AARHUS
UNIVERSITY
DEPARTMENT OF ENGINEERING

Architecture & Design of Embedded Real-Time Systems (TI-AREM)

Safety and Reliability Patterns

B.D. Chapter 9. 405-456

Version: 13-3-2015

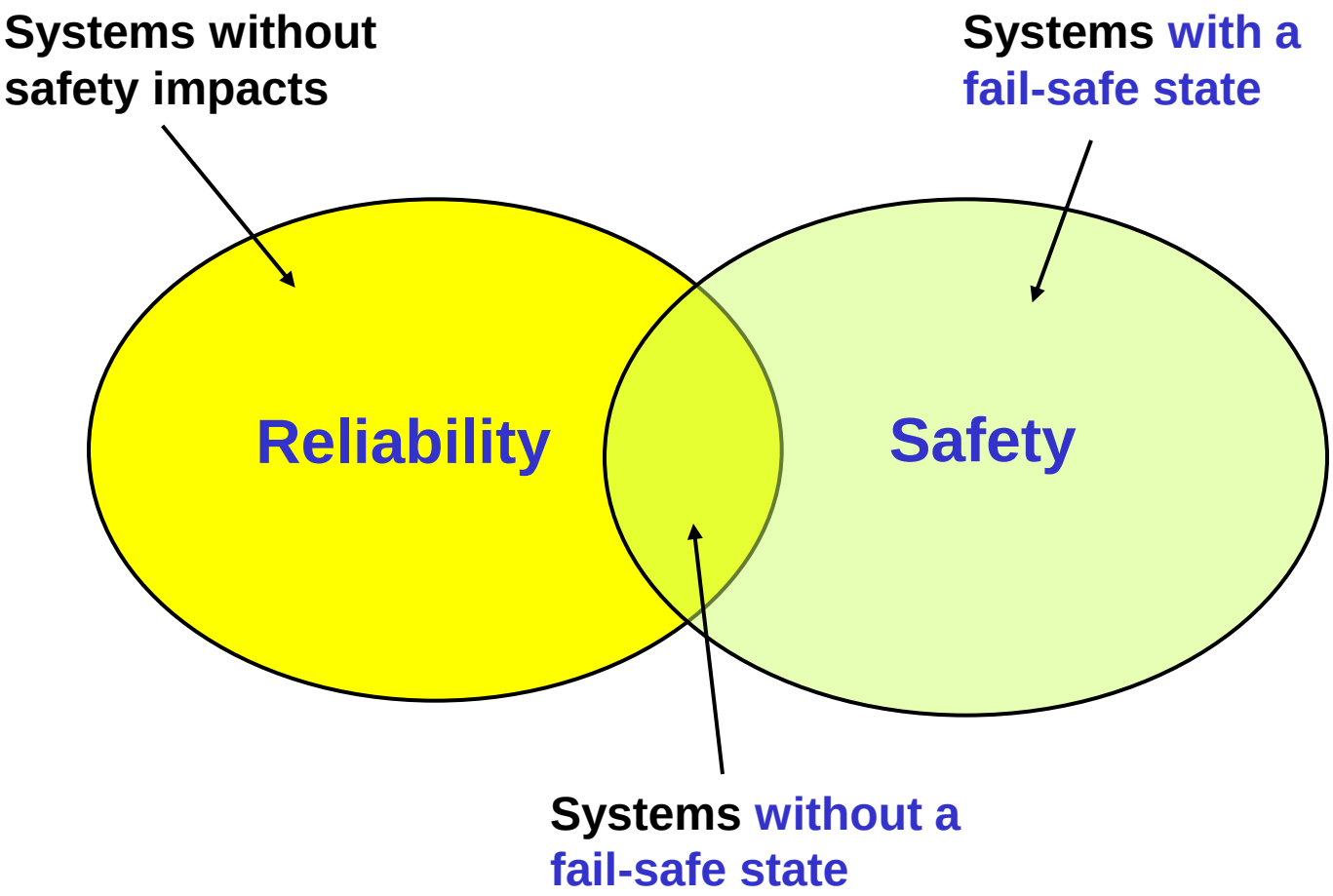
Agenda

- Introduction to safety
- Patterns:
  1. Protected Single Channel Pattern
  2. Homogeneous Redundancy Pattern
  3. Triple Modular Redundancy Pattern
  4. Heterogeneous Redundancy Pattern
  5. Monitor-Actuator Pattern
  6. Sanity Check Pattern
  7. Watchdog Pattern
  8. Safety Executive Pattern

Safety and Reliability

- Safety
  - defined as freedom from accident and losses
- Reliability
  - refers to the probability that a system will continue to function for a specified period of time
- Both requires some kind of redundancy
  - to identify the **dangerous condition or fault**
  - to take **corrective action**

Safety versus Reliability



Safety is a System Issue

- The system is ***either safe or it isn't***
  - not the software, not the electronics, not the mechanics
- It is the interactions of all these elements that determines system safety

Single Point Failures

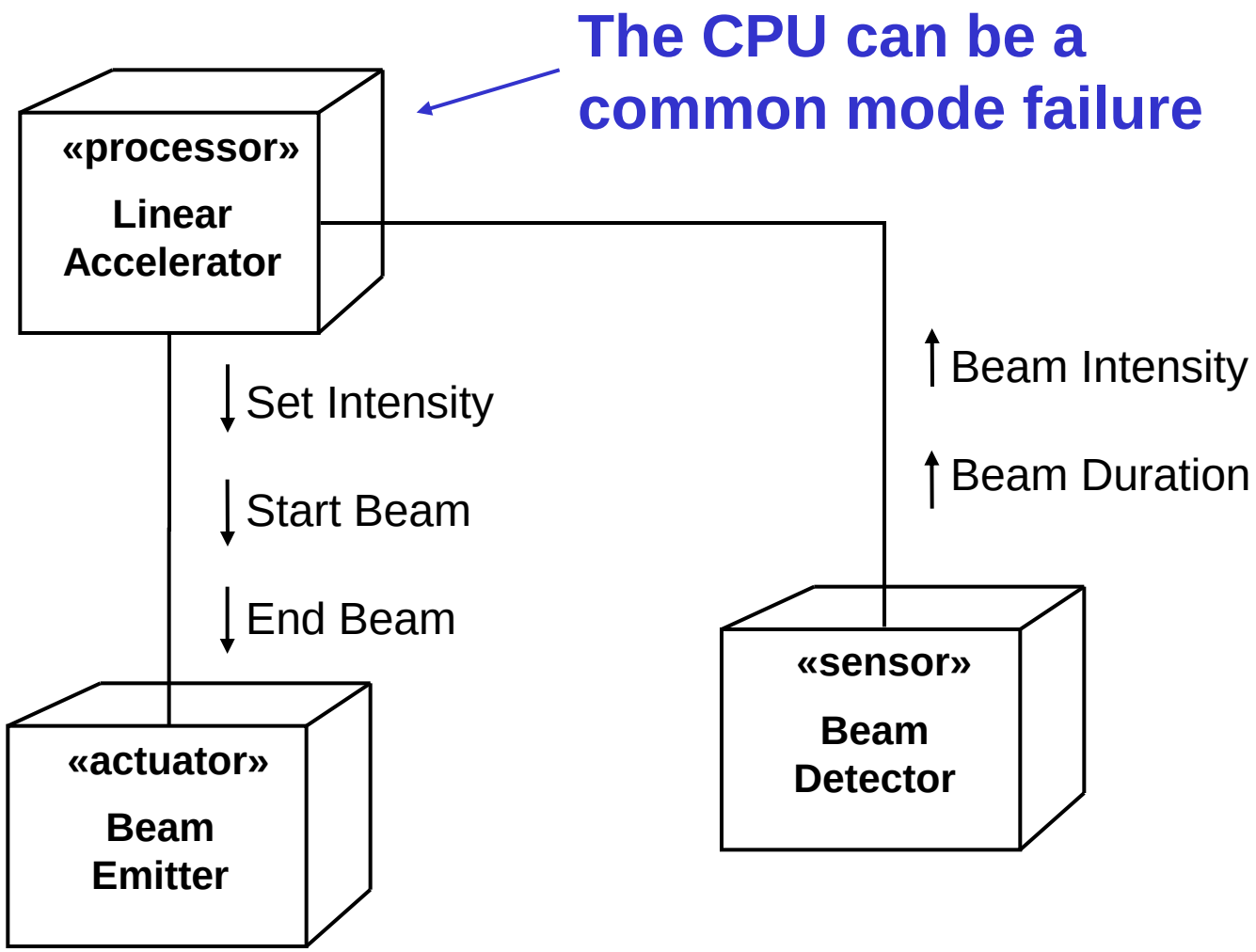
Most experts consider a device **safe**:
only when any single-point failure cannot lead to an incident

Common Mode Failures

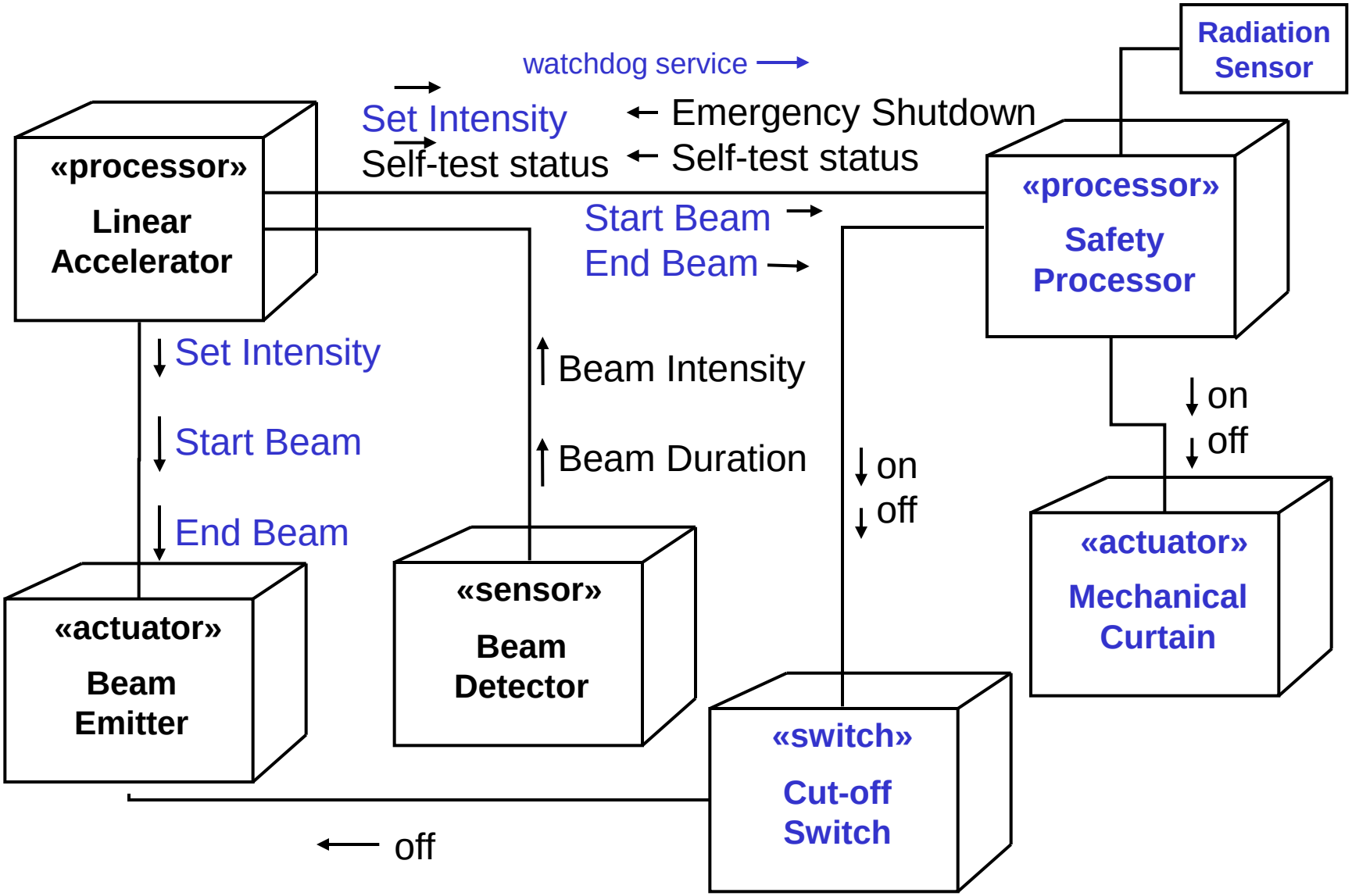
- A ***common mode failure***:
  - is a failure in multiple control paths due to a **common** or **shared fault**

