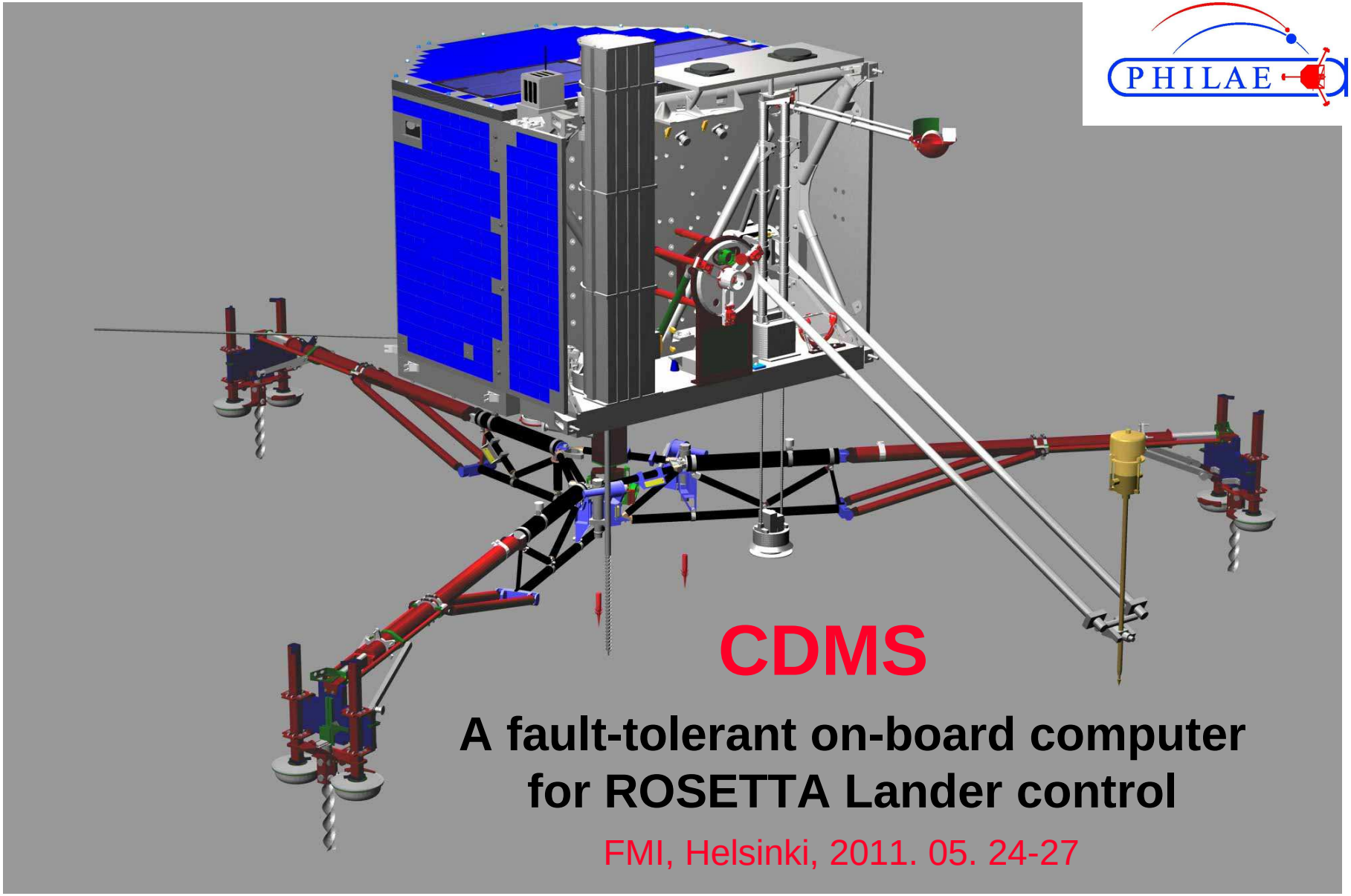


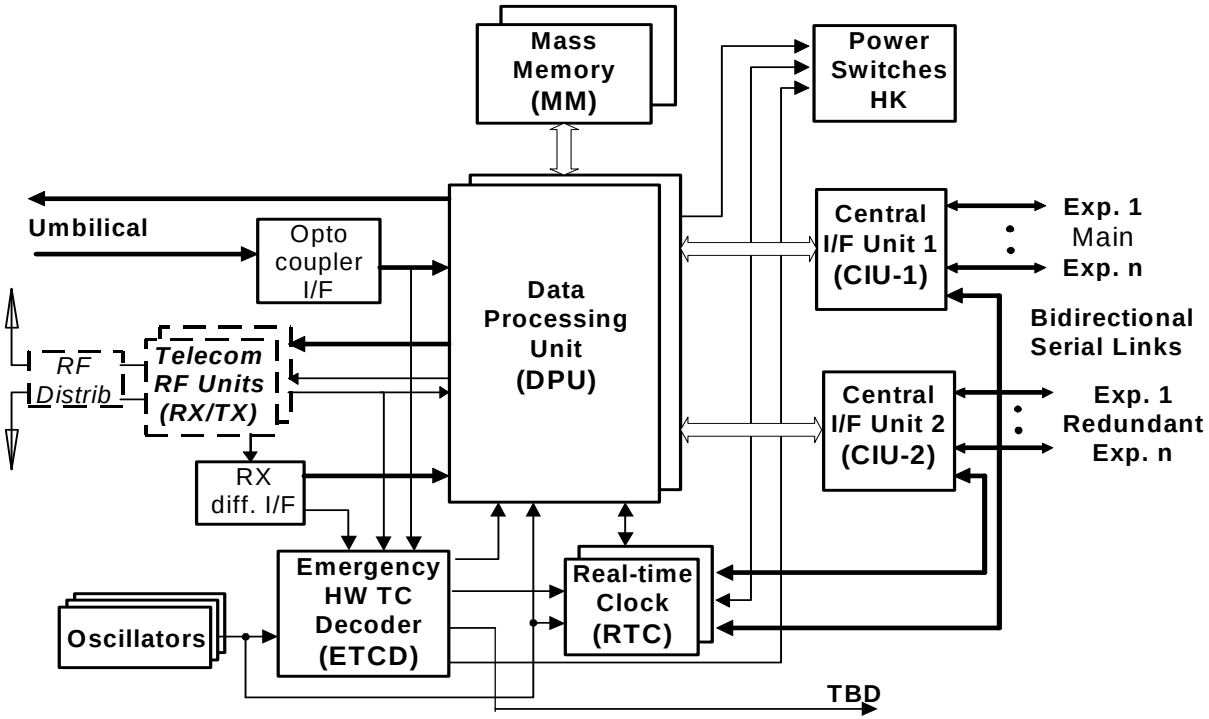
CDMS

A fault-tolerant on-board computer for ROSETTA Lander control

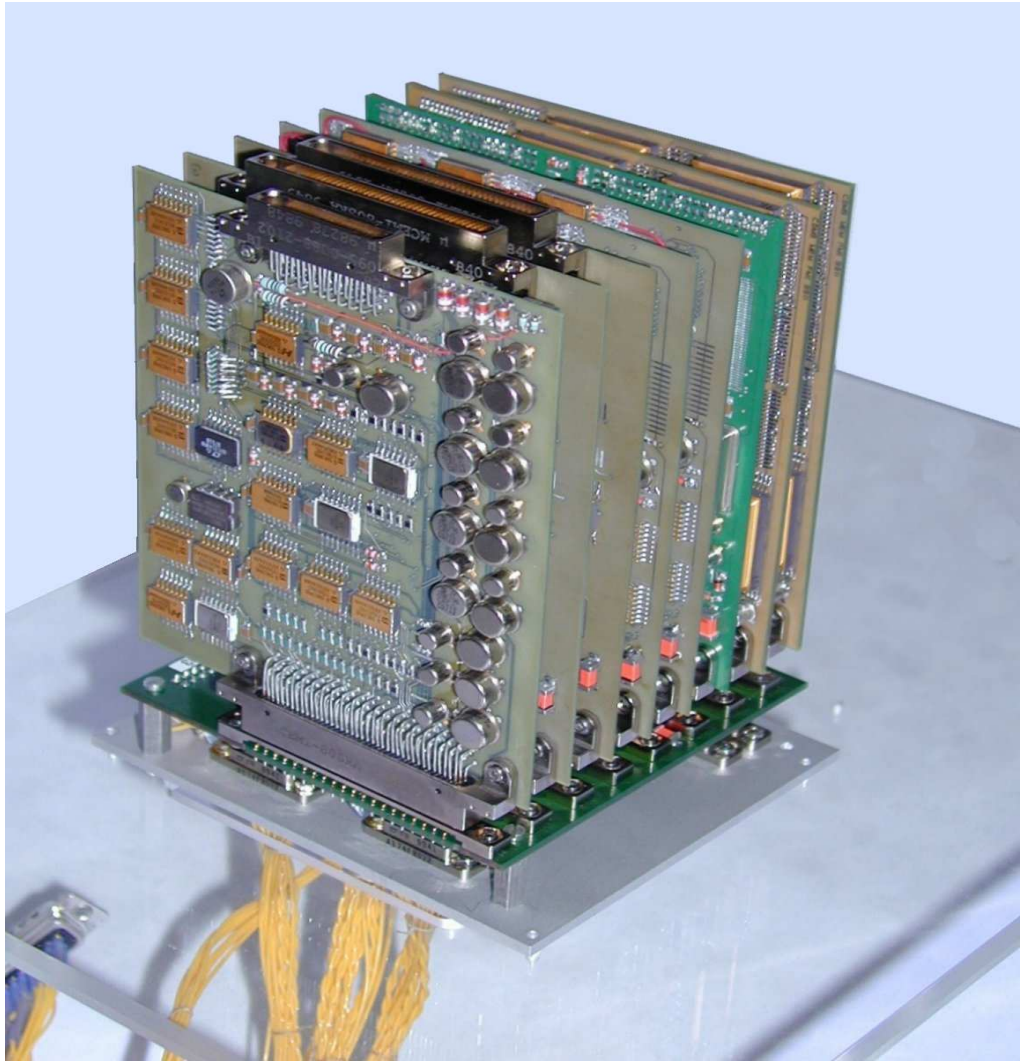
FMI, Helsinki, 2011. 05. 24-27

