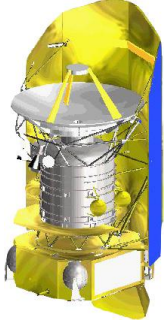


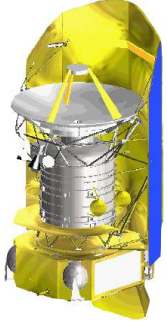

ACMS FDIR System for the Herschel / Planck satellites

J.F.T. Bos(1)

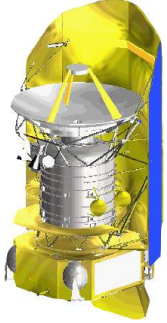
D. Zorita(2) , A. Bacchetta(3) , G. Chlewicki(3) , D. Guichon(4) , I. Rasmussen(5)

(1) Dutch Space B.V,

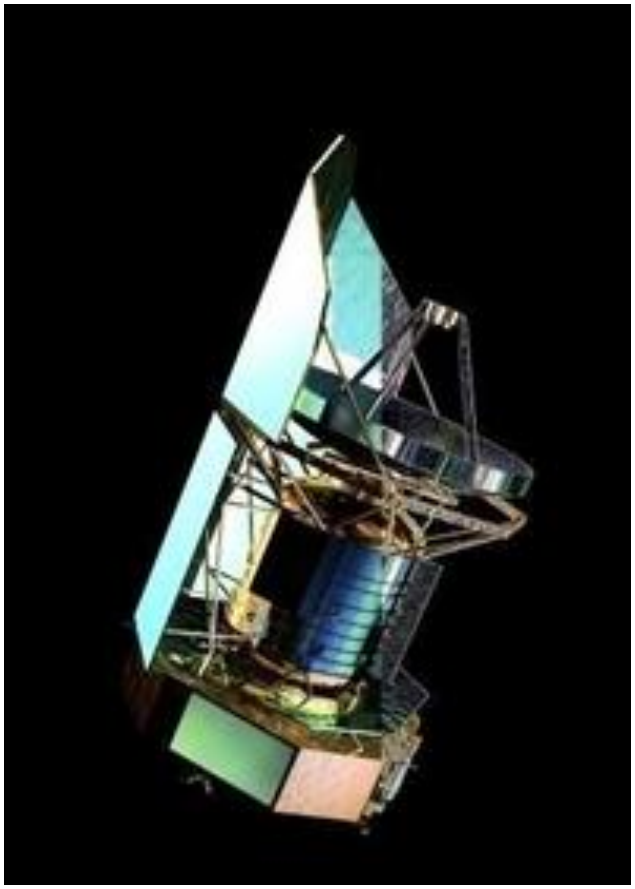
(2) Sener, (3) Alenia Aerospazio, (4) Alcatel, (5) ESA