- Example:
  - a cardiac pacemaker with a watchdog circuit controlling a CPU – both driven by the same crystal
    - if the crystal fails e.g. doubling the frequency the heart could be paced by 210 beats per min.

Example: Unsafe Linear Accelerator



Safe Linear Accelerator



Faults and Fail-Safe State

- Faults come in two flavors:
  - **Systematic faults** (errors or design faults)
  - **Random faults** (failures)
- Fail-safe state
  - Many, but not all, safety-critical systems have a condition of existence known to be safe

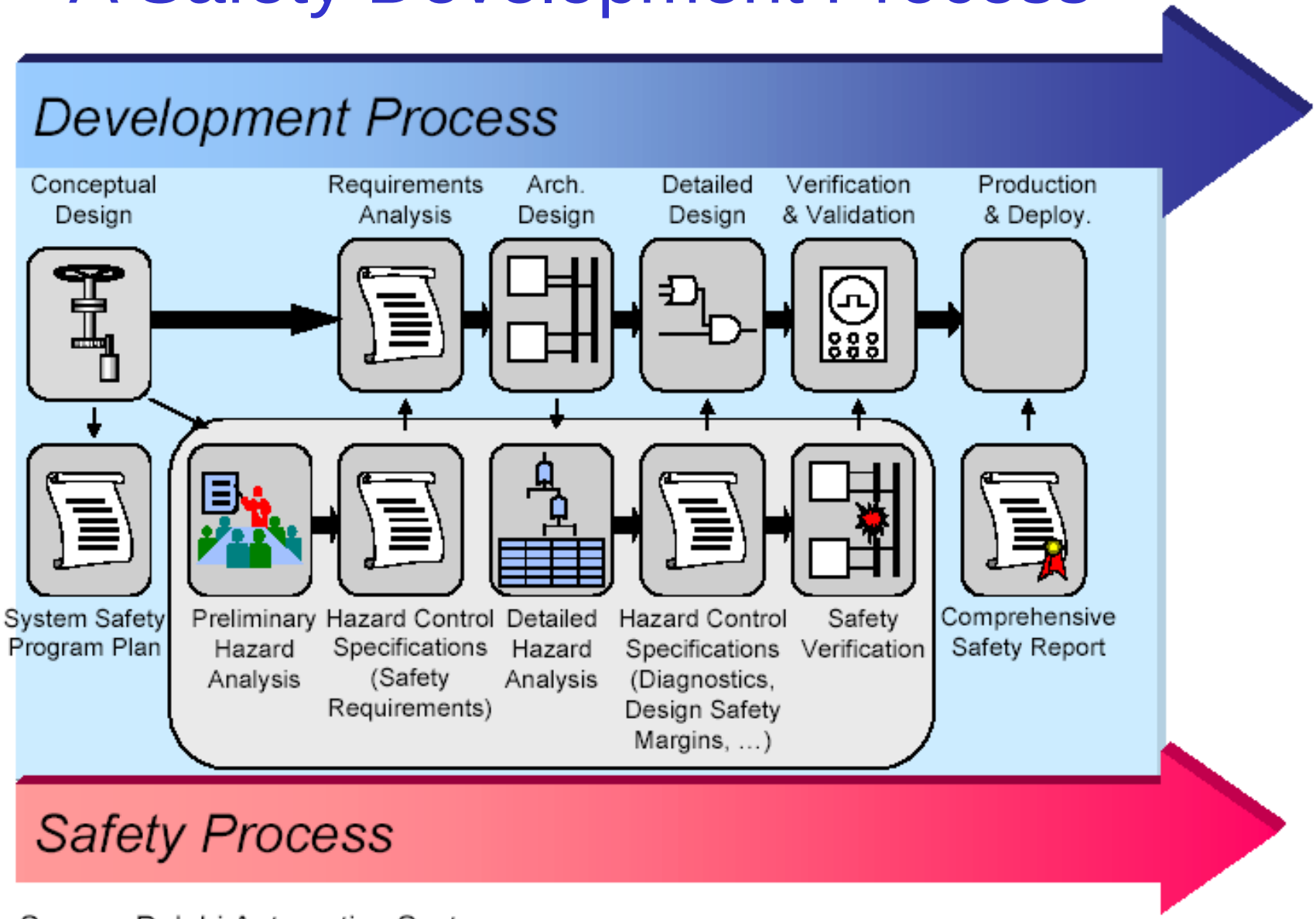
Fail-Safe State

- Different types of safe failure modes:
  - Off state
    - Emergency stop (cutting power)
    - Production stop (finish current task)
    - Protection stop (shuts down immediately)
  - Partial shutdown (degraded functional level)
  - Hold (no functionality)
  - Manual, or external control (via external input)
  - Restart (reboot or restart)

Achieving Safety

- Mechanisms to identify data corruption:
  - Parity
    - simple 1-bit parity identifies single-bit errors
  - Hamming codes
    - multiple parity bits to identify n-bit errors and repair (n-1)-bit errors
  - Checksums
  - Cyclic Redundancy Checks (CRCs)
  - Homogenous multiple storage
  - Complement multiple storage
    - store data in 1’s complement to protect against RAM faults

A Safety Development Process



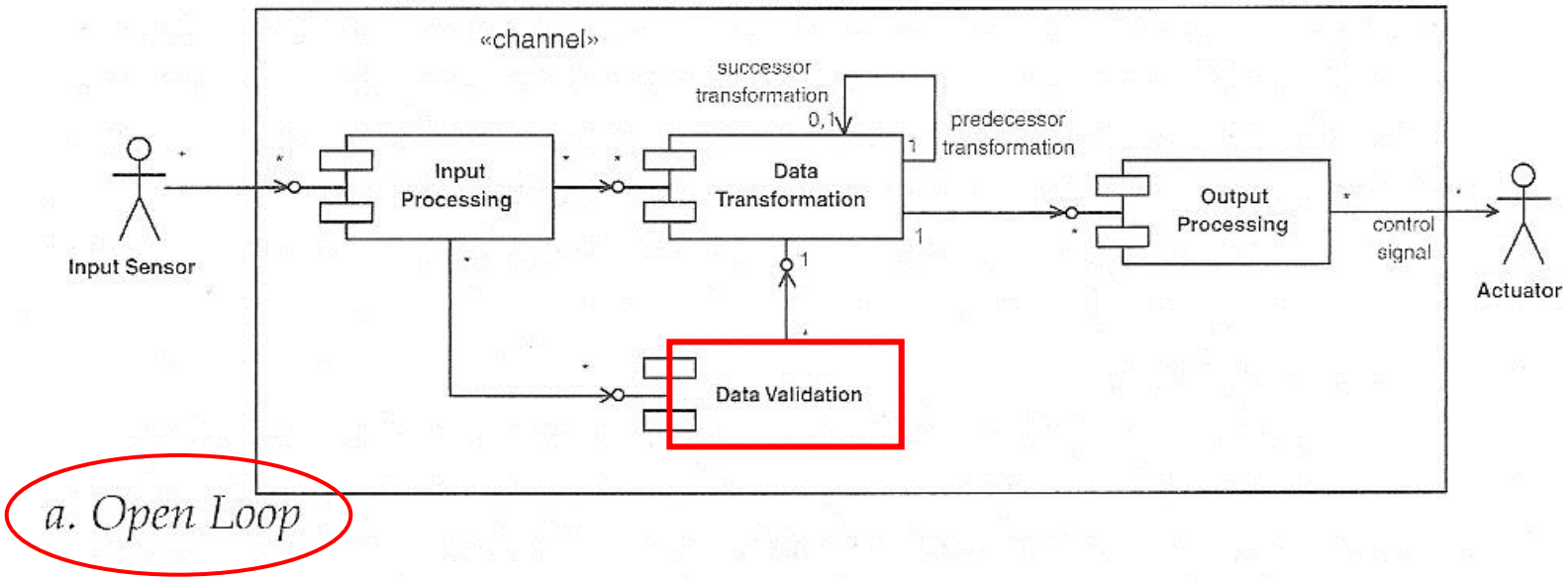
Source: Delphi Automotive Systems

1. Protected Single Channel Pattern

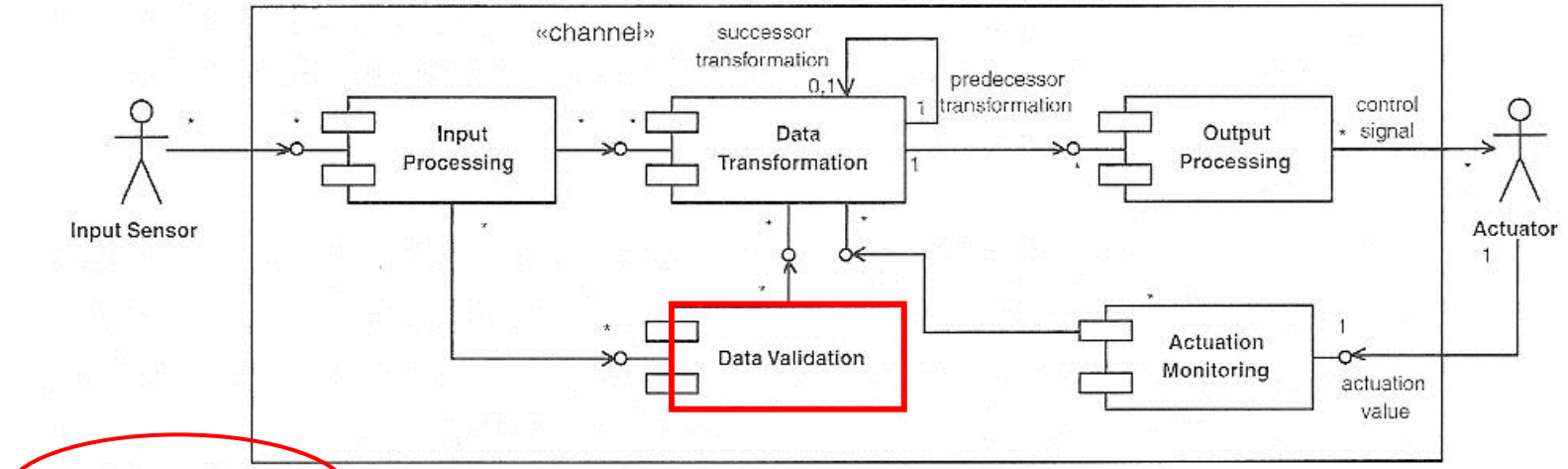
The Protected Single Channel Pattern uses a single channel to handle sensing and actuation.