HW & SW design concept

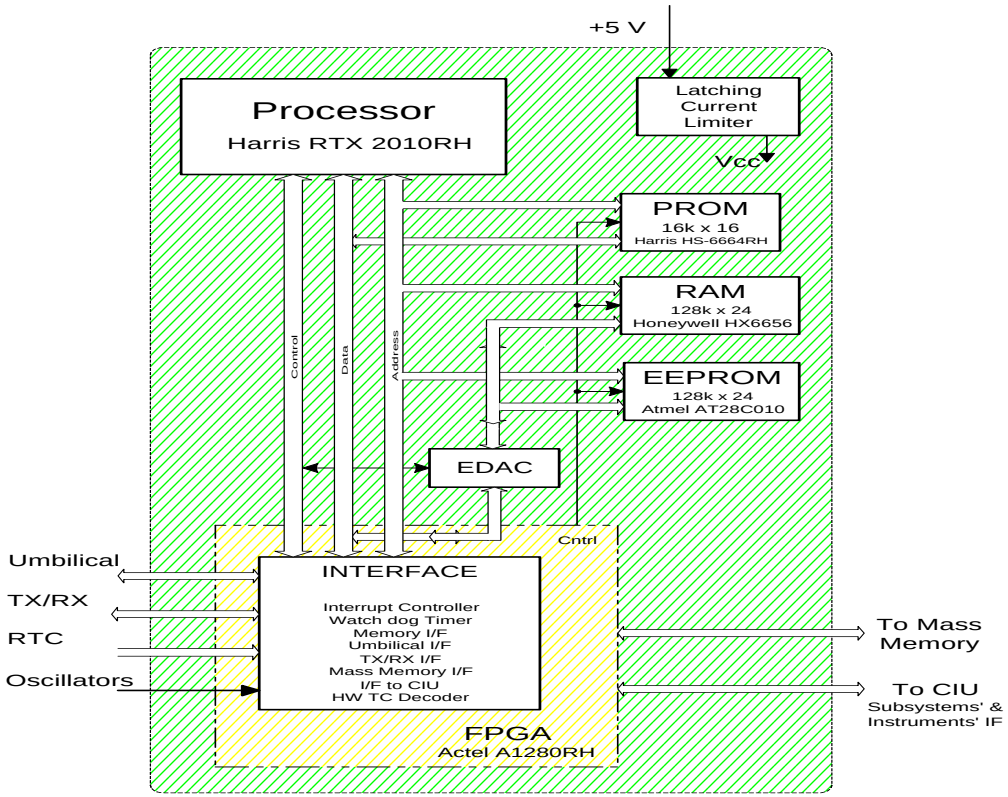
- Product of: KFKI-RMKI/Budapest, FMI/Helsinki, MPS/Lindau
- Fault tolerant design against ALL conceivable single-point-failures
- Redundant HW sub-units; Support/establish fault tolerance by SW
- Hot redundant DPUs and Real-time Clock
- Autonomous and commandable hot vs. cold redundancy control for MMs, CIUs, RX/TX units (aspect by aspect, i.e. power consumption, etc.)
- Failure recognition, isolation and recovery