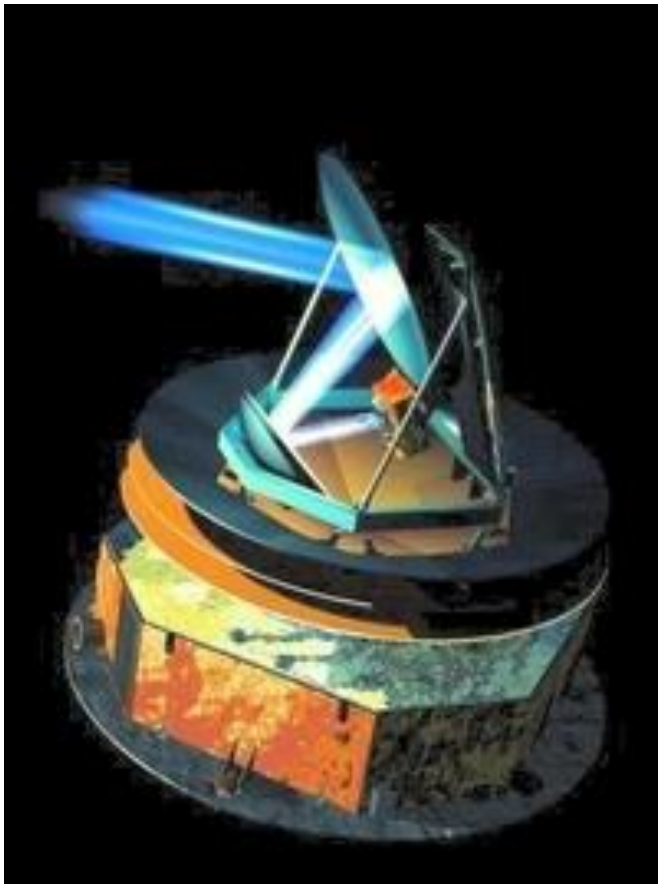


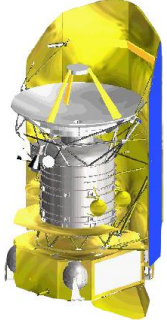
Contents




Introduction

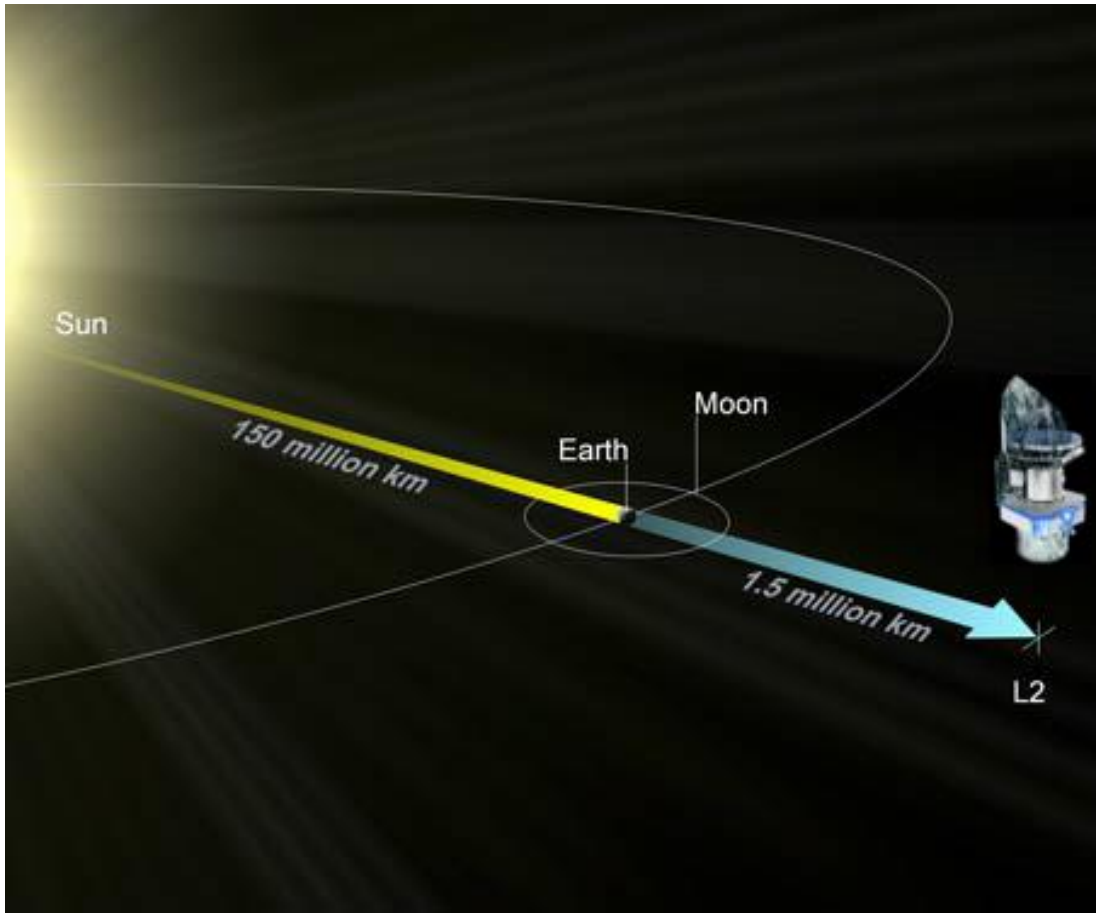




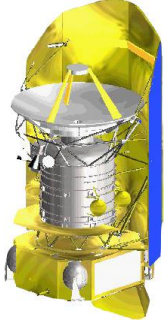


Herschel – Planck ACMS

Dutch Space

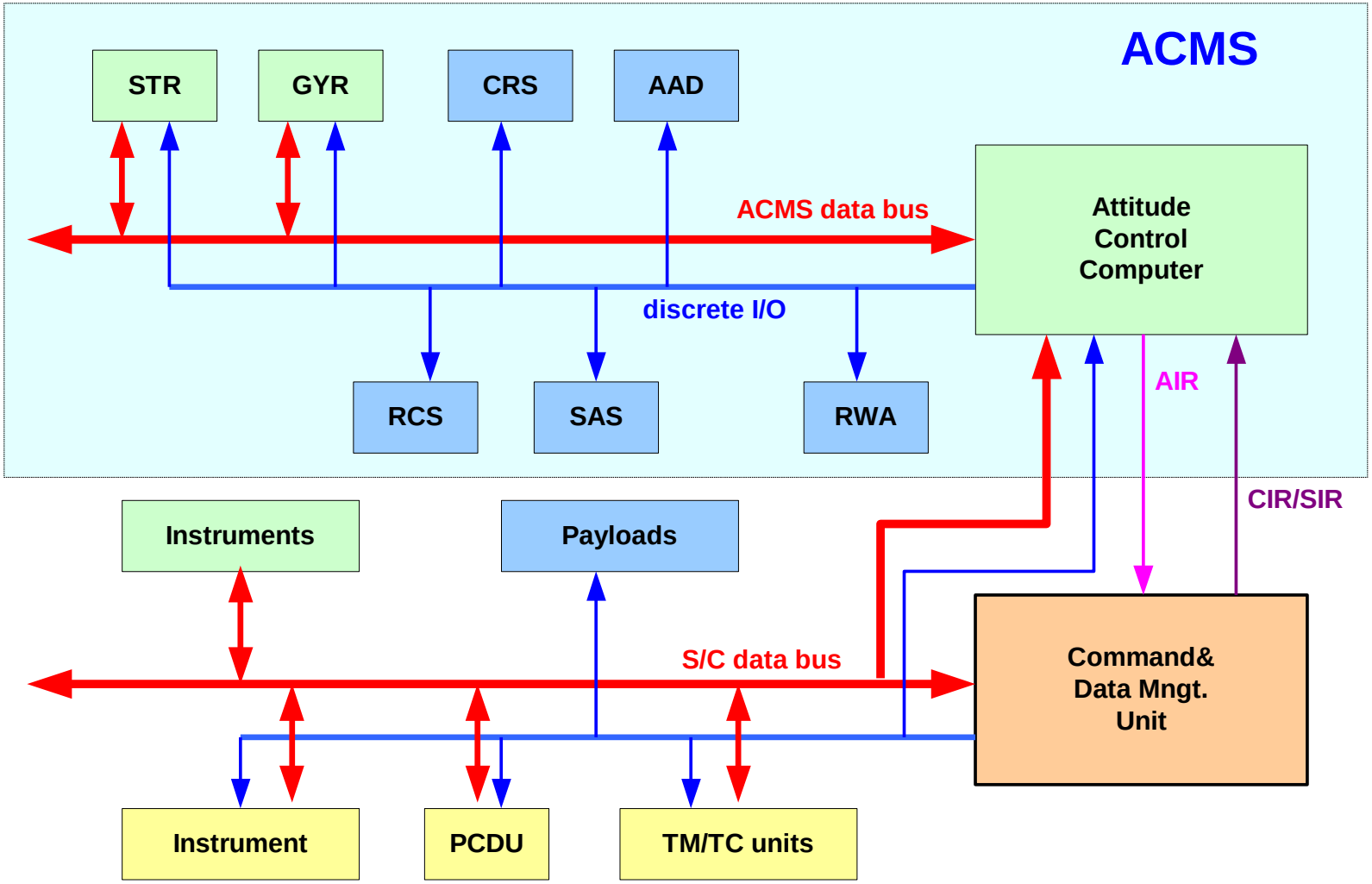


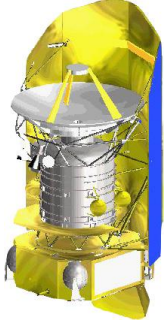
-Orbit around second Lagrangian Point in Earth/Moon - Sun System
-1.5 million kilometres from Earth.
-Transfer trajectories with duration of three months



Herschel – Planck ACMS

Dutch Space






General FDIR approaches

- only vital criteria, like attitude loss, checked by HW independent of HW nominal control loop.

Recovery by Ground

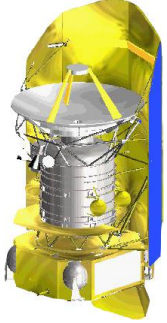
(**SOHO, XMM, Integral**)

- SW checks verifying sensors/actuators health.

Recovery autonomously by satellite.