Will not be able to continue to function in the presence of persistent faults, but it may be able to handle transient faults.

Protected Single Channel Pattern Structure



a. Open Loop



b. Closed Loop

Figure 9-2: *Protected Single Channel Pattern*

Protected Single Channel Pattern Example

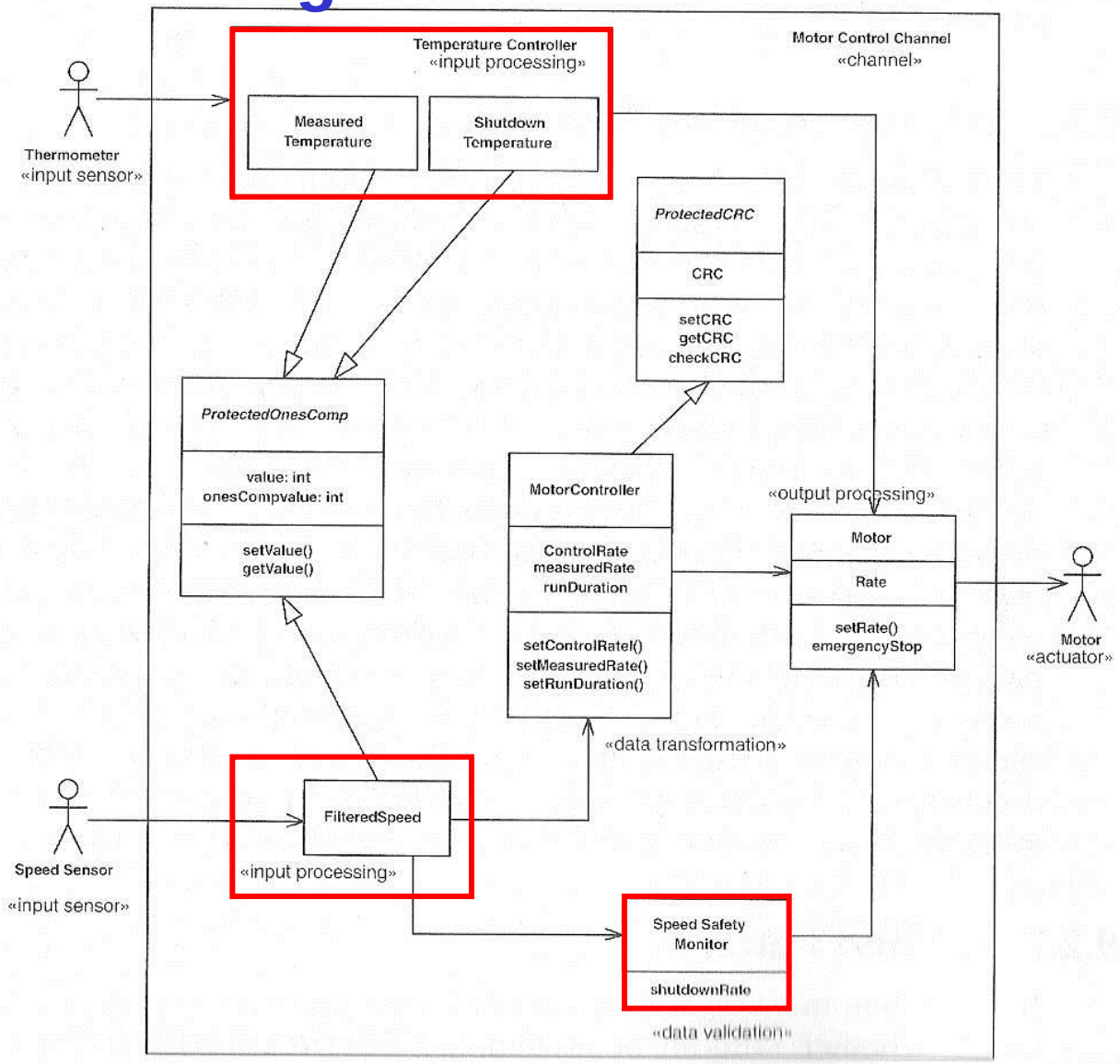


Figure 9-3: *Protected Single Channel Pattern Example*

2. Homogeneous Redundancy Pattern

The Homogeneous Redundancy Pattern uses replicated channels with a switch-to-backup policy in the case of an error.

The pattern improves reliability by addressing random faults (failures). Provides no protection against systematic faults.