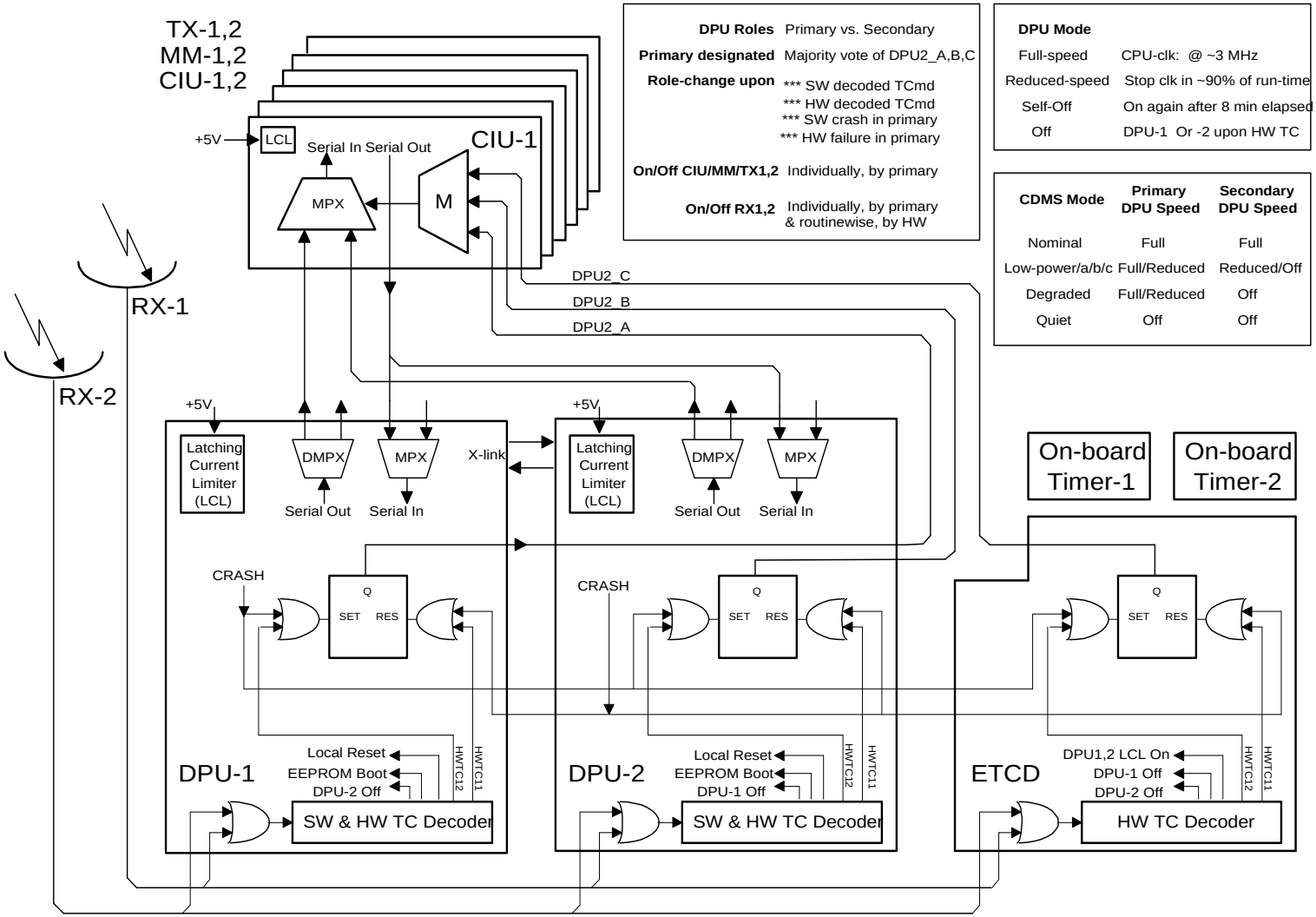
The CDMS HW stack



The DPU(s)


