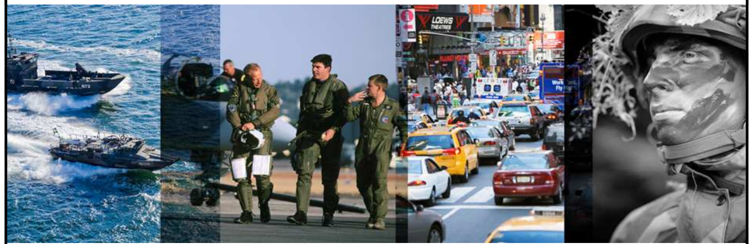
SAAB

SAAB AEROSYSTEMS

Dependable Aircraft Systems



Lars Holmlund
October 12, 2009
Chalmers University

70 years of experience

SAAB

Gripen in South Africa

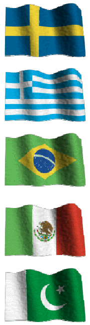
SAAB

Gripen Next Generation

SAAB

ERIEYE™ Airborne Early Warning & Control

Improved Surveillance Capability



Originally designed for the Swedish Air Force and now also in operation in; Brazil, Greece, Mexico,Pakistan

SAAB

Unmanned Aerial Vehicles

Ongoing projects

SKELDAR

NEURON

(www.youtube.com/saabgroup)

SAAB

Dependable Products

Gripen accident outside Karlskrona

SAAB

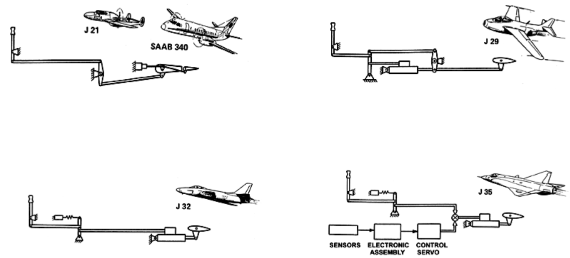
SAAB

Scope

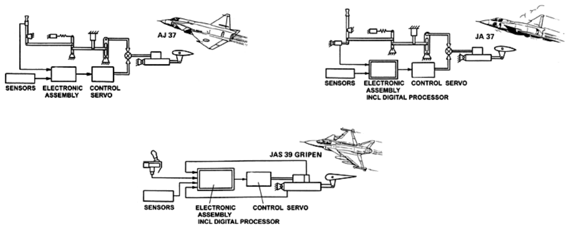
A retrospective of flight control system evolution

The Gripen Flight Control System
- Requirements
- Design decisions
- Principle of operation
- The philosophy behind redundancy - monitoring – fault accommodation
- System- and computer architecture

The Evolution of FCS 1945-1990



The Evolution of FCS 1945-1990

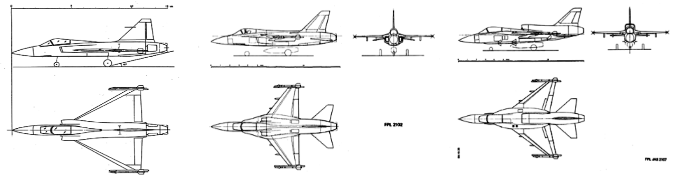


Design Drivers

- Performance
  E.g.: range, speed, altitude, acceleration, turn ratio
- Function
  operative, pilot relief functions
- Safety/Availability
  Prob. for loss of a/c , pilot survivability, "graceful degradation"
- Weight/ Volume
- Environmental
  Temp., mech., electrical (EME, EMI,) EMP
- Maintenance and Testability

Design Decision

• Different a/c configurations were suggested



Design Decision

Decision to choose an a/c with :

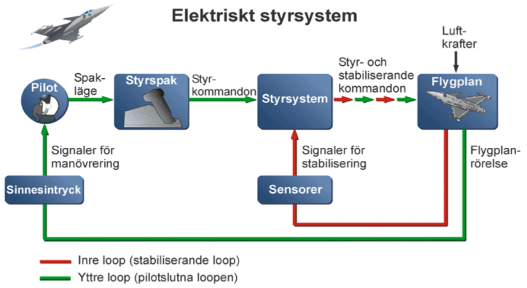
Relaxed stability in pitch, 7 primary control surfaces
- turn ratio, better weight/volume ratio