Homogeneous Redundancy Pattern Structure

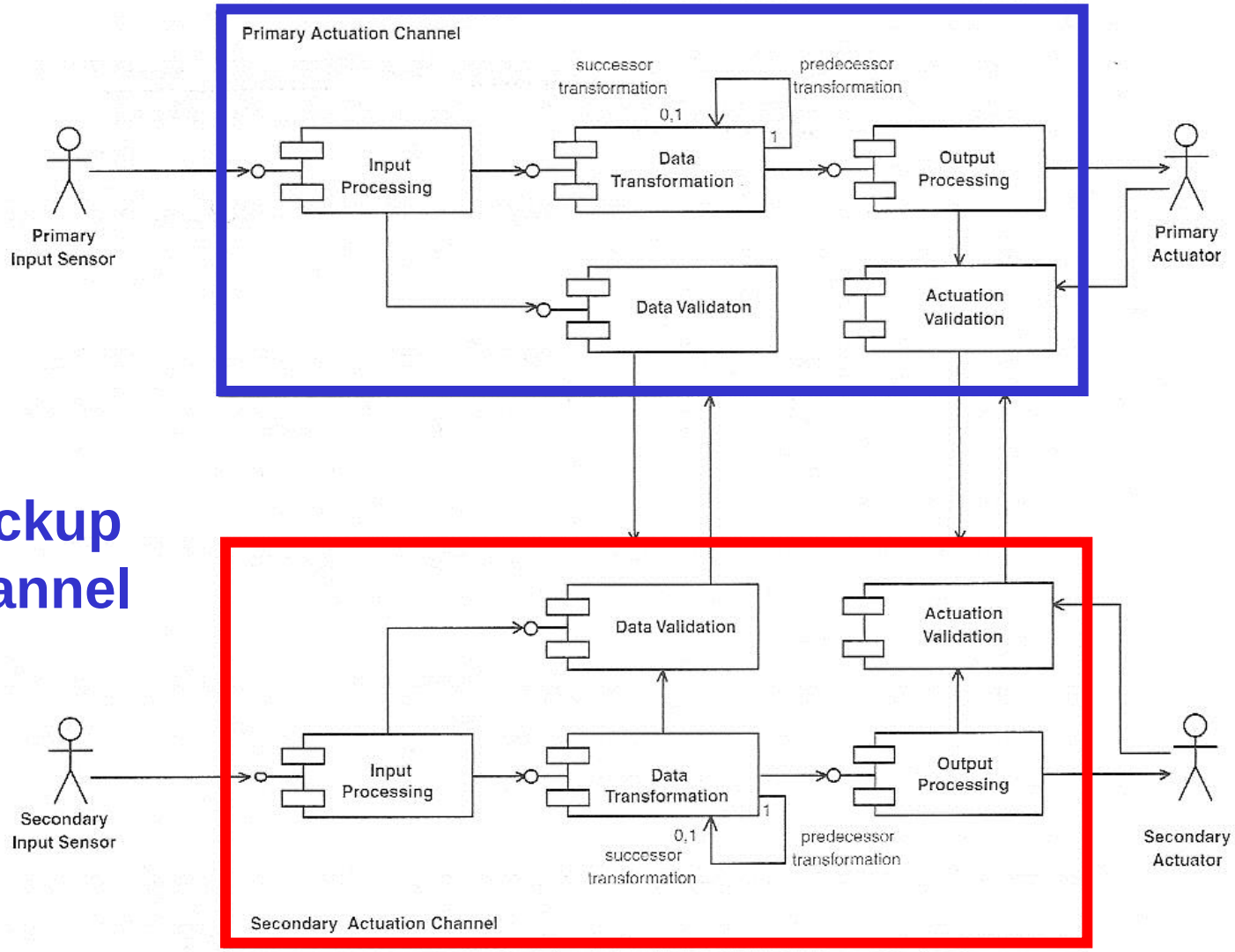


Figure 9-4: *Homogeneous Redundancy Pattern*

Homogeneous Redundancy Pattern Example

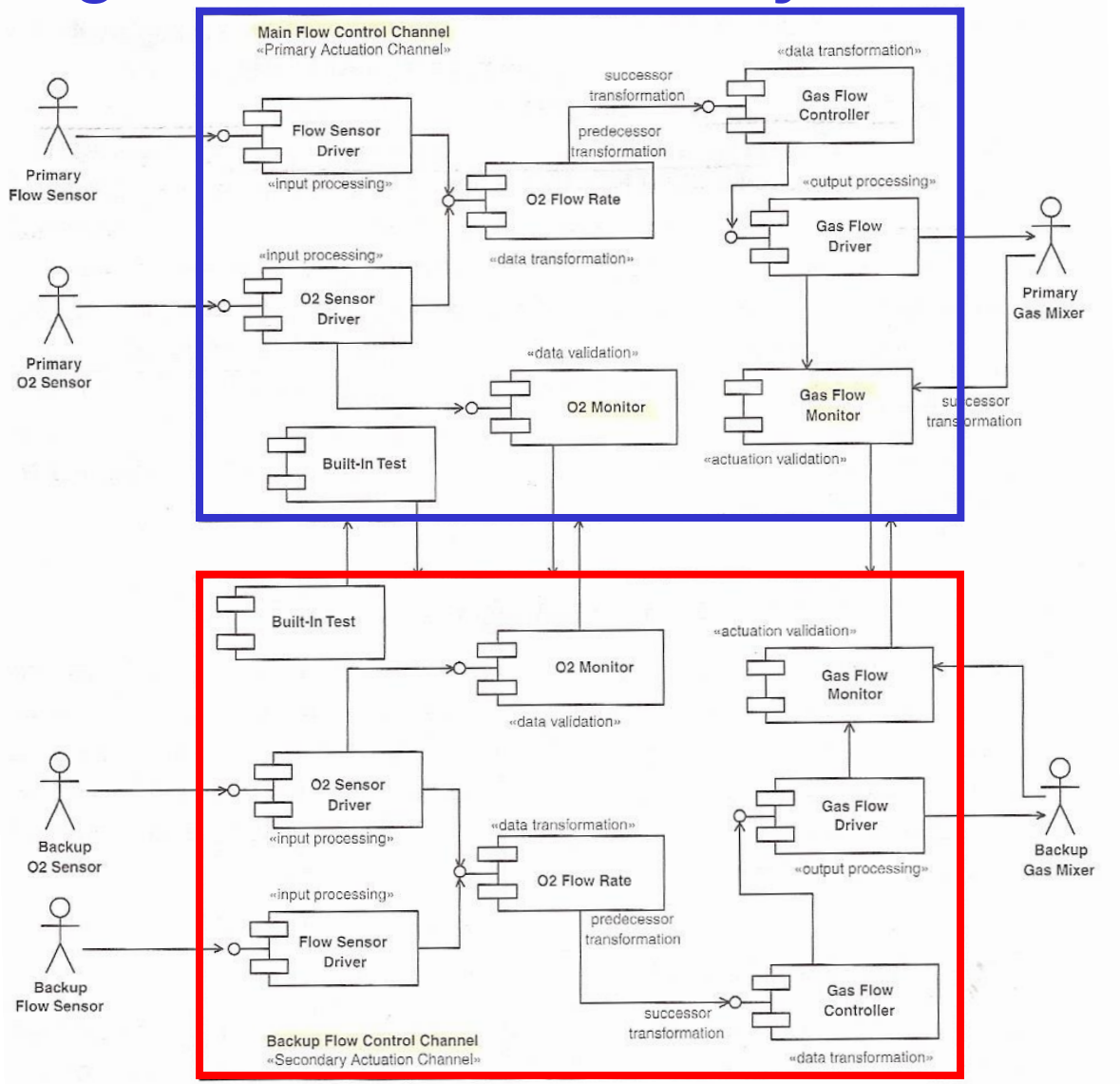


Figure 9-5: *Homogeneous Redundancy Pattern Example*

3. Triple Modular Redundancy Pattern

The Triple Modular Redundancy Pattern operates three channels in parallel used to enhance reliability and safety in situations where there is **no fail-safe state**.

Triple Modular Redundancy Pattern Structure

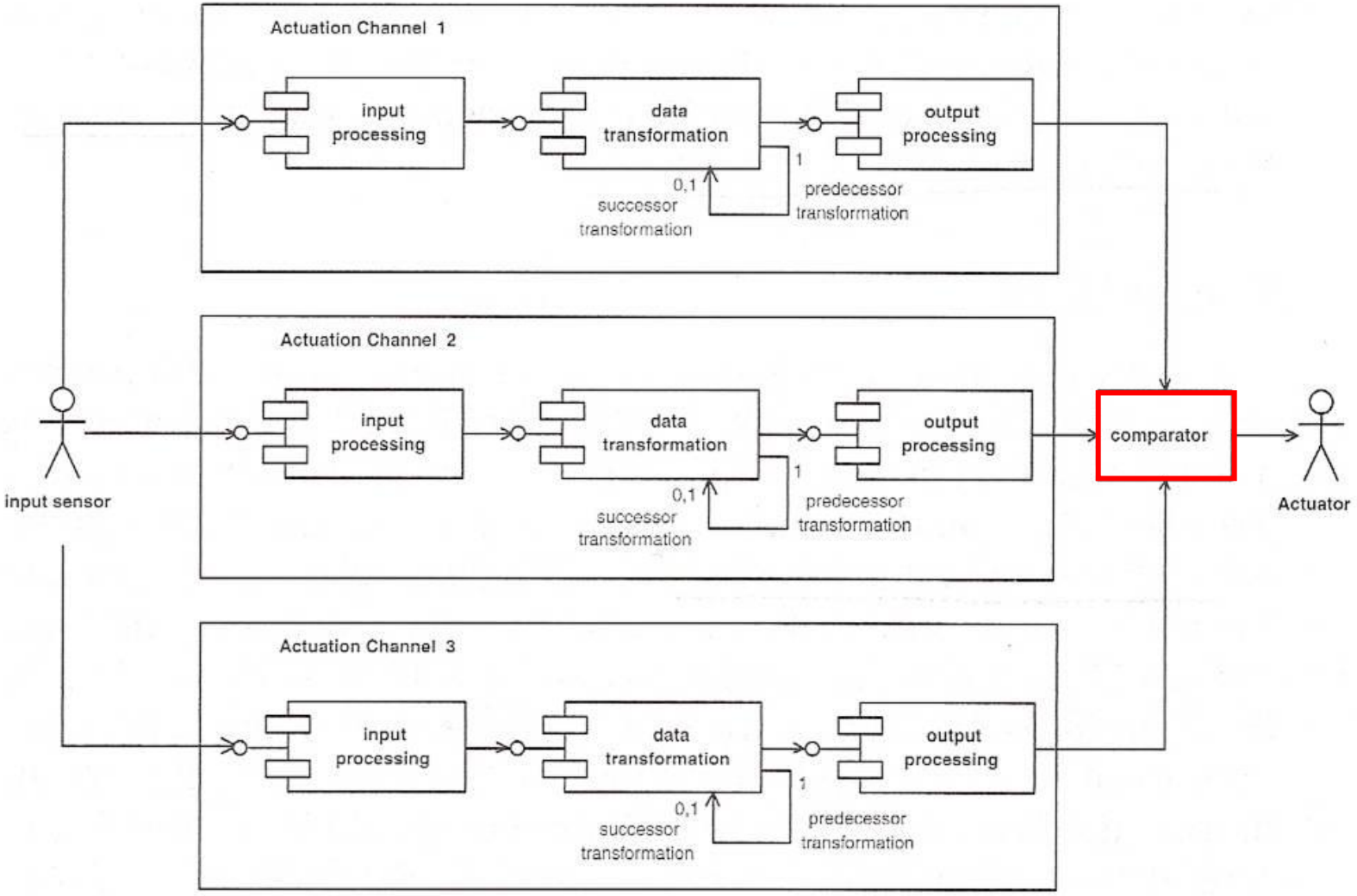


Figure 9-6: *Triple Modular Redundancy Pattern*

Triple Modular Redundancy Pattern Example

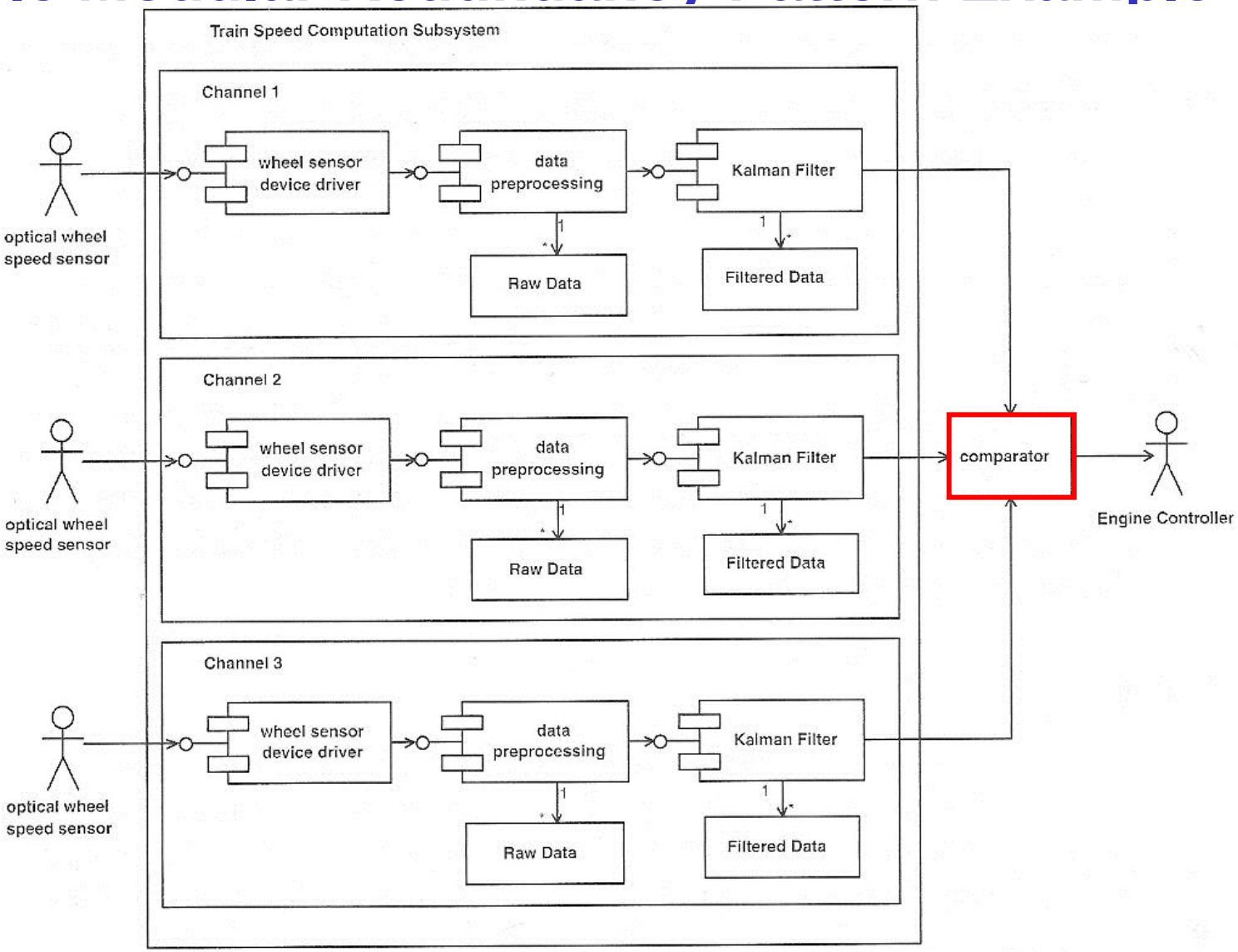
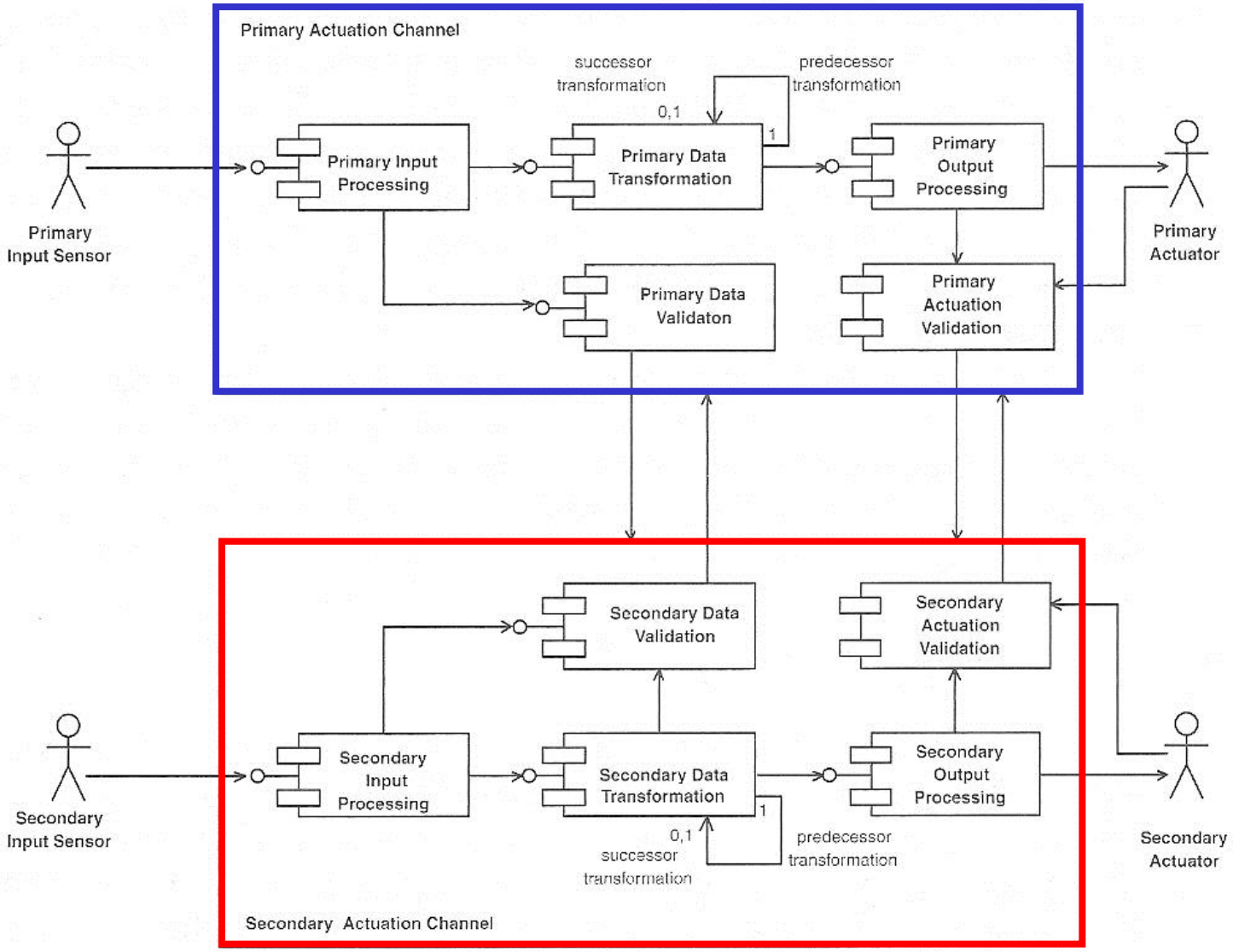