+5 V
Processor
Harris RTX 2010RH
Latching
Current
Limiter
Vcc
PROM
16k x 16
Harris HS-6664RH
RAM
128k x 24
Honeywell HX6656
EEPROM
128k x 24
Atmel AT28C010
Control
Data
Address
EDAC
Cntrl
Umbilical
TX/RX
RTC
Oscillators
INTERFACE
Interrupt Controller
Watch dog Timer
Memory I/F
Umbilical I/F
TX/RX I/F
Mass Memory I/F
I/F to CIU
HW TC Decoder
FPGA
Actel A1280RH
To Mass
Memory
To CIU
Subsystems' &
Instruments' IF

CDMS redundancy scheme



DPU Roles	Primary vs. Secondary
Primary designated	Majority vote of DPU2_A,B,C
Role-change upon	*** SW decoded TCmd *** HW decoded TCmd *** SW crash in primary *** HW failure in primary
On/Off CIU/MM/TX1,2	Individually, by primary
On/Off RX1,2	Individually, by primary & routinewise, by HW

DPU Mode	
Full-speed	CPU-clk: @ ~3 MHz
Reduced-speed	Stop clk in ~90% of run-time
Self-Off	On again after 8 min elapsed
Off	DPU-1 Or -2 upon HW TC

CDMS Mode	**Primary DPU Speed**	**Secondary DPU Speed**
Nominal	Full	Full
Low-power/a/b/c	Full/Reduced	Reduced/Off
Degraded	Full/Reduced	Off
Quiet	Off	Off

Subsystem Interface design aspects

- Possibly simple data/message structure -> “Easy” reception/decoding at Unit side thru simple HW;
- Serial information transmission with “built-in” synchro patterns (to reduce harness)

SSADR Subsystem Address Word (CDMS → Subsystem, Instrument)

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
SSADR					T/R	ACTC / Subaddress					WRDC				

SSADR	Subsystem Address
T/R	Transmit/Receive bit
ACTC	Action Code / Subaddress
WRDC	Word Count

SSCMD Subsystem Command Word(s) (CDMS → Subsystem, Instrument)

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
16 bit DATA															

SSTS Subsystem Status Word (CDMS ← Subsystem, Instrument)

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
SSADR					ME	CE	SR	1	0	0	0	BSY	SM	0	0

SSADR	Subsystem Address
ME	Message Error Flag
CE	Count Error Flag
SR	Service Request Flag
BSY	Busy Flag
SM	Sleep Mode Flag

SSDAT Subsystem Data Word(s) (CDMS ← Subsystem, Instrument)

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
16 bit DATA															

Subsystem Interface design aspects

- Common protocol to cover communication with both “non-intelligent” and intelligent Units
  - Experiments:
    MUPUS, CIVA, ROMAP, PTOLEMY, COSAC, APX, SESAME, COSAC
  - Subsystems: PSS, LandingGear, FLW, ANCHOR, ADS, SD2
- General Services: OBT and Lander/CDMS status distribution to Payload
- Passive but scheduled TC forwarding to Experiments and Subsystems (ADS, LG)
- Acive autonomous operation timing and control of Subsystems (PSS, Anchor)
- Permanent TM data collection (HK regularly, Science on request)
- Bitrate -> Neither “too low”, nor “too high”
- TM=16 kbit/sec → SSIF=2*16=32 kbit/sec (for data collection/packetizing)
- Message transfer/timing: Strict in timing on HW level ->
  on SW level (no time-outs)
- Failure tolerance/isolation:
  - Star instead of Bus Structure; Main/Redundant SSIF

