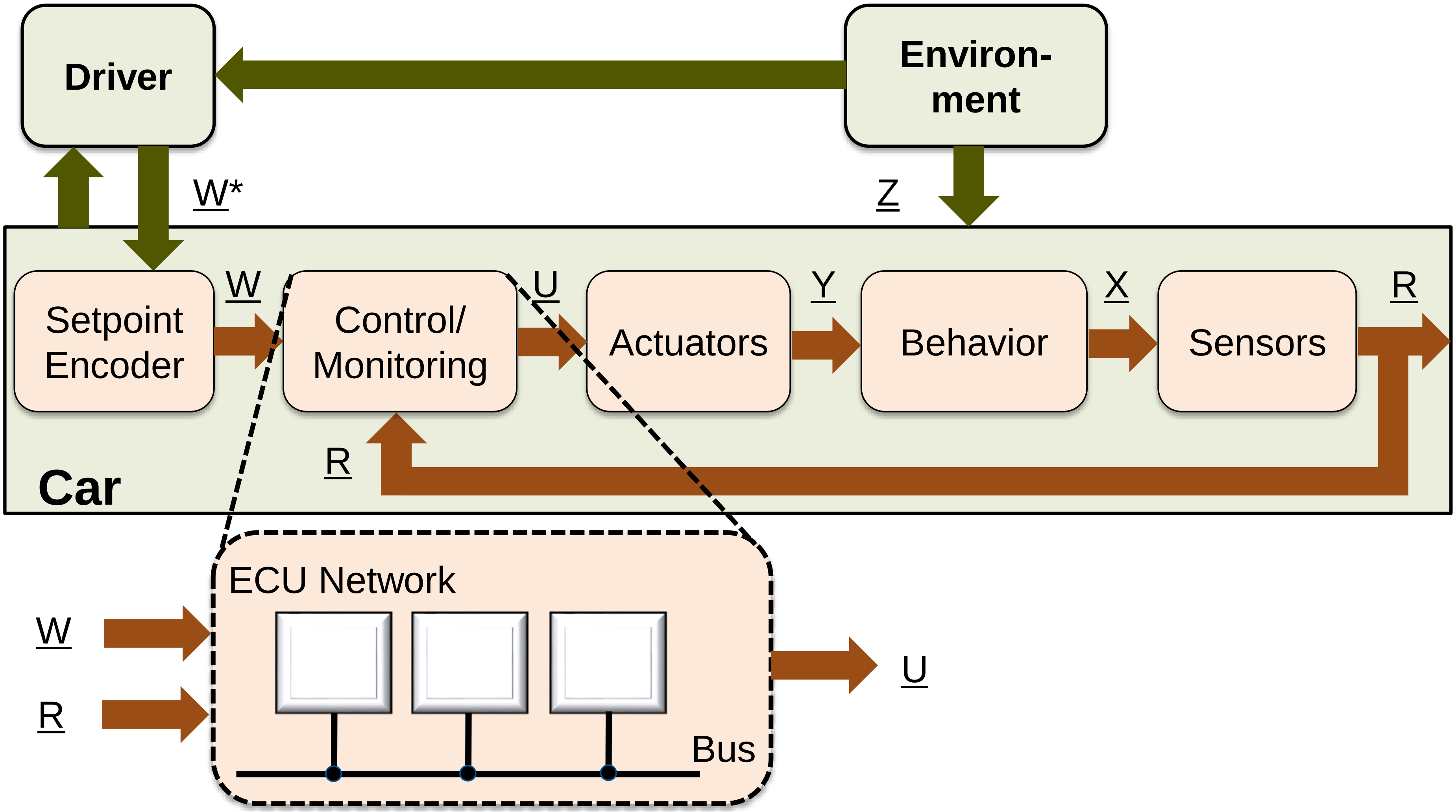
Software Platforms for Automotive Systems

Lecture 3: Reliability, Availability, and Safety

Alejandro Masrur

29th October 2015, TU Chemnitz

ECU Network = Control Tasks



Requirements on E/E Systems

- Harsh environmental conditions
  - EMI, wide temperature range, high humidity and vibration
- Relatively long product life cycles
  - Around 20 to 25 years
- Reliability and availability
  - Providing required functions in specified time interval
- Functional Safety
  - Risk analysis and criticality levels
  - Avoiding potential hazards for passengers and others

Safety Requirements

- **Accidents may cause material and human losses**
  - **Need for E/E systems that help reduce and avoid accidents**
- **For safety-critical tasks of E/E systems**
  - **Analyzing and assessing the situation**
    - **Monitoring engine and outside temperature, etc.**
    - **Glaze warning, traffic jam, etc.**
  - **Suggesting an action**
    - **Navigation, warnings on the instrument panel, etc.**
  - **Accomplishing an action**
    - **Braking, Steering, turning on lights, etc.**

Concepts

- There are norms concerned with these topics
  - Reliability: DIN 40041
  - Availability: DIN 40042
  - Safety: DIN 31000
- Some necessary nomenclature
  - System or subsystem:

    “Any Software and/or hardware component needed for implementing functionality within a car.”
  - Operational state:

    “The condition of a system or subsystem by which it provides the required functions.”