Figure 9-7: *Triple Modular Redundancy Example*

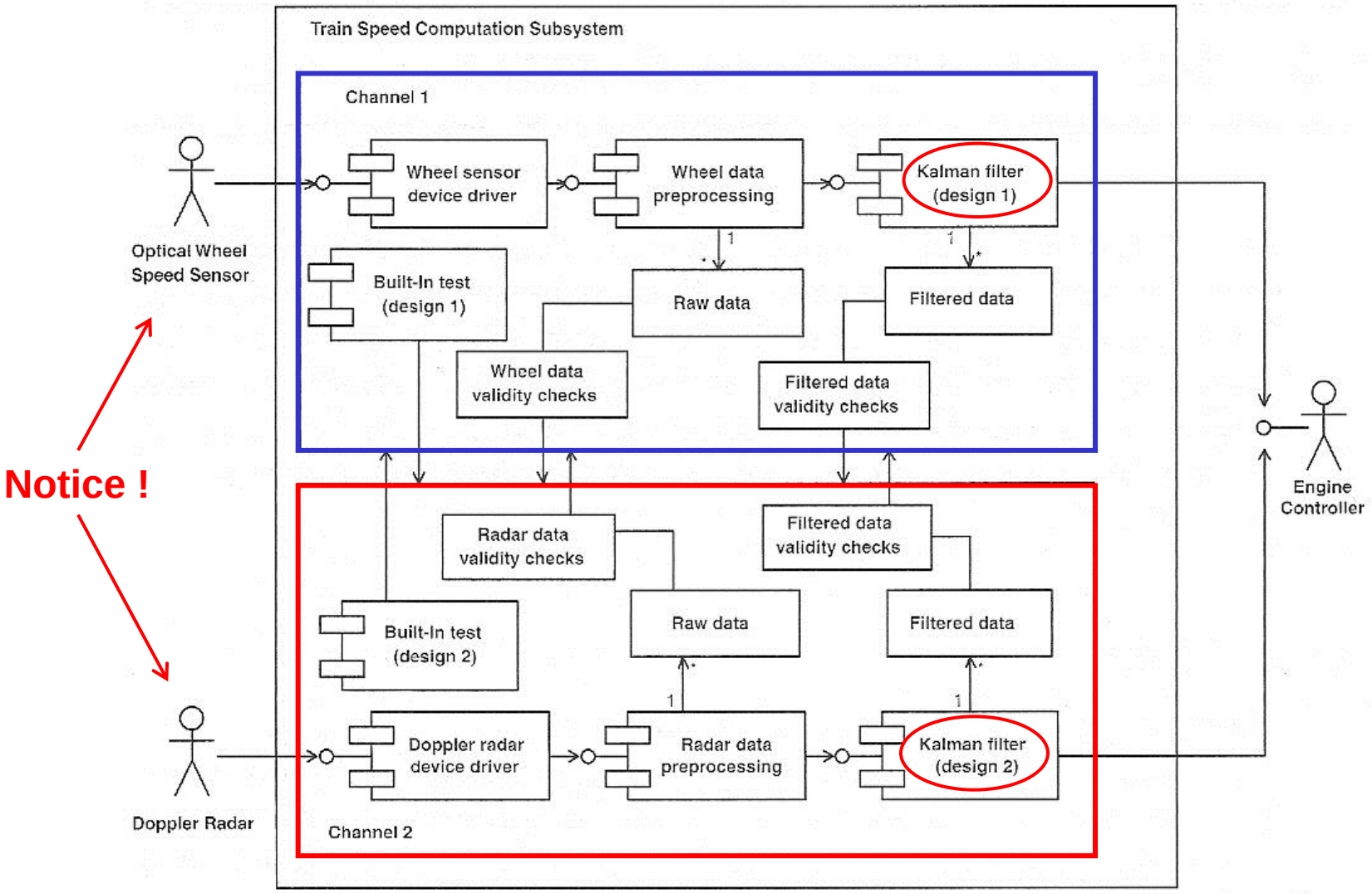
4. Heterogeneous Redundancy Pattern

The Heterogeneous Redundancy Pattern uses multiple channels that have **independent designs and/or implementations**.
Can also detect systematic faults.

Heterogeneous Redundancy Pattern Structure



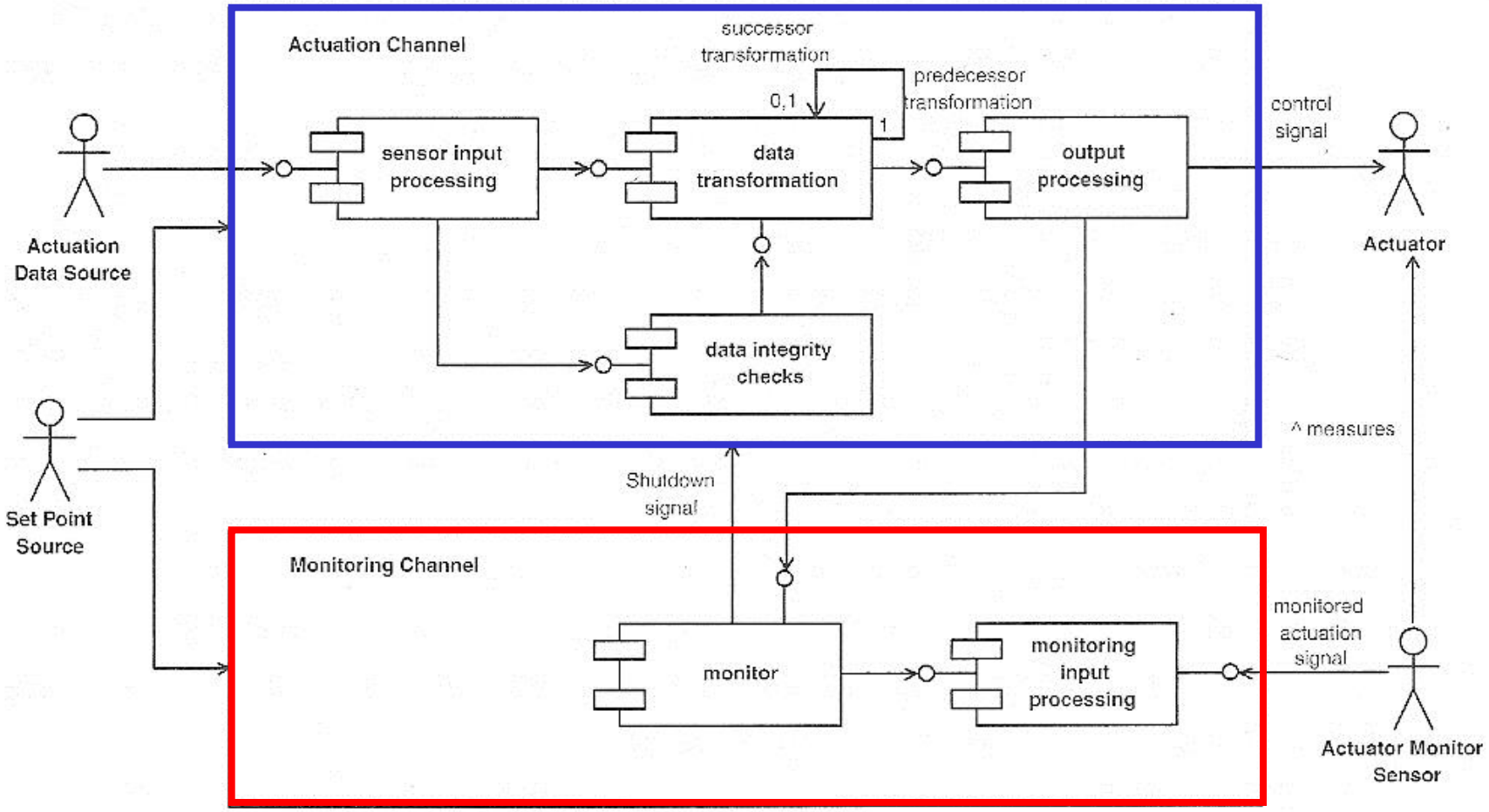
Heterogeneous Redundancy Pattern Example