No independent hardware

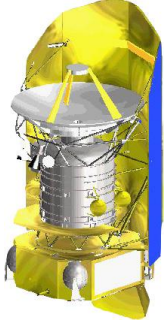
(**Rosetta, Mars Express**)



General FDIR approaches (2)

<u>"SOHO" (independent HW)</u>

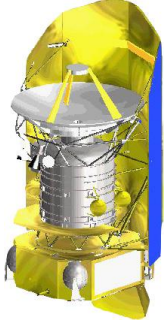
- **1 fail-safe guaranteed**
- **simple straightforward FDIR design**
- **relatively small verification effort**
- **relatively large effort in Ground procedures**
- **execution recovery procedures relatively time-critical**



General FDIR approaches (3)

“Rosetta” (SW only)

- **no extra HW**
- **complex FDIR design**
- **large verification effort**
- **easier for Ground**
- **less outage time**



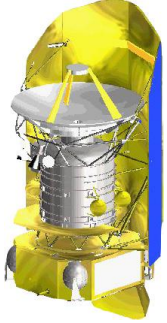
Herschel / Planck FDIR design

2 goals:

- **ensure safety**
- **guarantee mission continuation after 1 failure**

2 FDIR modes:

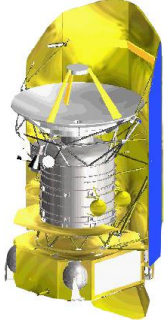
- **Autonomous Fail Safe**
- **Autonomous Fail Operational**