Subsystem Interface communication protocol

Code	Mnemo	Action Code / Subaddress	BRD	T/R	WRDC	CMD Word(s)	DATA Word(s)
00000	TRSW	Trm Status Word	No	1	void	——	——
00001	TRQC	Trm Request Code Word	No	1	1	——	Request Code
00010	STBY	Standby Mode / Power Down	Yes	0	TBD	TBD	
00011	RMOD	Rcv Current CDMS Mode	Yes	0	1	CDMS Mode; SSCLK	——
00100	RTIM	Rcv On-Board Time	Yes	0	2	On-Board Time Code	——
00101	RSST	Rcv Service System Status	Yes	0	TBD	Service Sys. Status	——
00110	RAXT	Rcv Action Code / Subaddress Extension	Yes	0	1	ACTC / Subaddress	——
00111	RHFM	Rcv Housekeeping Data Format Count	Yes	0	1	HK Format Count	——
–\\–	THKD	Trm Housekeeping Data Word	No	1	1	——	HK Data Word
01000	RCMD	Rcv Telecommand Sequence	No	0	n	Command Sequence	——
01001	TCMO	Trm Offset/Length of Stored Tcmd. Buffer Section	No	1	2	——	Offset; Length
–\\–	RCMS	Rcv Stored Telecommand Buffer Section	No	0	Length	Buffer Section	——
01010	RASV	Rcv Allocated Science Data Volume	No	0	2	Packet counts	——
–\\–	TSCR	Trm Science Data Burst	No	1	4; 32	——	Science Data Burst
01111	RSCS	Receive Science Data Packet Checksum	No	0	1	Check Sum	——
01011	RBUS	Rcv Allocated Backup RAM Buffer Size	No	0	1	Record count	——
–\\–	TBUP	Trm Pointer of Backup RAM Buffer Record	No	1	1	——	Unit, Pointer
01100	TBUF	Trm Backup RAM Buffer Record	No	1	32	——	Data Record
–\\–	RBUF	Rcv Backup RAM Buffer Record	No	0	32	Data Record	——
01110	TTRG	Trm Trigger Word	No	1	1	——	Dest. & Trigger
–\\–	RTRG	Rcv Trigger Word	Yes	0	1	Source & Trigger	——
01101	RERC	Rcv Error Code Word	No	0	1	Error Code Word	——

*** Subaddresses 10000 thru 11110 are reserved for direct register addressing of non-intelligent Units

Code	Mnemo	Request Code	
0001	SSST	Send Service System Status	
0010	SCMD	Send Stored Tcmd. Buffer Section	*
0011	SASV	Send Allocated Science Data Volume	
0100	SRDY	Science Data Ready	
0101	SBUS	Send Allocated Backup RAM Buffer Size	*
0110	WRBF	Write Backup RAM Buffer Record	*
0111	RDBF	Read Backup RAM Buffer Record	*
1000	PTRG	Pass Trigger Word	*
1001	FLSP	Flush Last Science Data Packet	
1010	OCPL	Operation Completed	

Bit0 Illegal Request Code
Bit1 Illegal Unit, Pointer, Offset, Length
Bit2 Request Code Undue
Bit3 Mass-memory Full
Bit4 Allocated Science Data Volume Exhausted
Bit5 Destination Unit Off
---

* May be Undue during RF visibility

*** Bits15..8 of the Request Code Word are reserved for non-intelligent Units

Telecommunication (Lander vs. Spacecraft)

- Orbiter/ESS = master; Lander/CDMS = slave
- Request-to-send-like handshaking protocol on 2 telecom media; Umbilical = wire as long as attached; RF = radio after separation
  - In terms of information transfer: half-duplex (either TC, or TM)
  - In terms of link maintenance: full-duplex (either “information” or “link-pattern”)
- Link establishment (specific link patterns with specific timing in specific order)
  - TC session (ESS: RTO patterns -> CDMS: ACK patterns -> ESS: TC packet(s))
  - TM session (ESS: STO patterns -> CDMS: TM packet(s))
  - Link maintenance (ESS: STO patterns -> CDMS: MOL patterns)
- Information transfer by means packetized data structures (TC, TM)
  - Constant packet sizes to facilitate management and simplify HW design (i.e. MM)
  - Packet structure adapted to that of ROSETTA Orbiter

Mass memory (Product of FMI)

- A standalone HW controlled FIFO,
  with specific protocol between CDMS and MM.

- RAM = “work area”;
  EEPROM = 1to1 copy of RAM, “backup memory” if unpowered;
  - MMRAM->EEPROM save prior to turn off,
  - MMEEPROM->RAM retrieveal after turn on.

- TM data/packets (min CDMS, PSS HK) are always generated in/by CDMS
  - If telecom link is not established -> forward TM data into one of the MMs
  - If telecom link is established and MM is not empty -> dump TM data from MM
  - If telecom link is established and MM is empty -> forward TM data directly onto the link