Definitions

- **Reliability:**

  “This is the property or ability of a system or subsystem of being operational according to specified operation conditions and for a specified time interval.”

- **Availability:**

  “This is the probability that a system or subsystem is in operational state at a given point in time.”

- **Unavailability:**

  “This is the probability that a system or subsystem is in non-operational state at a given point in time.”

- **Safety:**

  “This defines the *state of affaires* by which risk is kept within acceptable bounds.”

Definitions

- **Fault or defect:**

  "This is an unacceptable deviation of one or more parameters of a system or subsystem making it behave different than expected."

  - **Different kinds: design, software, hardware faults, etc.**

- **Failure:**

  "This is an interruption in the normal operation of a system or subsystem which then stops being operational."

  - **Different kinds: random, systemic, deterministic failures, etc.**

- **Malfunction:**

  "This is a temporary interruption in the normal operation of a system or subsystem."

Fault vs. Failure/Malfunction

"A lamp burns out. Car's lights are unavailable."

- **Hardware fault: filament burns out**
- **Failure: car's lights are unavailable…**

"Routine addresses wrong RAM space. ACC resets."

- **Software fault: wrong addressing**
- **Malfunction: ACC resets…**

"Gas pedal gets trapped in carpet. Gas pedal blocks."

- **Design defect: gas pedal gets trapped**
- **Malfunction/failure: Car accelerates without control…**

Reliability

- **Ideally a system should always be operational**
  - **However, this rarely happens in reality**
- **Need to model the failure behavior of systems**
  - **Statistical methods have established**

Reliability Function

- *Empirical* normalized sum of failures

$$\hat{F}(t) = \frac{n(t)}{N_0} \begin{cases} n(t) = \text{number of failing systems} \\ N_0 = \text{total number of systems} \end{cases}$$

- *Empirical* reliability function

$$\hat{R}(t) = \frac{N_0 - n(t)}{N_0}$$

Reliability Function

- **Failure probability function:**

$$N_0 \to \infty \Rightarrow \hat{F}(t) \to F(t)$$

By law of large numbers

- **Reliability function**

$$\hat{R}(t) = 1 - \frac{n(t)}{N_0} \xrightarrow{N_0 \to \infty} \underbrace{R(t)}_{\text{Probability system is operational}} = 1 - F(t)$$

Failure Rate

- **Empirical failure rate**

$$\hat{\lambda}(t) = \frac{n(t+\Delta t) - n(t)}{N_0 - n(t)} \times \frac{1}{\Delta t}$$

$n(t)$ = number of failing systems

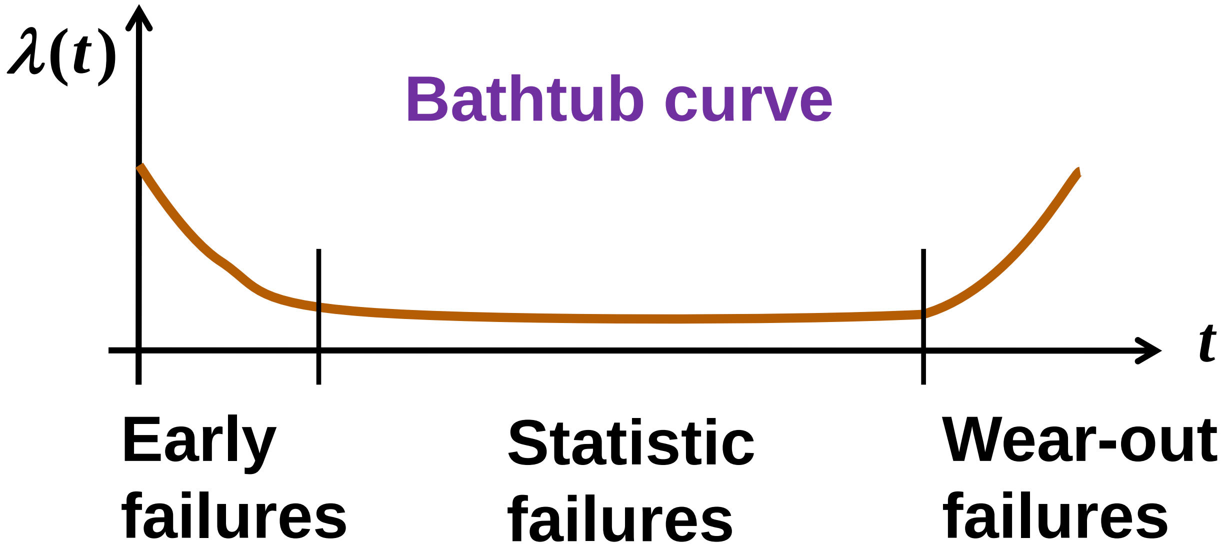
N_0 = total number of systems

$$\hat{\lambda}(t) = \frac{\frac{n(t+\Delta t)}{N_0} - \frac{n(t)}{N_0}}{1 - \frac{n(t)}{N_0}} \times \frac{1}{\Delta t} \qquad N_0 \to \infty, \Delta t \to 0 \Rightarrow \hat{\lambda}(t) \to \lambda(t)$$