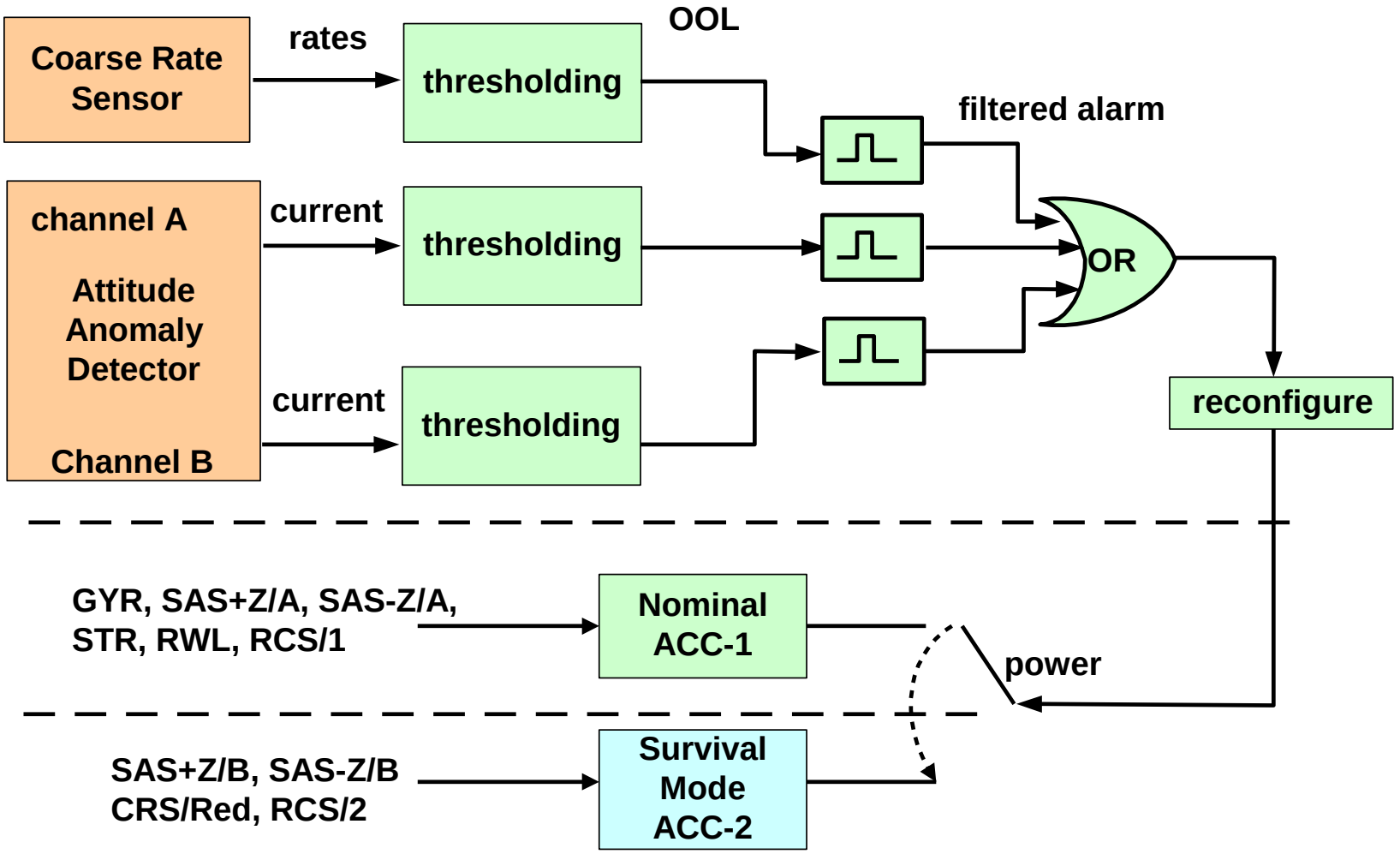

Hierarchical structure

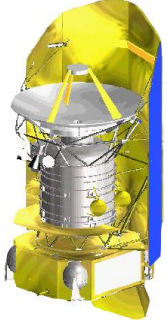
- **failure severity**
- **functions involved in detection (HW/SW)**
- **recovery sequence**

levels 0 - 4

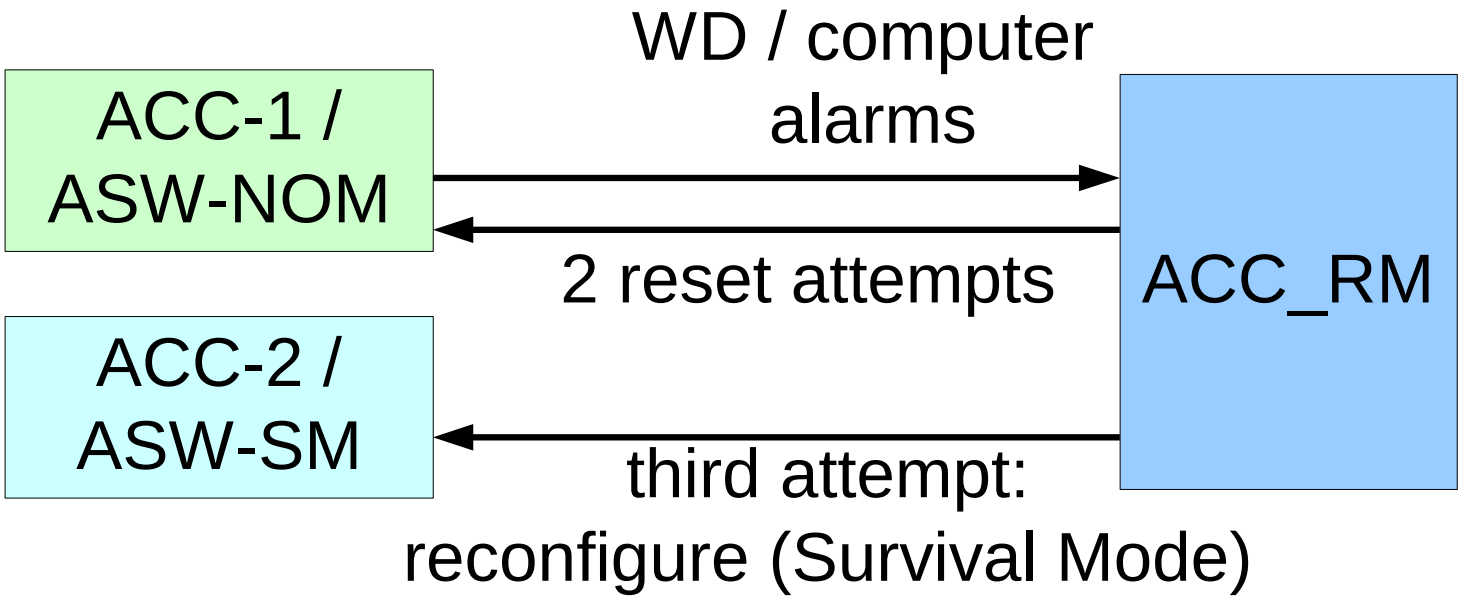


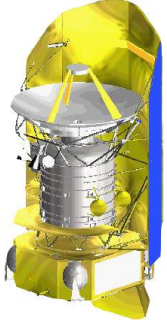
Level 4 (ARAD)


Coarse Rate Sensor
rates
thresholding
OOL
filtered alarm
channel A
Attitude Anomaly Detector
Channel B
current
thresholding
current
thresholding
OR
reconfigure
GYR, SAS+Z/A, SAS-Z/A,
STR, RWL, RCS/1
Nominal ACC-1
power
SAS+Z/B, SAS-Z/B
CRS/Red, RCS/2
Survival Mode ACC-2