TC Packets structure / aspects

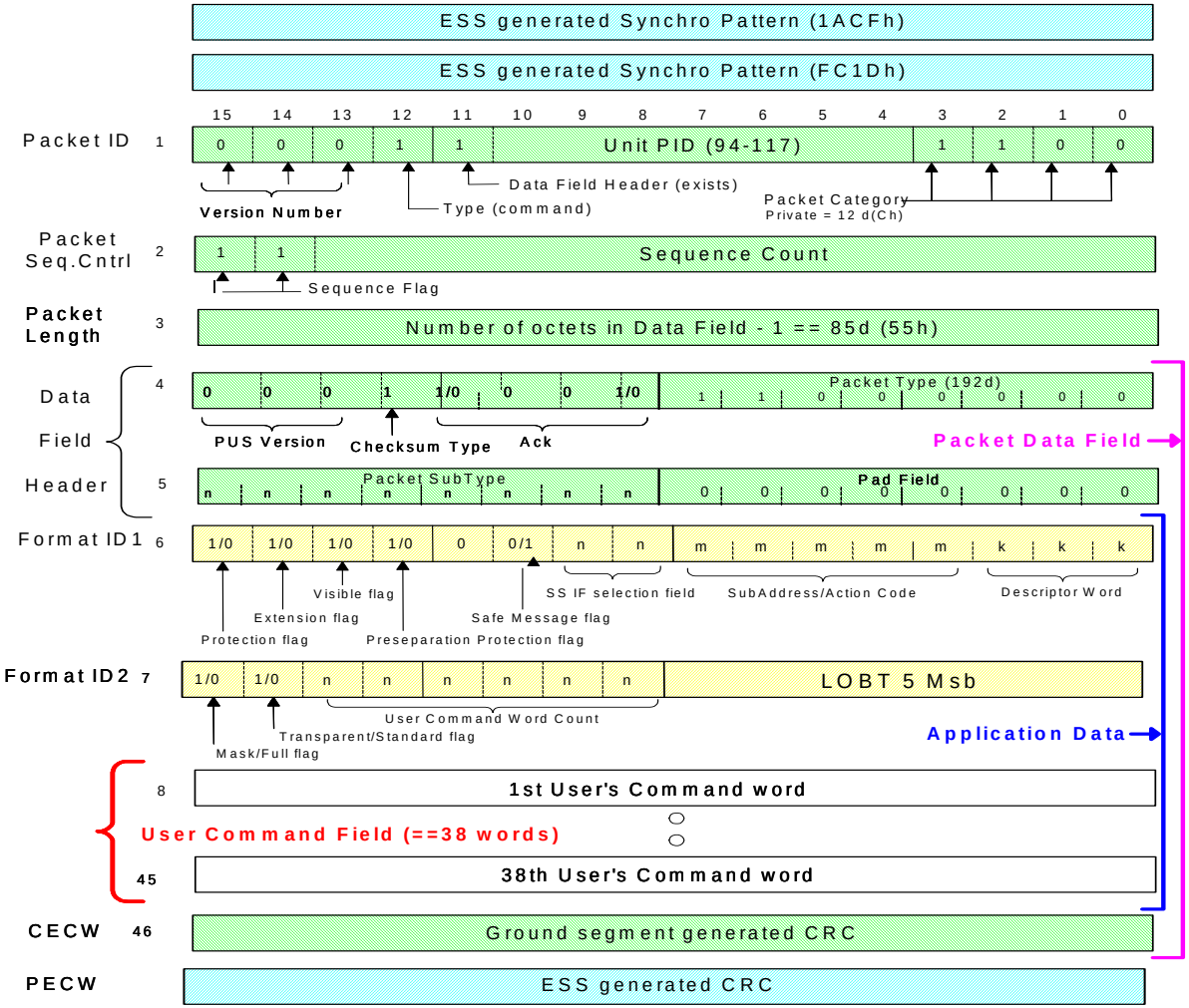
- TC structure adapted
  - to that of the ROSETTA Orbiter (ESA Header, ESA Data Field)
  - to the command/data structure on the Subsystem Interface (SSIF)
  - to the way of operational sequencing/timing by CDMS SW (AMSTs, AMDTs)

- ESA Data Field accommodates a specific internal data structure

- An internal header (Format ID1 & 2) for general TC definition and control
- Descriptor words for TC storage, timing and execution control

  - **MCOD** manipulation code / timing mode / block size
  - **OFFS** offset of the addressed buffer section
  - **TIMM** time-tag for buffer section - middle order word
  - **TIML** time-tag for buffer section - low order word
  - **AMDT** AMDT identifier which the time-tagged TC is associated to
  - **CRCW** CRC code word for the selected buffer section
  - Series of Command words to forward them to the addressed Unit