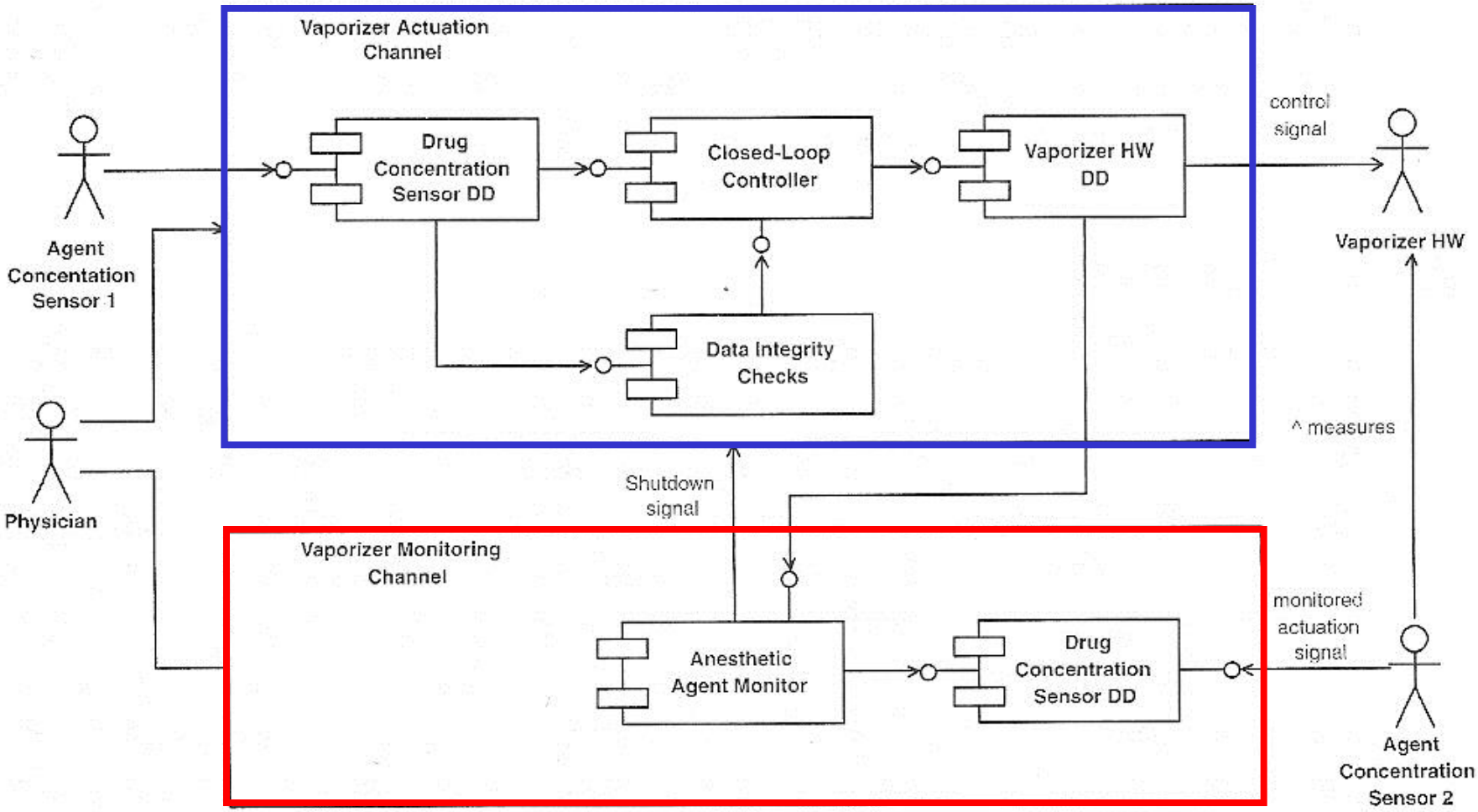
5. Monitor-Actuator Pattern

In the Monitor-Actuator Pattern an **independent sensor** maintains a watch on the actuation channel looking for an indication that the system should be commanded **to its fail-safe state**.