$$\lambda(t) = \frac{1}{R(t)} \cdot \frac{dR(t)}{dt}$$

Failure rate: number of failures per time unit

Failure Rate over Time

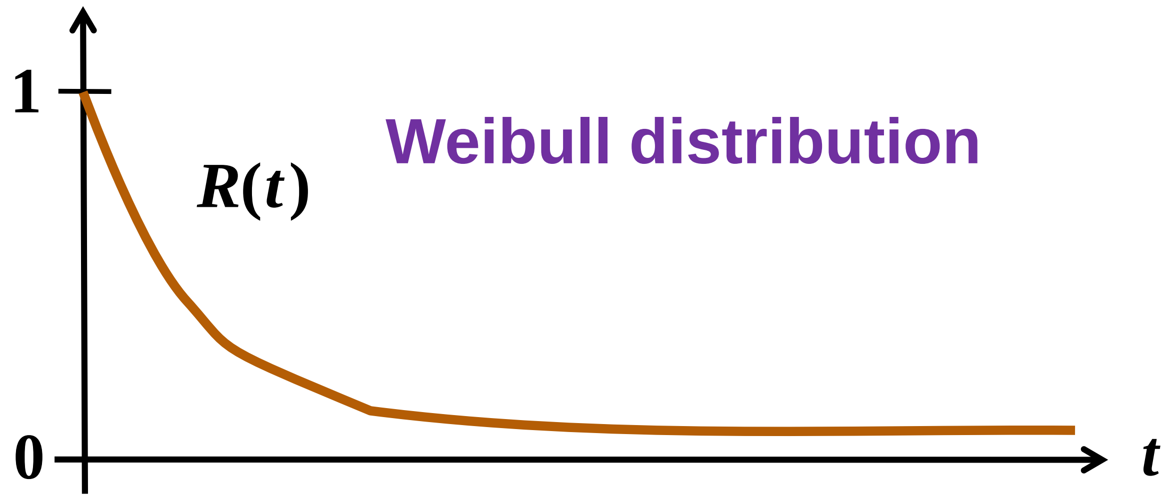


- Early failures: fabrication defects
- Statistic failures: non-deterministic defects/faults
- Wear-out failures: aging effects

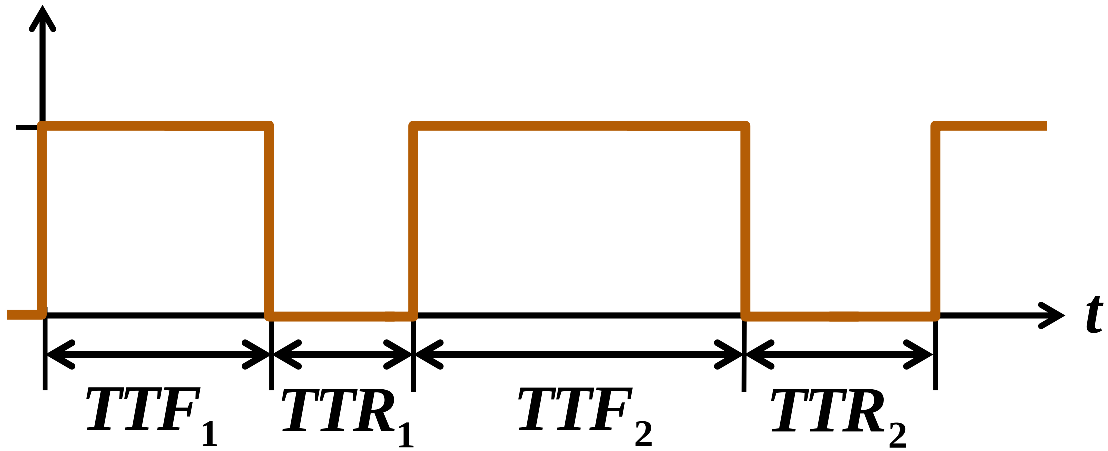
Statistic Failures

- Affect the system for a longer period of time
- Have (almost) constant nature

$$\lambda(t) = \frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \xrightarrow{\lambda(t)=\lambda} R(t) = \frac{1}{\lambda} \cdot \frac{dR(t)}{dt} \Rightarrow R(t) = e^{-\lambda t}$$



MTTF and MTTR



- **Mean Time To Failure (MTTF)**

$$MTTF = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N} TTF_i \xrightarrow{\lambda(t)=\lambda} MTTF = \frac{1}{\lambda}$$

- **Mean Time To Repair (MTTR)**

Repair rate

$$MTTR = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N} TTR_i \xrightarrow{definition} MTTR = \frac{1}{\rho}$$