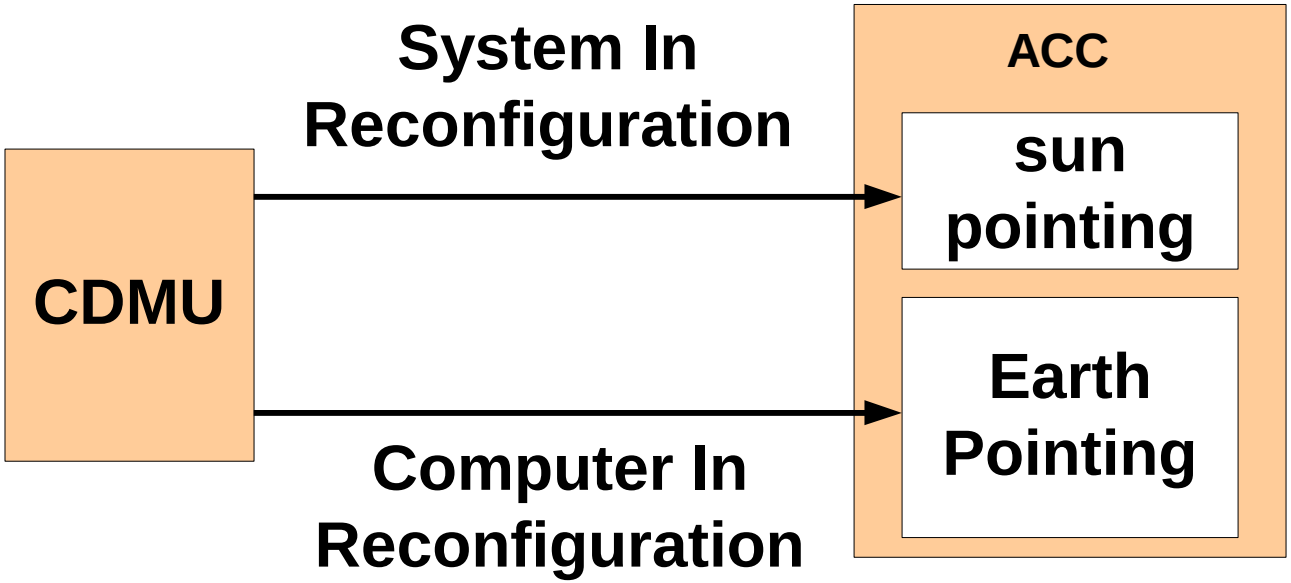


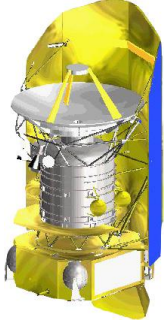
Level 3


WD / computer alarms
ACC-1 / ASW-NOM
2 reset attempts
ACC_RM
ACC-2 / ASW-SM
third attempt: reconfigure (Survival Mode)