Monitor-Actuator Pattern Structure



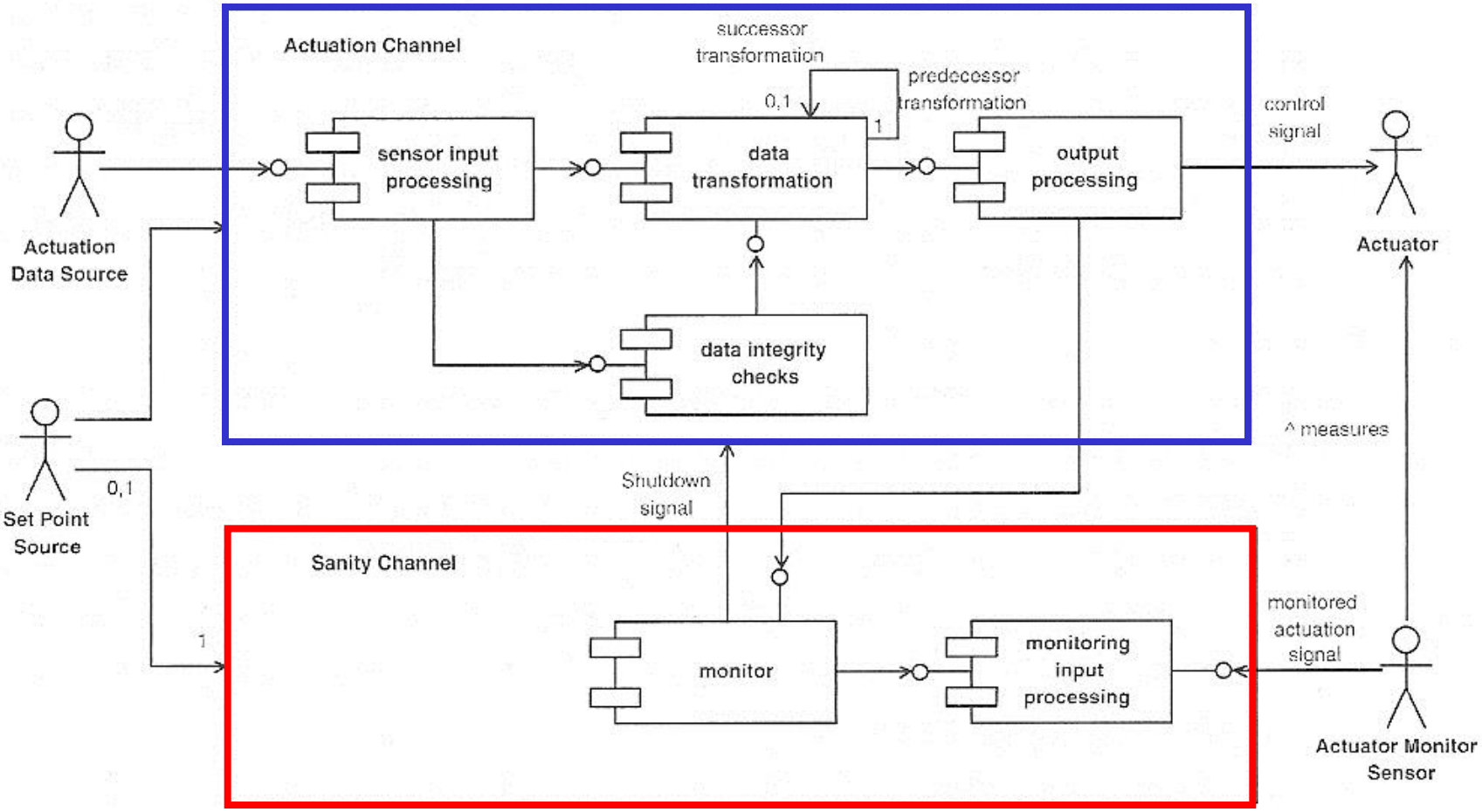
Monitor-Actuator Pattern Example



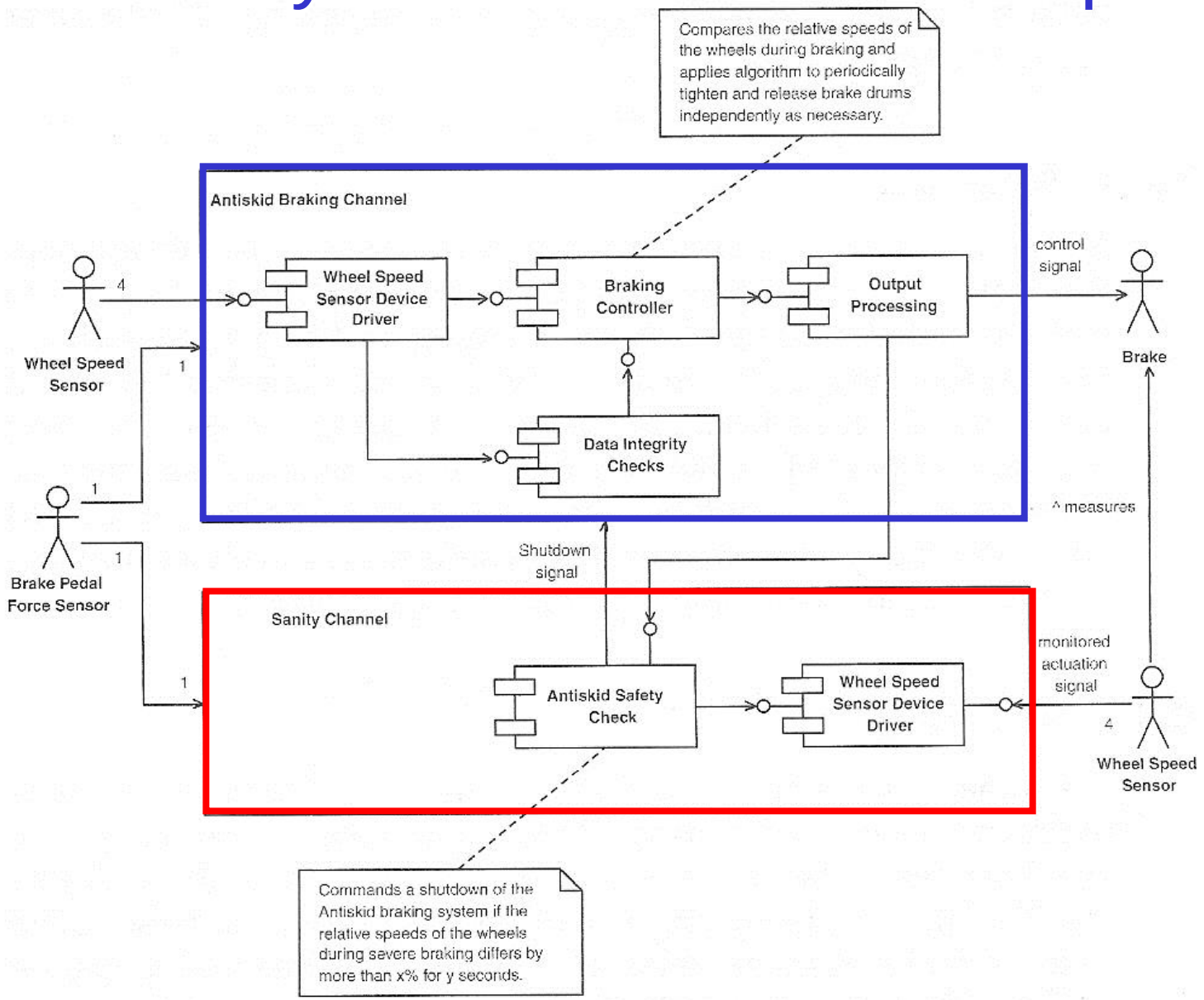
6. Sanity Check Pattern

The Sanity Check Pattern is a variant of the Monitor-actuator pattern.
The pattern exists to ensure that the actuation is approximately correct.

Sanity Check Pattern Structure



Sanity Check Pattern Example



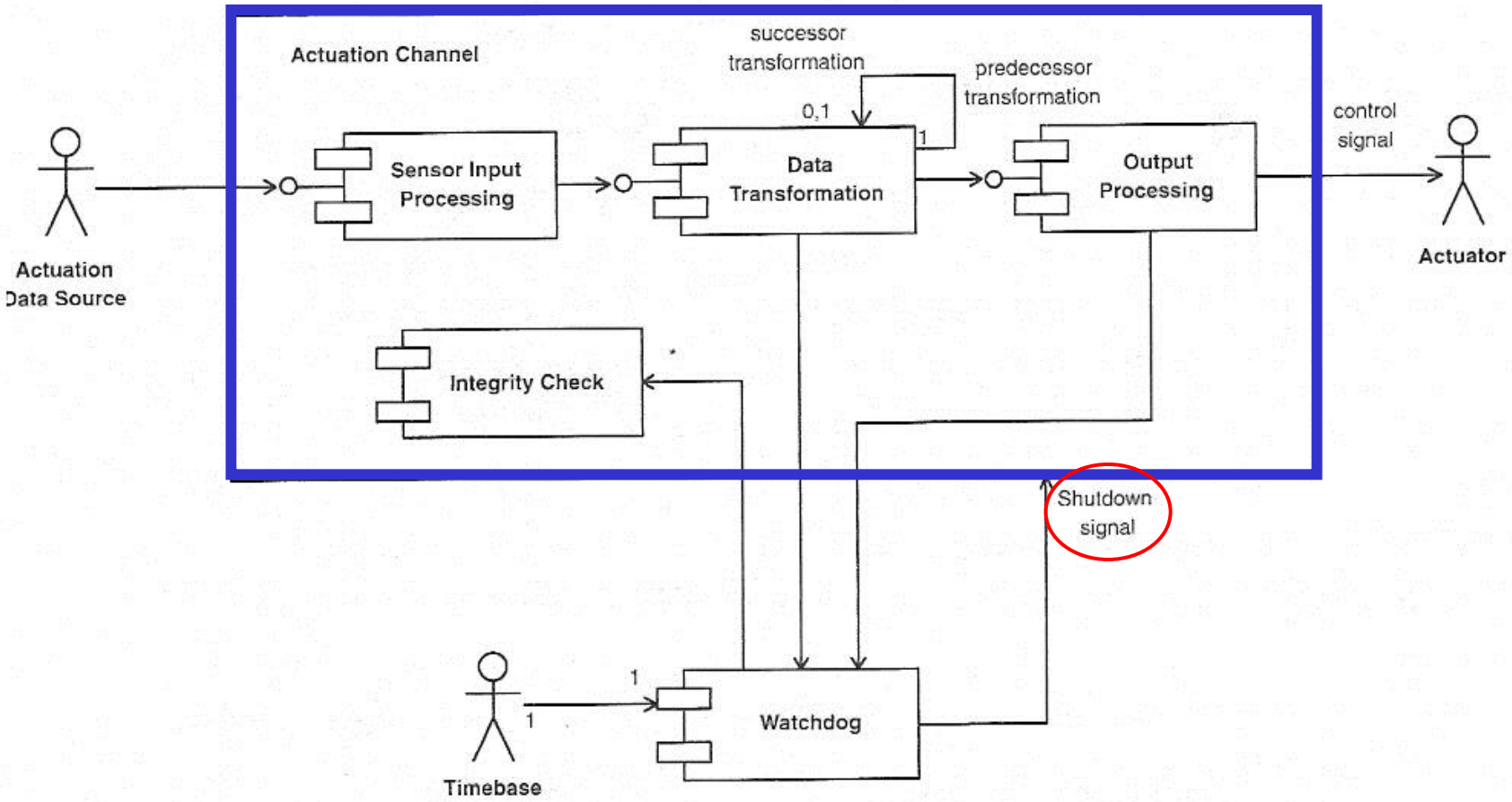
7. Watchdog Pattern

The Watchdog Pattern checks that the internal computational processing is proceeding as expected.

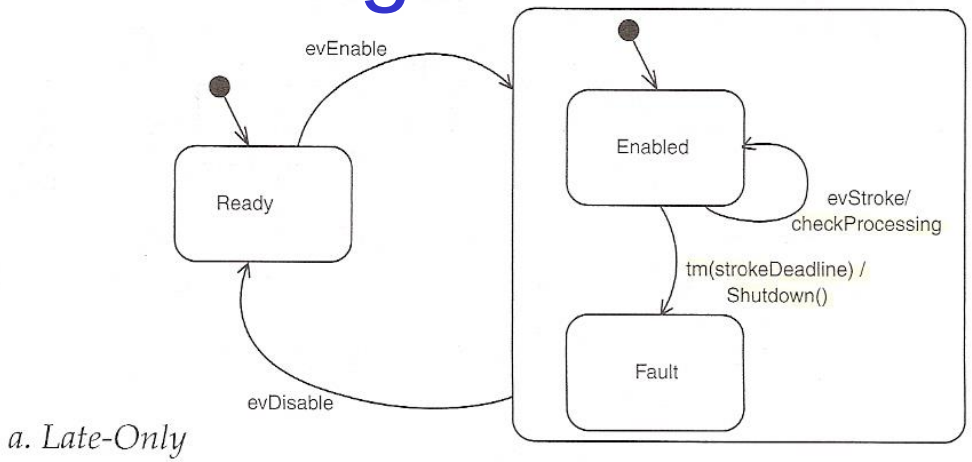
Can detect **timebase faults and deadlocks.**

It may be combined with any other safety patterns in this chapter.