Availability and Unavailability

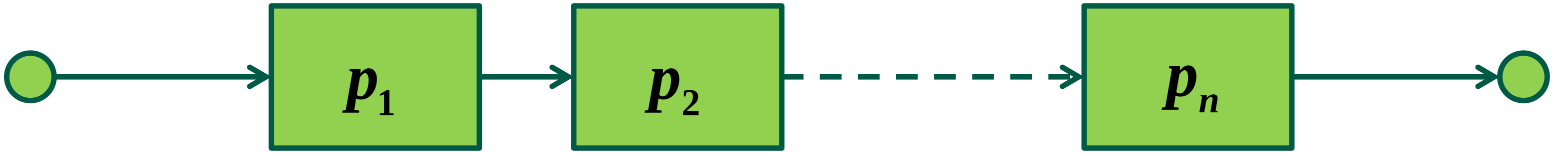
- **Availability**

$$p = \frac{MTTF}{MTTF + MTTR} = \frac{1}{1 + \dfrac{MTTR}{MTTF}} \Rightarrow \frac{1}{1 + \dfrac{\lambda}{\rho}}$$

- **Unavailability**

$$q = 1 - p = 1 - \frac{MTTF}{MTTF + MTTR} = \frac{1}{1 + \dfrac{MTTF}{MTTR}} \Rightarrow \frac{1}{1 + \dfrac{\rho}{\lambda}}$$

Serial Connection of Systems



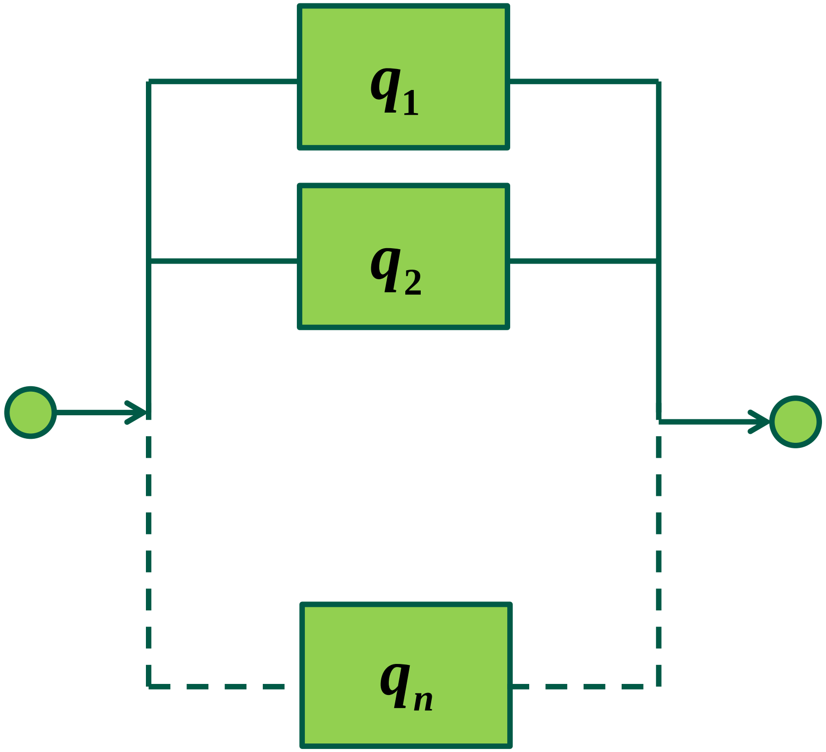
$$p_{total} = \prod_{i=1}^{n} p_i$$

Systems have to be Independent

$$p_{total} = 1 - q_{total} = \prod_{i=1}^{n} (1 - p_i) \xrightarrow{q_i << 1} \approx 1 - \sum_{i=1}^{n} q_i$$

$$q_{total} = 1 - p_{total} = 1 - \prod_{i=1}^{n} p_i \xrightarrow{p_i >> 0} \approx \sum_{i=1}^{n} q_i$$