Electric control system
- eliminates mechanical linkage and equipment
- simplified installation and maintenance, less vulnerable

Computerized flight control system
- flexibility during development and design, good growth potential (40 years)

Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB

The Gripen flight control system’s control loops



Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB

Design Decisions

Pros :
- Light and “small” system
- Advanced control law calculations
  - Automatic stability in pitch
  - Optimized control and stability characteristics
  - Gust alleviation
  - Maneuvering load limits
  - Outer loop functions
- Simplified and improved maintenance and test

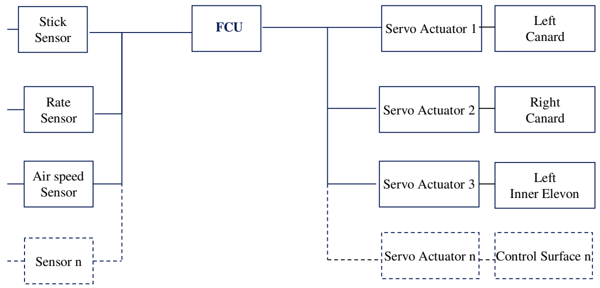
Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB

Design Decisions

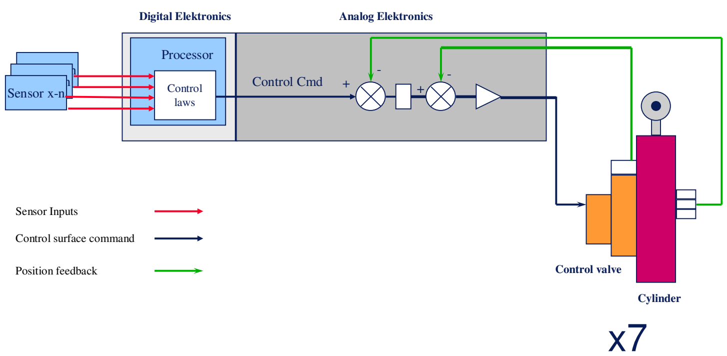
Cons:
- Requires a reliable power supply
- Needs precautions when handling:
  - EME and EMI
  - Cosmic and nuclear radiation
- Extensive qualification/verification

Fault Tolerance

A simplex system will meet functional and performance requirements



Concept of redundancy, simplex system



Fault Tolerance

Other requirements affect the design of the system, e.g. safety req. :

No single failures may cause loss of a/c
Maximum allowed probability for loss of a/c
Maximum allowed A/C transients as a result of a fault in the system

Probability for mission success

Fault Tolerance

Fault tolerance in the Gripen FCS is built up by:

- Redundancies
- Voting planes
- Monitoring
- Redundancy Management
- Asynchronous operating FCU
- Pre flight test

The Philosophy Behind The Redundancy Concept

- Good flying qualities with 6 out of 7 primary control surfaces operating
- Maneuverable with 5 out of 7 primary control surfaces operating
- Able to cope with all single faults and most double faults
- QUAD vs TRIPLEX
  - Economical system – slim as far as resources are concerned
  - Brain power instead of muscles
- Safety critical function must be tripled
- Important functions are doubled, "tie break"

Redundancies within the system

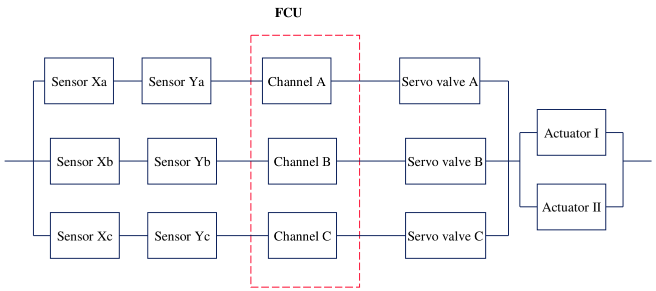
- Example of tripled functions (lack fail-safe position)
  - Three channel FCU
    - Independent BU-mode (HW/SW)
  - Control stick sensors
  - Rate gyro
  - Electrical power supply