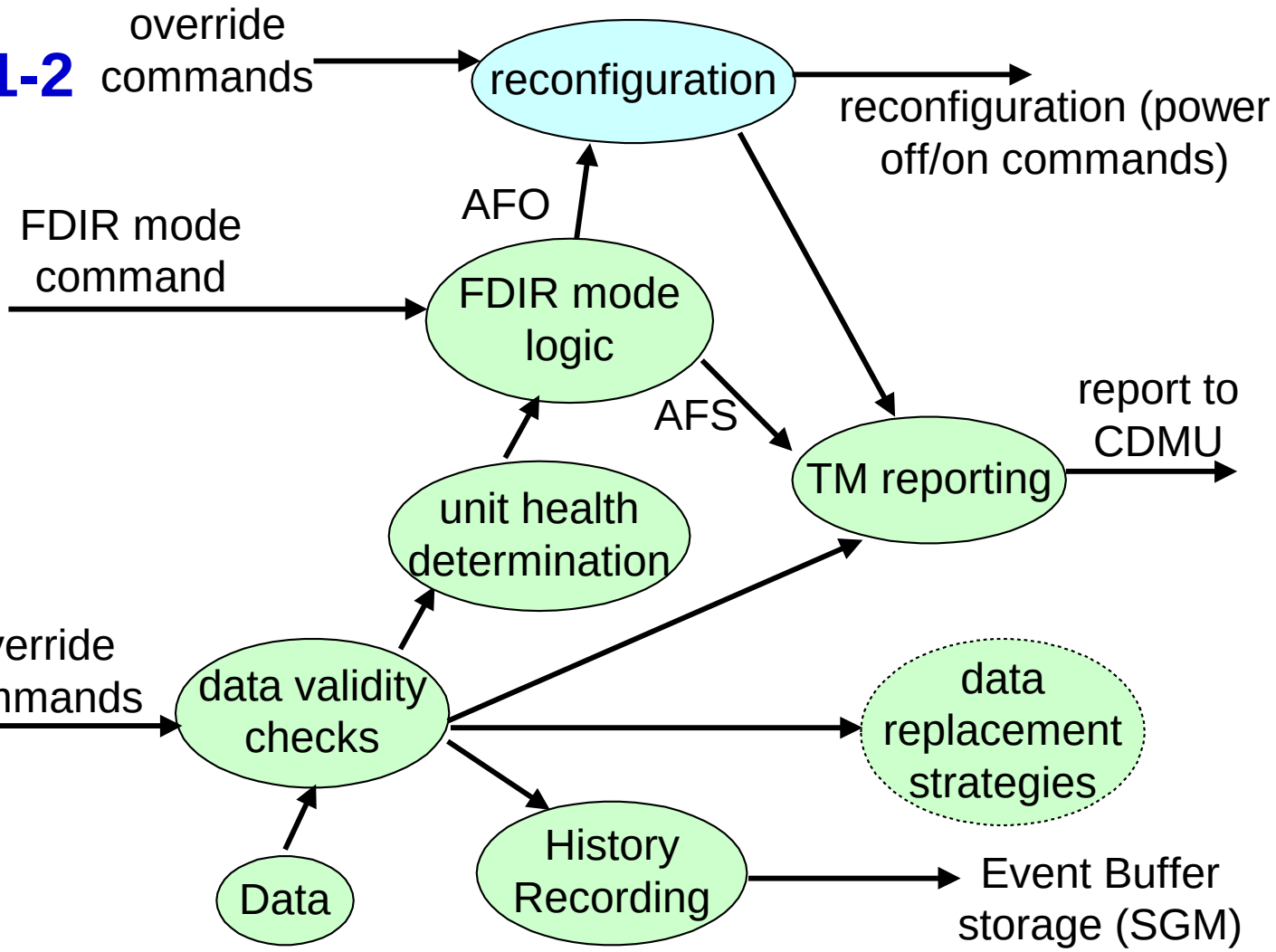


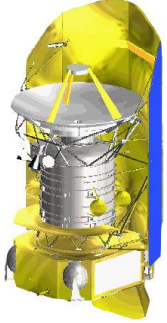

Level 3 (2)


System In
Reconfiguration
CDMU
Computer In
Reconfiguration
ACC
sun
pointing
Earth
Pointing