Parallel Connection of Systems

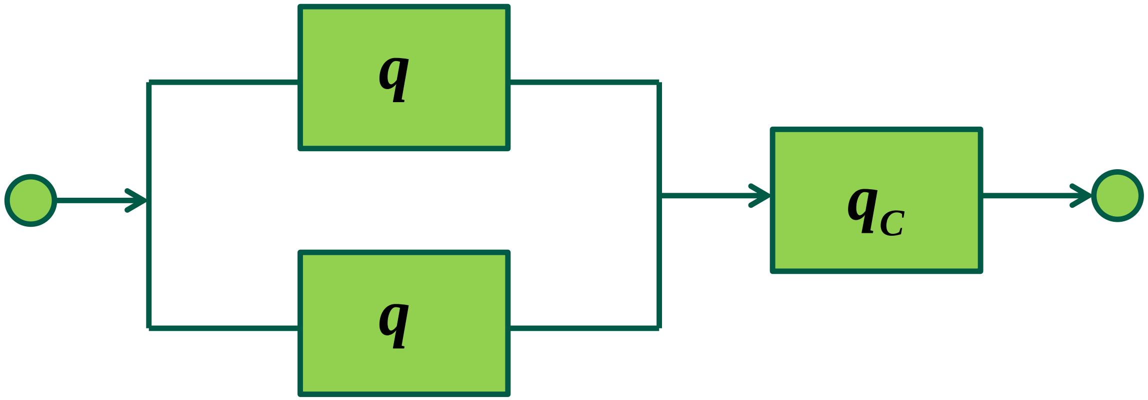


$$q_{total} = \prod_{i=1}^{n} q_i$$

Systems have to be independent

$$p_{total} = 1 - q_{total} = 1 - \prod_{i=1}^{n} q_i$$

Redundant Connection of Systems

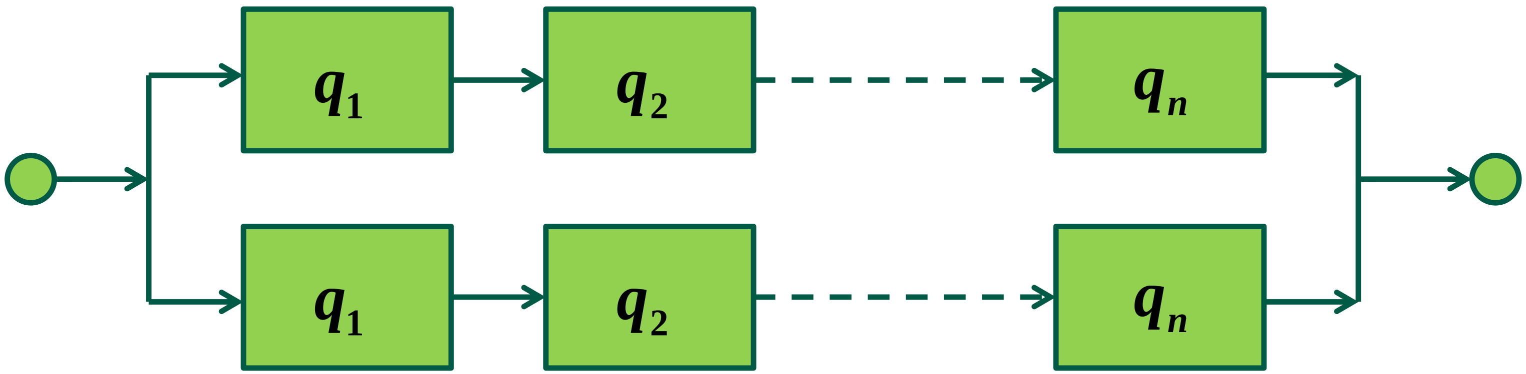


$q^2 + q_C << q$ **Necessary requirement**

$q^2 << q$ **Normally holds**

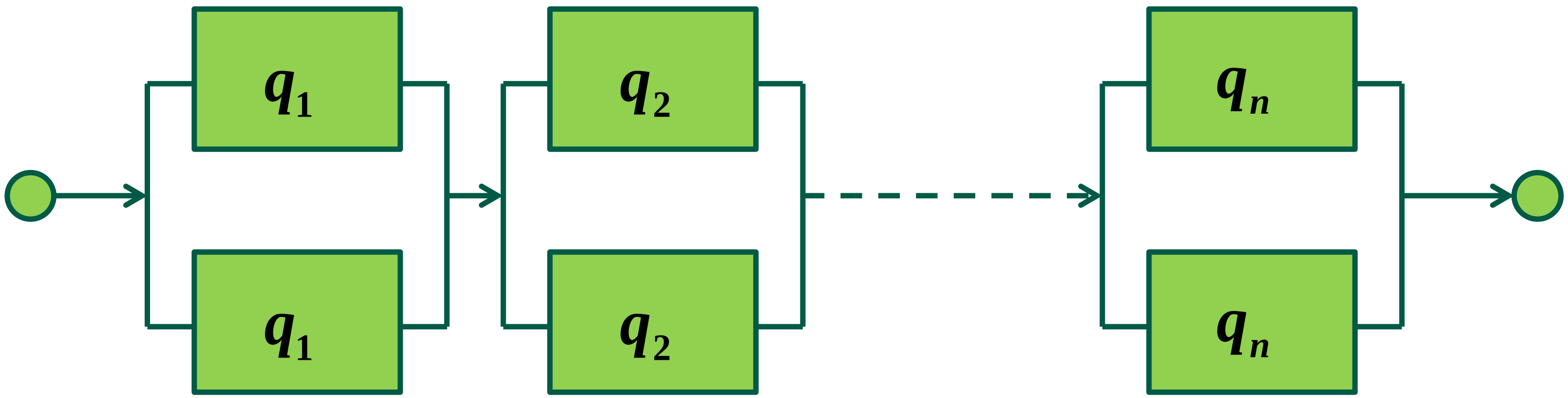
$\Rightarrow q_C << q - q^2$ **Requirement for coupling**

Mixed Connection of Systems



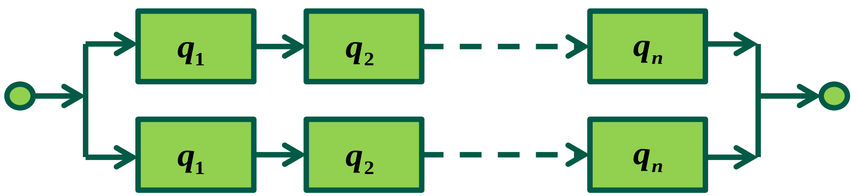
$$q_A \approx (q_1 + q_2 + \ldots + q_n)^2$$