Redundancies within the system

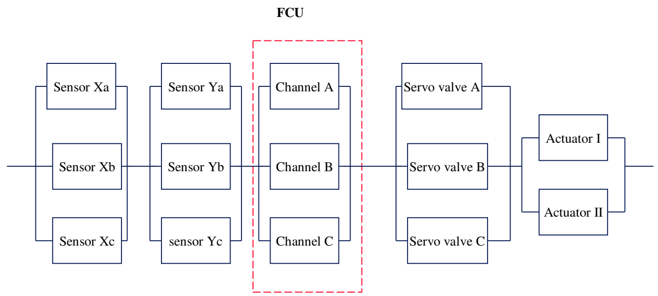
- Example of doubled functions (have a "fail-safe" position*)
  - Accelerometers
  - Angle of attack sensors
  - Air data (speed and altitude)
  - Hydraulic power supply

* as long as we can detect a fault

General simplified architecture



General simplified architecture II



Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB
SAAB

Fault Tolerance

Fault tolerance is built up by:

- Redundancies
- Voting planes
- Monitoring
- Redundancy Management
- Asynchronous operating FCU
- Pre flight test

Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB
SAAB

Voting planes

MLV – Mid Level Voting

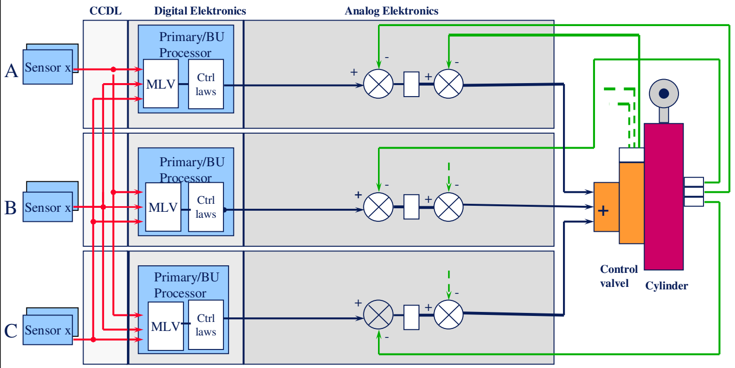
Input signal voting (S/W)

Voting of computed control signals (H/W)

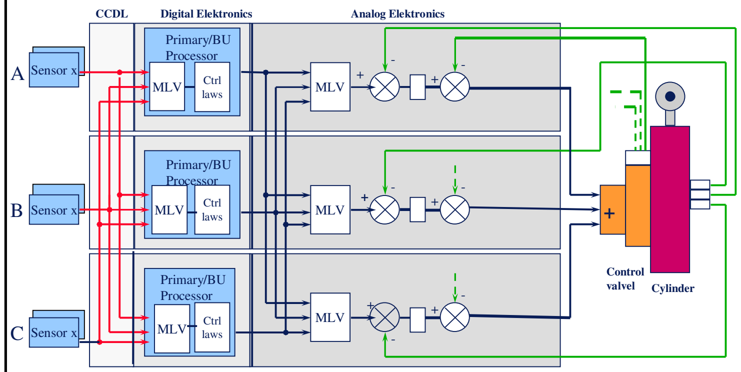
”Flux summing” (H/W)

Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB
SAAB

Concept of redundancy, triplex EFCS



Concept of redundancy, triplex EFCS



Fault Tolerance

Fault tolerance is built up by:

- Redundancies
- Voting planes
- Monitoring
- Redundancy Management
- Asynchronous operating FCU
- Pre flight test

Functional Monitoring and Redundancy Management

- Extensive functional monitoring and redundancy management compensates for lack of redundancy
- Functional monitoring detects the fault and informs the A/C system and pilot about the fault.
- Redundancy management allows for reconfigurations, graceful degradation and high survivability

Functional Monitoring

- Methodology
  - Cross channel monitoring
  - In line monitoring
  - Direct monitoring
  - Reasonableness monitoring
- Self healing
  - Minimizes the effect of nuisance trips
  - Creates resilience within the system