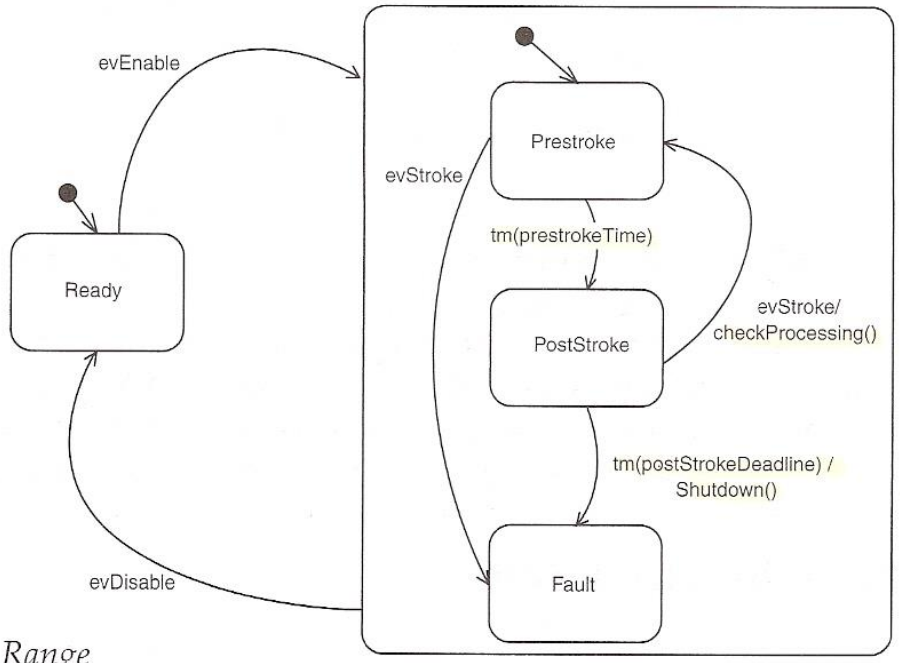
Watchdog Pattern Structure



Watchdog Pattern State Machine

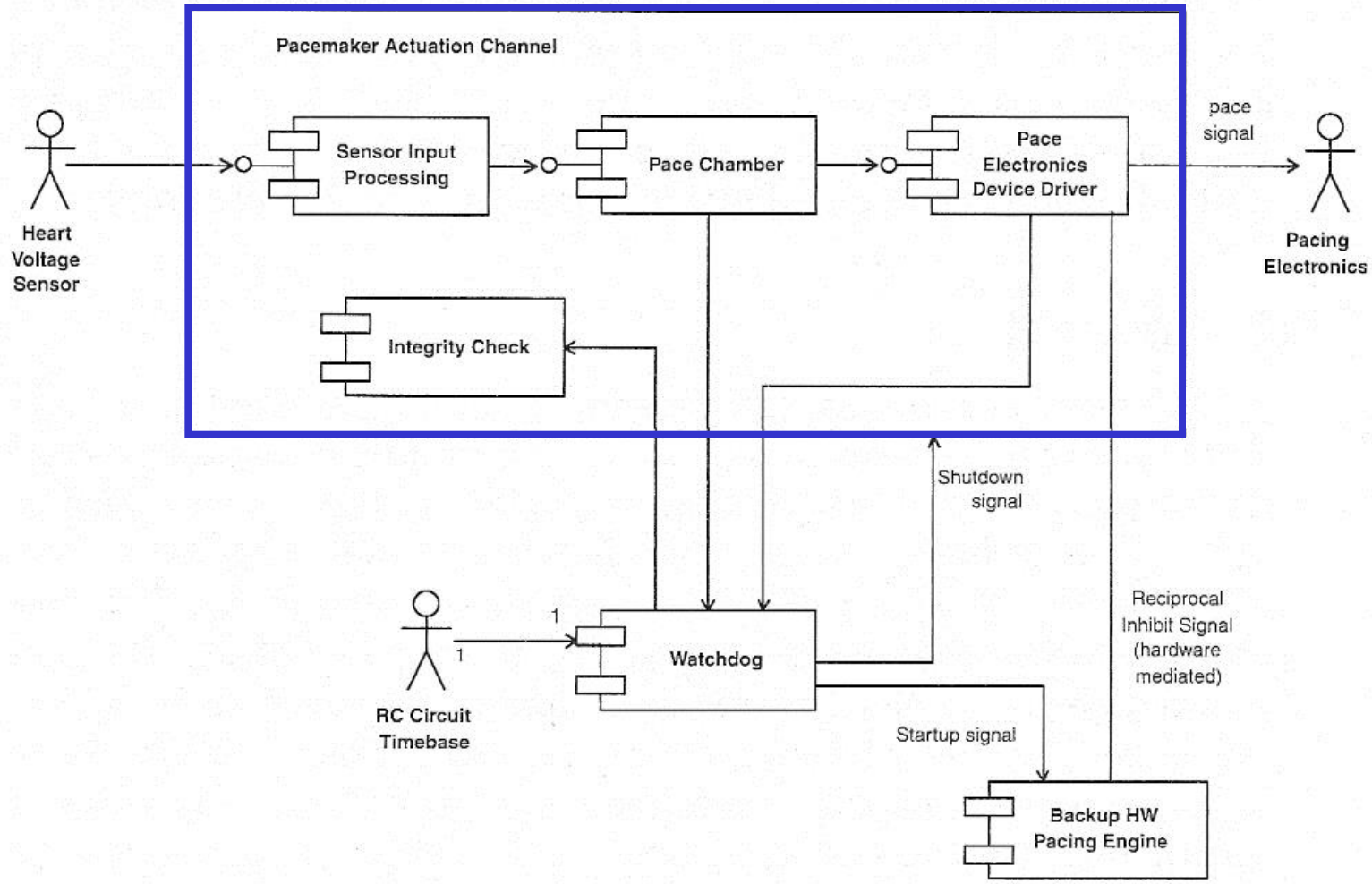


a. Late-Only



b. Time Range

Watchdog Pattern Example



8. Safety Executive Pattern

The Safety Executive Pattern provides a safety executive to oversee the **coordination of potentially multiple channels** when safety measures must be actively applied.

Safety Executive Pattern Structure

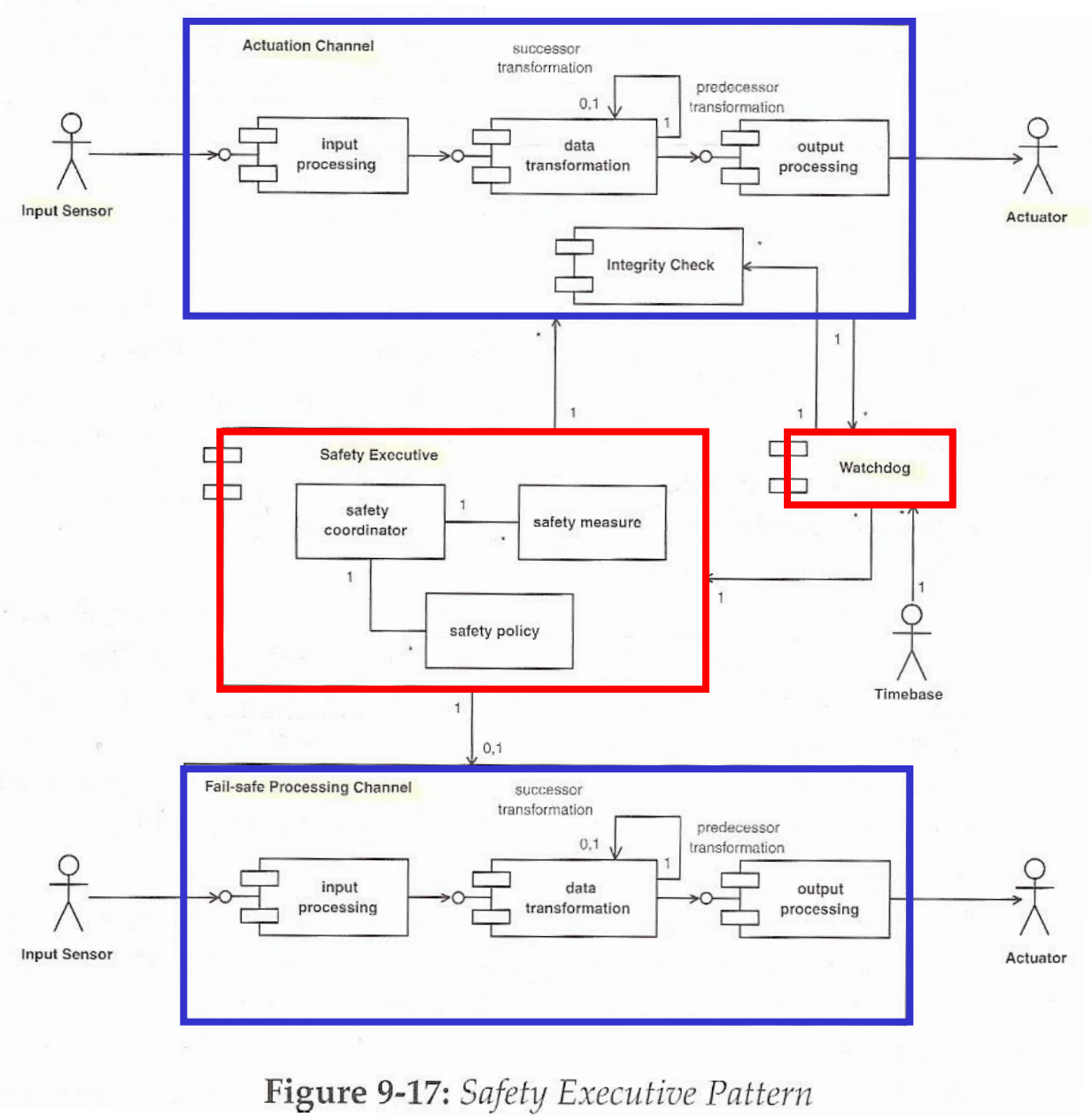


Figure 9-17: *Safety Executive Pattern*

Safety Executive Pattern Example

The example includes:

- **Watchdog pattern**
- **Monitor Actuator pattern**
- **Safety Executive pattern**

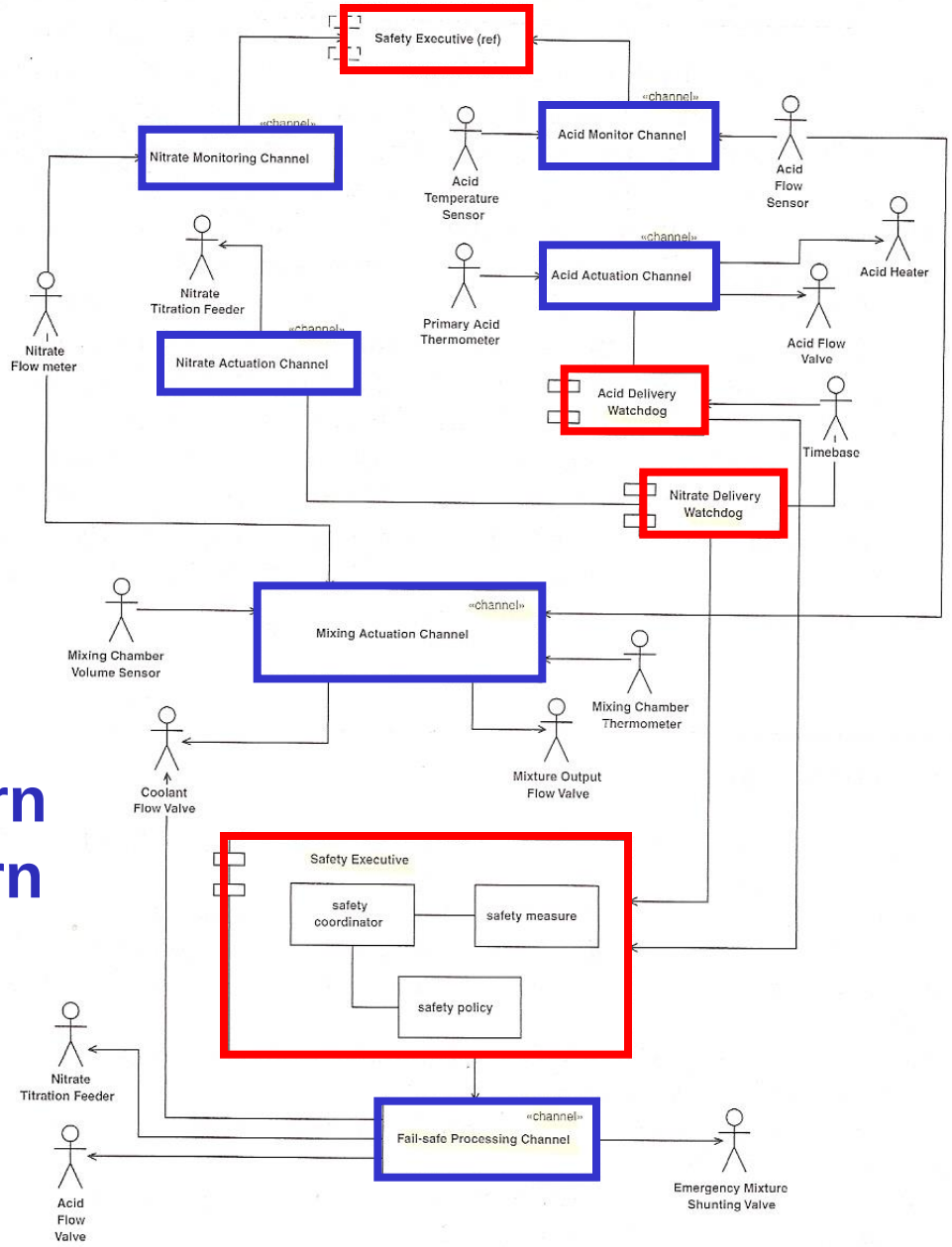


Figure 9-18: *Safety Executive Pattern Example*

Summary

Safety is a system architecture/design issue

1. Protected Single Channel Pattern
2. Homogeneous Redundancy Pattern
3. Triple Modular Redundancy Pattern
4. Heterogeneous Redundancy Pattern
5. Monitor-Actuator Pattern
6. Sanity Check Pattern
7. Watchdog Pattern
8. Safety Executive Pattern