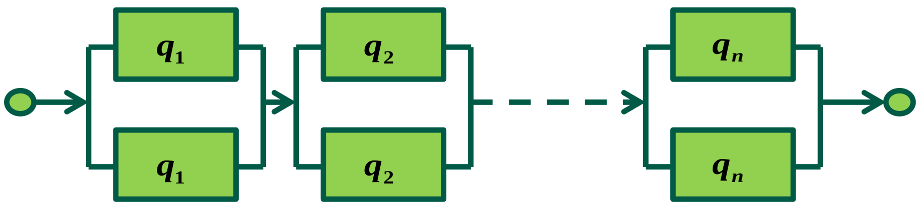
Mixed Connection of Systems



$$q_B \approx (q_1^2 + q_2^2 + \ldots + q_n^2)$$

Which is Better?





$$q_A \approx (q_1 + q_2 + \ldots + q_n)^2$$

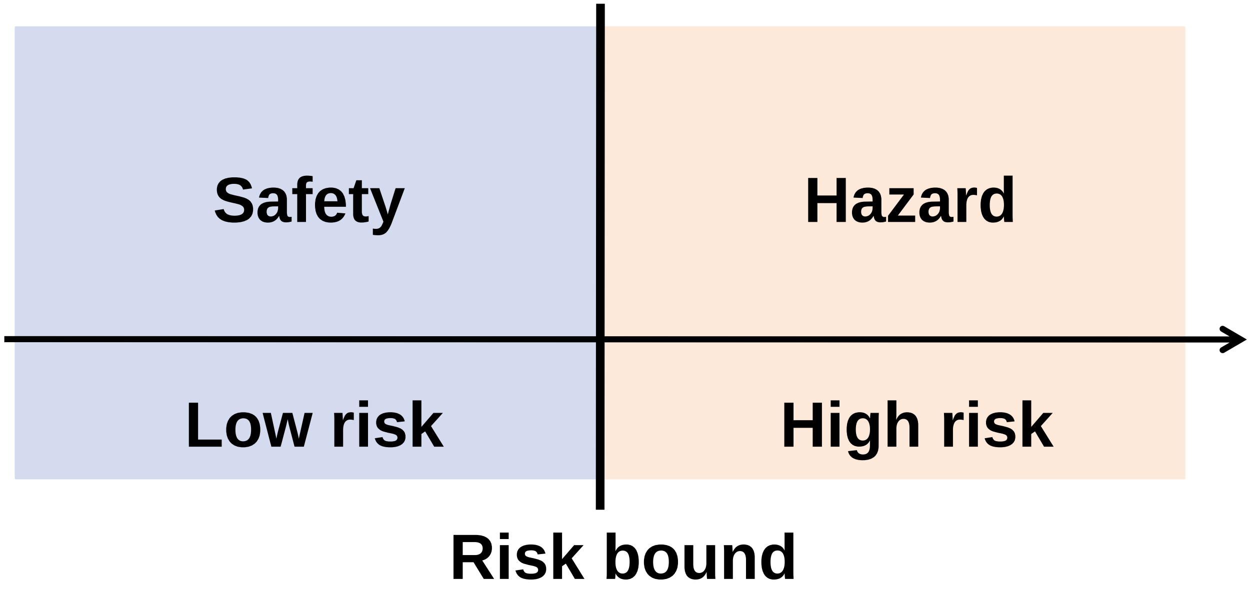
$$q_B \approx (q_1^2 + q_2^2 + \ldots + q_n^2)$$