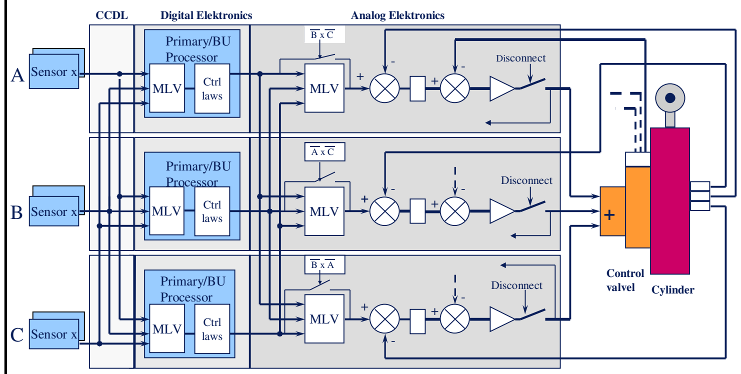
Redundancy Management

- Reconfiguration helps minimizing the possible effect of a fault
  - Selects and removes the faulty signal. Continues operation with the remaining ones or substitutes the faulty signal with another similar signal
- Reconfiguration can also compensate for lack of resources
  - Control surfaces, fail-safe values, model based signals

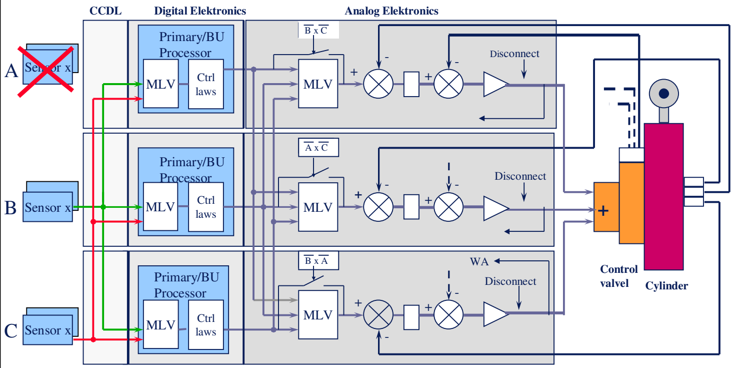
Redundancy Management

- Example of reconfigurations:
  - Sensor faults, i.e:
    - oRate gyro
    - oAngle of attack
    - oAngle of side slip
    - oAccelerometer
  - Data bus faults
  - Servo actuator faults
  - Computer faults

Concept of redundancy, triplex EFCS

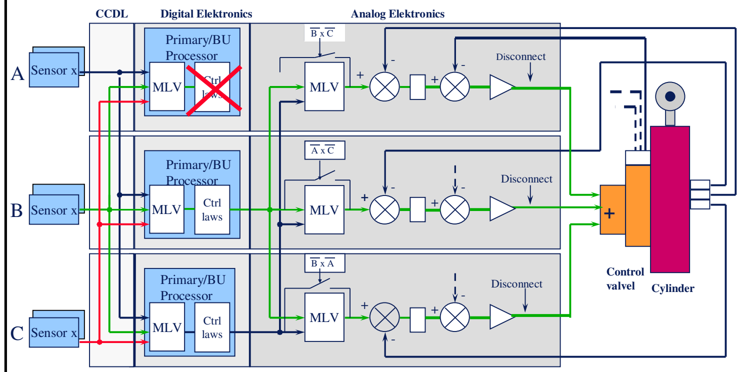


Concept of redundancy, Sensor fault



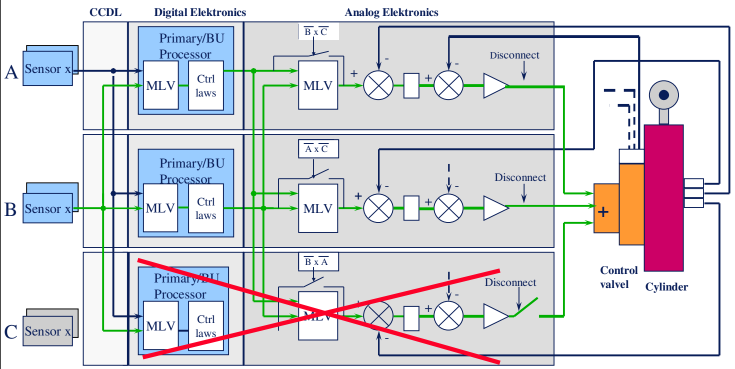
Lars Holmlund Saab Aerosystems
2009-10-12