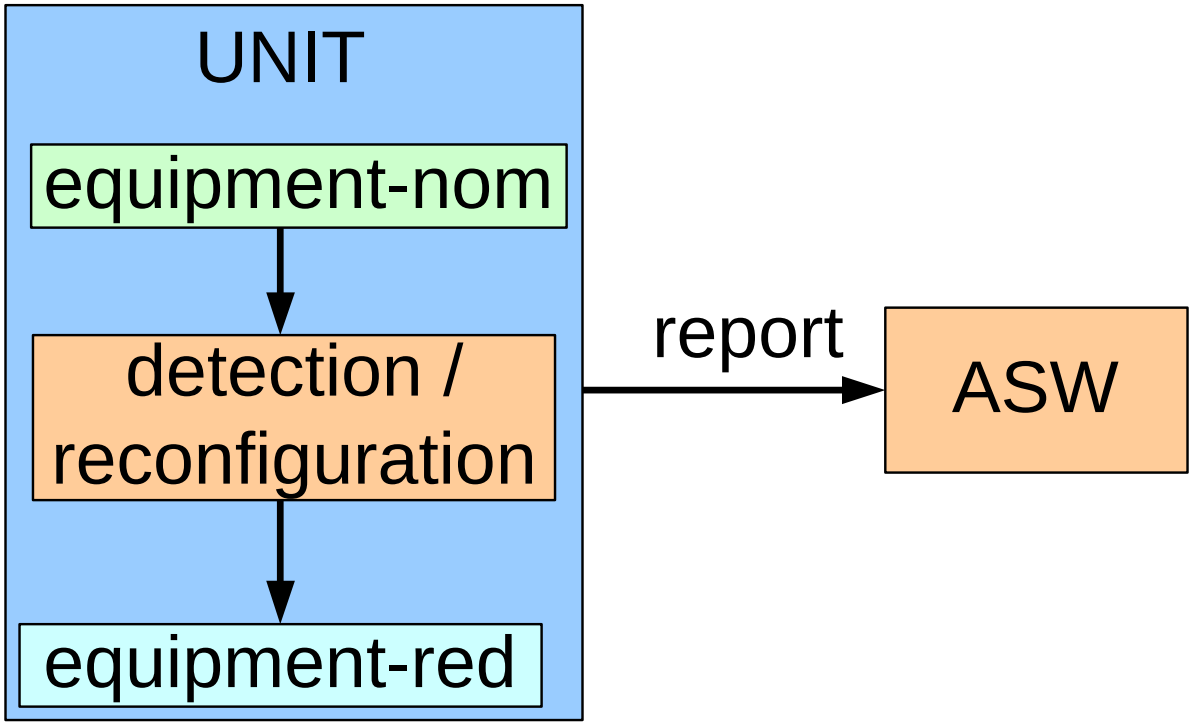


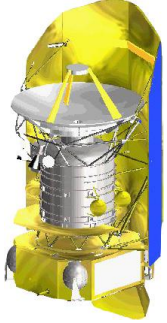
Levels 1-2


override commands
reconfiguration
reconfiguration (power off/on commands)
AFO
FDIR mode command
FDIR mode logic
AFS
report to CDMU
TM reporting
unit health determination
override commands
data validity checks
data replacement strategies
History Recording
Event Buffer storage (SGM)
Data



Level 0


UNIT
equipment-nom
detection / reconfiguration
equipment-red
report
ASW




Discussion

2 goals:

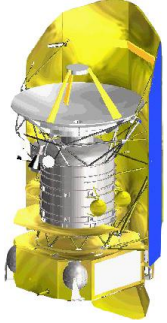
- **ensure safety**
- **guarantee mission continuation after 1 failure**

safety ⇒ independent HW/SW

independent?

Similar HW ⇒no guard against design errors

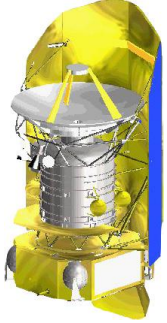
Similar SW ⇒ drivers, OS, …….. , algorithms



Independent HW ⇒ easily proven safety:

- **no Monte Carlo needed to prove effect under all dynamical conditions**
- **no fault diagnosis needed for safety**
- **S/W failures do not need to be analyzed**
- **checks ⇒ no guarantee necessary that all subtle failures are detected**

⇒ small verification effort



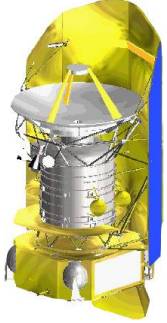
Single failure ⇒ Survival Mode inadvertently

- **can be avoided by majority voting of 3 sensors**

Not done

justification:

- **spike filtering**
- **conservative thresholds**
- **AAD simple & highly reliable**



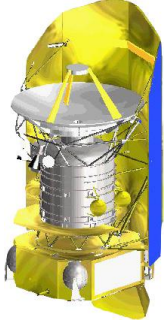
guarantee mission continuation after 1 failure

All units subject to health checking

Mode : AFS (no reconfiguration allowed) ⇒ Sun Acq., dV

AFO (reconfiguration allowed) ⇒ science

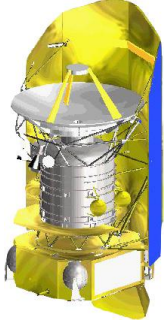
more optimal when only more complex units used in scientific operations subject to health checking




subject to health checks ⇒ depend on reliablity

- **SAS ⇒ simple, highly reliable, flight proven ⇒ not needed**

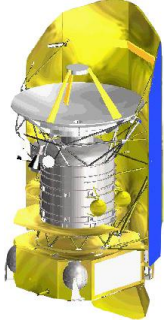
- **STR ⇒ complex, sensitive for solar flares ⇒ needed**



Herschel – Planck ACMS

Dutch Space

	SOHO	Rosetta	H/P
power	—	+	—
mass	—	+	—
extra HW (costs)	—	+	—
design effort	+	—	+
verification effort	+	—	+
safety	+	—	+
availability	—	+	+
Ground effort	—	+	+




Conclusion

<u>Herschel/Planck FDIR design</u>:

- **Combined best aspects of both main FDIR approaches**
- **Easily verified safety of the s/c**
- **Autonomous mission continuation enhanced**
- **More optimal when only more complex units used in scientific operations subject to health checking.**