$$q_A \approx ((q_1 + q_2) + (\ldots + q_n))^2$$

$$q_A \approx (q_1 + q_2)^2 + 2(q_1 + q_2)(\ldots + q_n) + (\ldots + q_n)^2$$

$$q_A \approx q_B + 2(q_1 q_2 + q_1 q_n + q_2 q_n + \ldots) > q_B$$

Safety

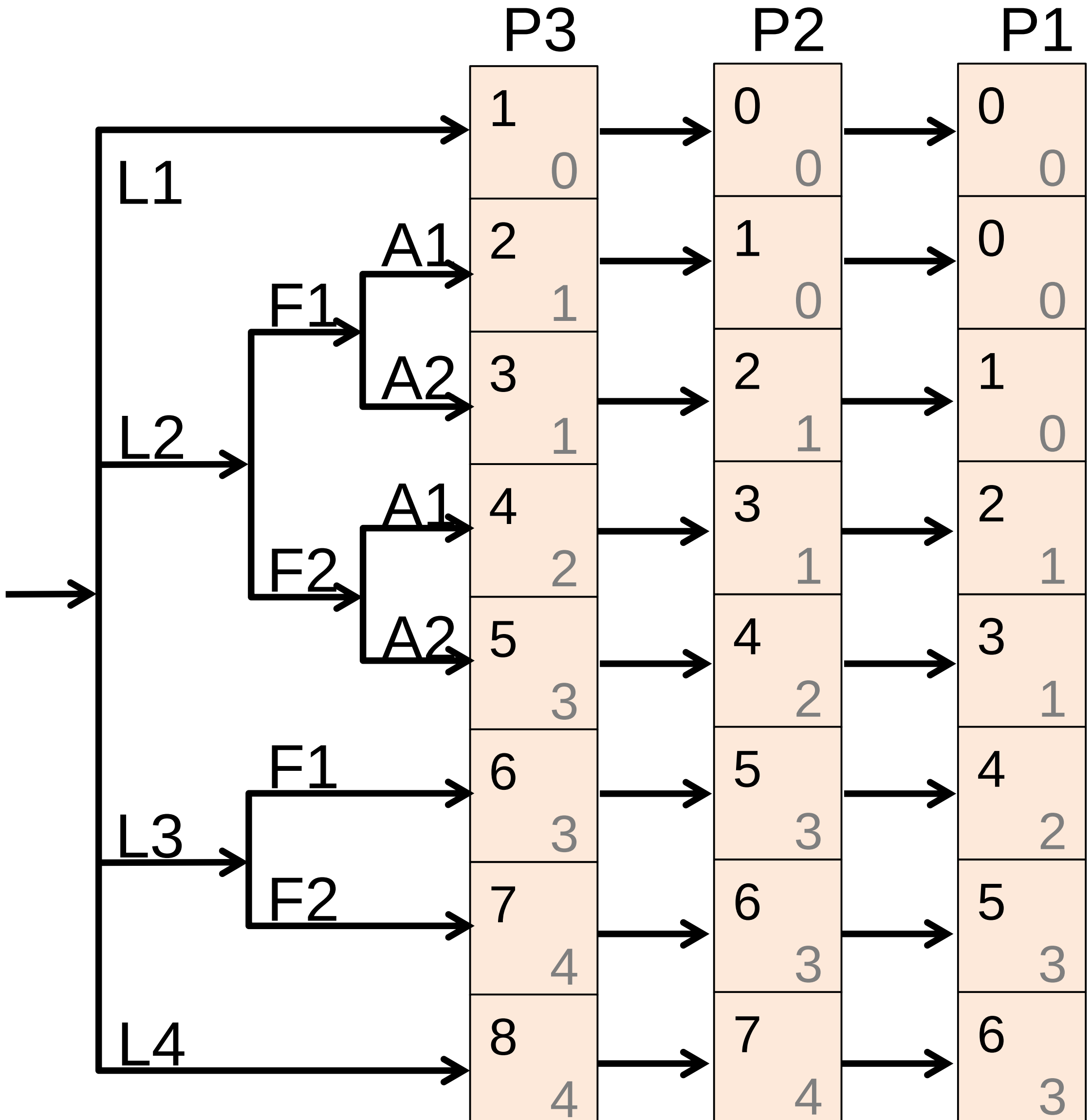


- DIN 31000 deals with safety aspects
  - Risk of potential damage to either material or humans
  - Risk in the automotive domain:
    - Probability of an accident vs. probability of damage

Analysis of Risk

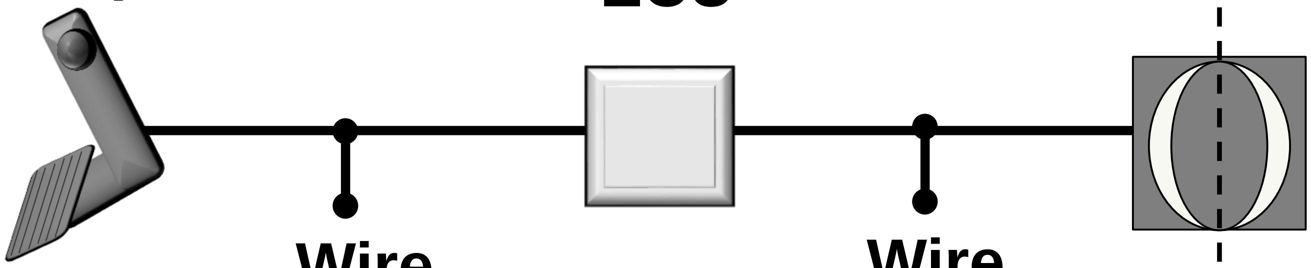
- There are norms for analysis of risk
  - DIN 19250
  - IEC 61508
- The risk graph determines
  - Probability and frequency of a hazardous event
  - Level of damage and possibility of avoidance
  - Requirements class (RC) according to DIN
    - RC from 0 to 8
  - Safety Integrity Level (SIL) according to IEC
    - SIL from 0 to 4