Concept of redundancy, Processor fault



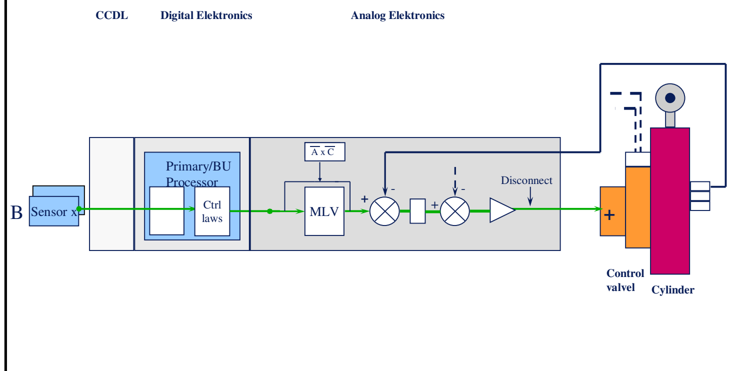
Lars Holmlund Saab Aerosystems
2009-10-12

Concept of redundancy, loss of channel



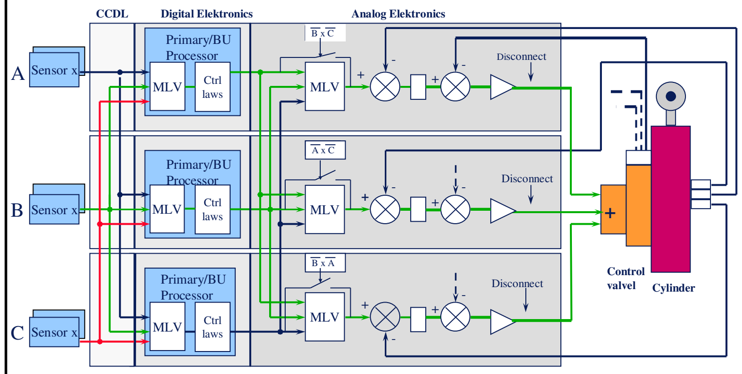
Lars Holmlund Saab Aerosystems
2009-10-12

Concept of redundancy, loss of two channels



Lars Holmlund Saab Aerosystems
2009-10-12

Concept of redundancy, output monitoring



Output monitoring

SAAB

Fault Tolerance

Fault tolerance is built up by:

- Redundancies
- Voting planes
- Monitoring
- Redundancy Management
- Asynchronous operating FCU
- Pre flight test

SAAB

Fault Tolerance

Fault tolerance is built up by:

- Redundancies
- Voting planes
- Monitoring
- Redundancy Management
- Asynchronous operating FCU
- Pre flight test

SAAB

Fault Tolerance

- Extensive pre-flight test guarantees safe function of flight critical functions, redundancies and monitoring circuits

SAAB

Summary: The Gripen FCS - A Hybrid System

Static Redundancy
- Basically a triplex system – but not a fully TMR system
- MLV- used to isolate faults
- Asynchronous System

Dynamic Redundancy
- Fault Detection – Application specific due to an asynchronous system
- Reconfiguration (Graceful Degradation)
- S/W redundancy – but not a real N-version programming
- Warm standby system for processor and S/W faults

Byzantine faults
- The system is not sensitive to single Byzantine faults– due to three independent asynchronous channels + MLV

SAABGROUP.COM

Lars.Holmlund@saabgroup.com

System Safety Work

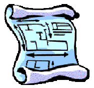
Processes – Methodology
Random and Systematic Faults
Fault Injection

System Safety Work

MIL-STD-882C

http://stinet.dtic.mil/str/dodiss4_fields.html, search for the above

- **Random failure.** Failures that result from a variety of degradation (wear out) mechanisms in hardware. System failure rates arising from random hardware failures can be quantified with reasonable accuracy based on past experience *(e.g. previous in service failure rate =* 10^{-6} */ flight hour)*



Systematic failure. Failures resulting from faults in the specification, design, construction, operation or maintenance of the system or its components. A systematic failure will always occur under a particular combination of inputs, or under some particular environmental conditions.

RTCA/DO-178B

"Software Considerations in Airborne Systems and Equipment"

www.rtca.org

Lars Holmlund Saab Aerosystems
2009-10-12
This document is the property of Saab AB and must not be reproduced in any form or distributed to third party without the written consent of Saab AB

SAABGROUP.COM

Lars.Holmlund@saabgroup.com