Risk Graph



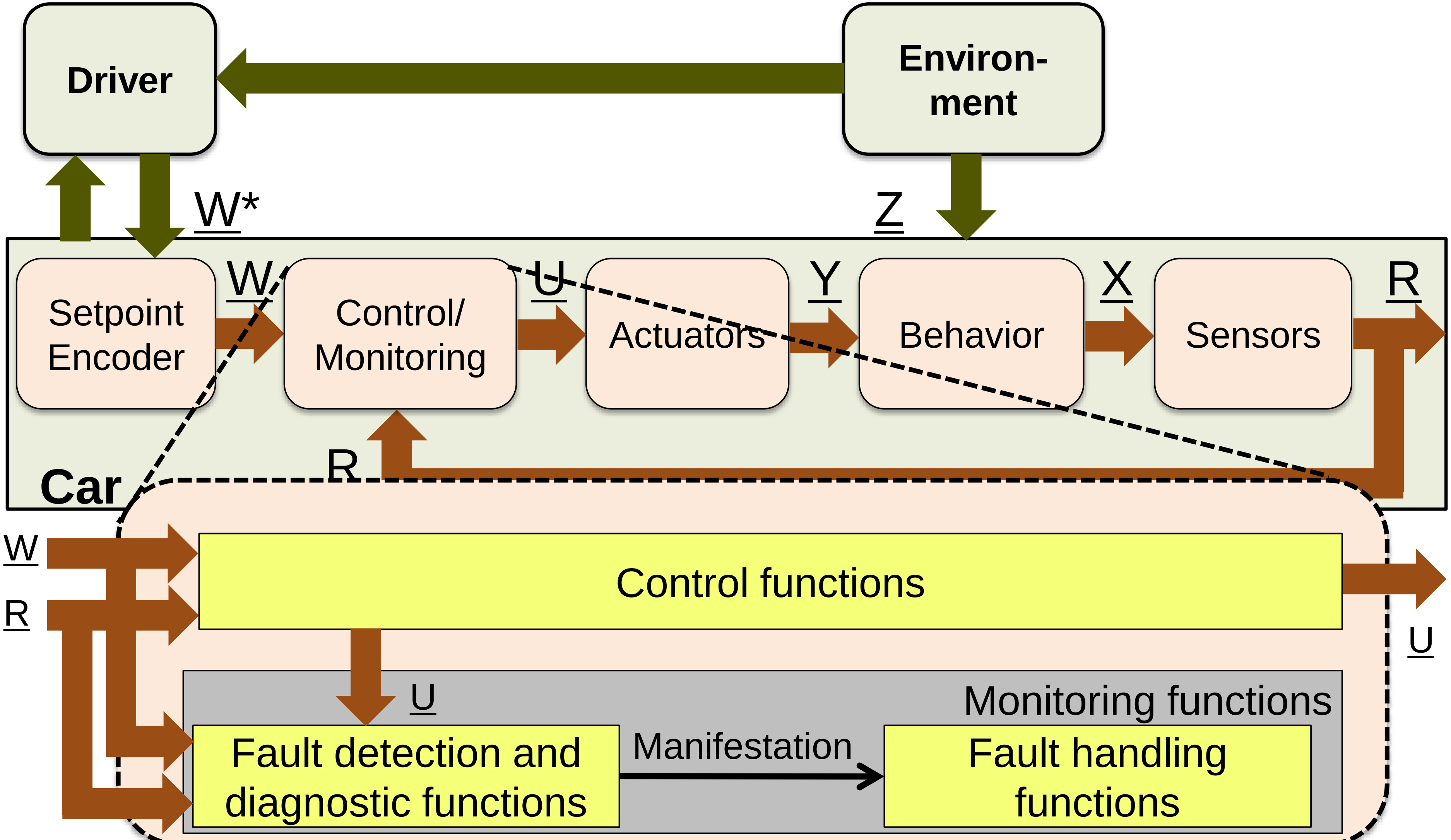
- **Level of damage**
  - **L1: light**
  - **L2: severe**
  - **L3: extreme**
  - **L4: catastrophic**
- **Frequency:**
  - **F1: seldom – often**
  - **F2: frequent-continuous**
- **Possibility of avoidance**
  - **A1: possible**
  - **A2: not possible**
- **Probability of occurrence**
  - **P1: rare**
  - **P2: low**
  - **P3: high**
- **RC <--> SIL**

Example: E-Gas System



- Situation: convoy at high speed
- Potential hazard: undesired acceleration and crashing
- Risk Analysis
  - L3: injuries and possibly deaths of many people
  - F1: seldom up to often
  - P1: rare
- RC 4 and SIL 2

Monitoring and Diagnostics



Safety-Aware Systems

- Fail-Safe Systems
  - System is turned off to avoid damage
    - Very restrictive, but sometimes necessary
- Fail-Reduce Systems
  - System‘s functionalities are degraded to avoid damage
    - Degradation modes
    - Criticality level need to be defined
- Fail-Operational Systems
  - System continues operation in normal way
    - Redundancy required

Summary

- **Reliability**
  - **Empirical functions and failure rate**
  - **Reliability function**
- **Availability**
  - **Mean Time To Failure**
  - **Mean Time To Repair**
  - **Connections of Systems**
- **Safety**
  - **DIN norm, IEC norm and risk graph**
  - **Safety level of classes and safety-aware systems**