TC Packets structure



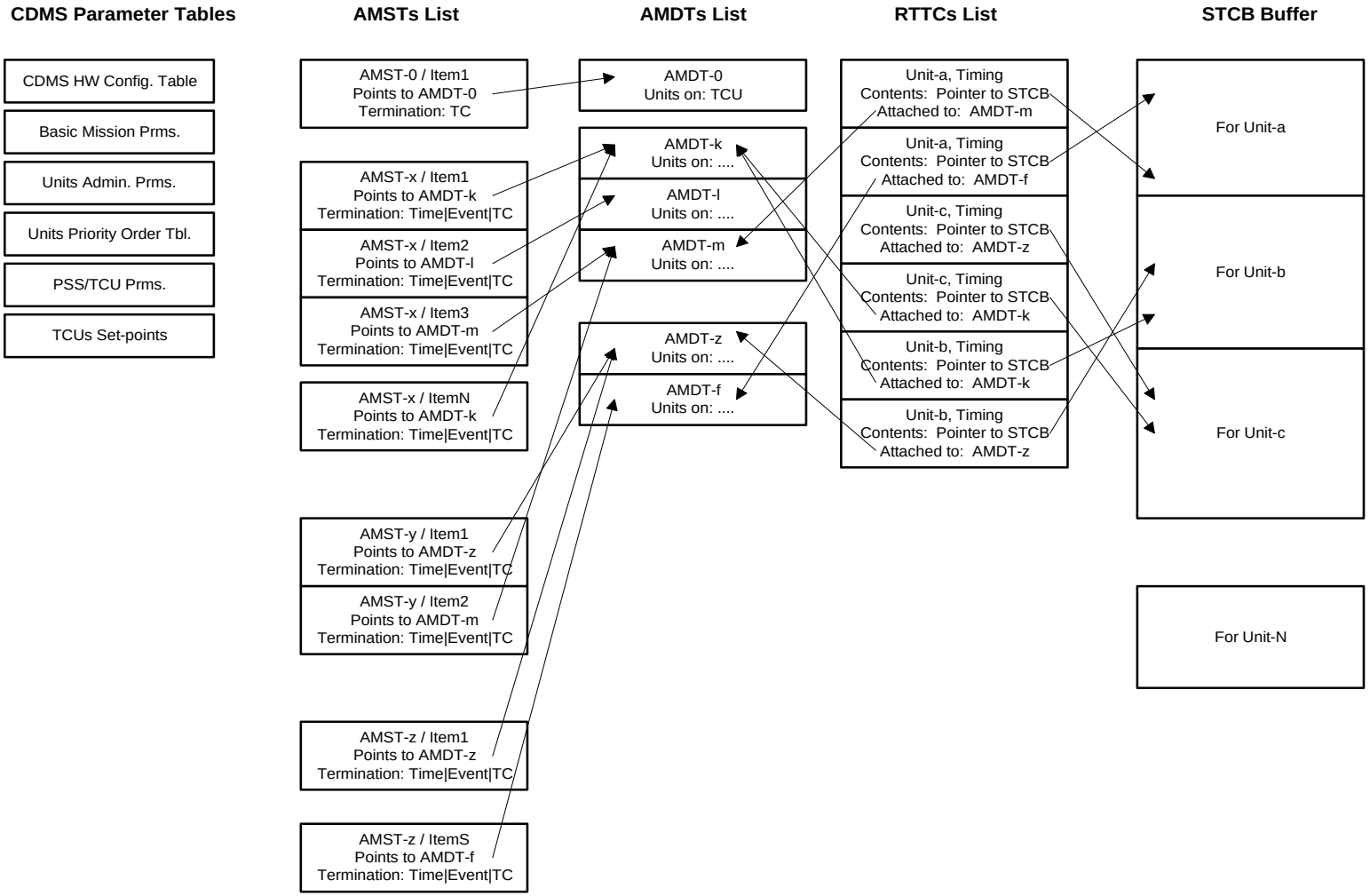
Autonomous on-board sequencing

- Acquisition Mode DESCRIPTOR Tables (AMDTs) = payload configuration of “Lander”
  - CDMS mode (nominal vs. low power, etc…)
  - What units to turn on
  - Allocated Mass-memory quotas
- Acquisition Mode SEQUENCER Tables (AMSTs) = steps of configuration changes
  - An AMST = series of so called AMST items
  - “Machine code of sequencing”
- AMST Items
  - what to do (Nominal Activities + link to an AMDT with RelTtagTCs)
  - how long (time-out, event)
  - how to proceed upon completion (flow-control, i.e. jump forward/backward; repeat a certain part of the sequence upon non-nominals, i.e. overload)

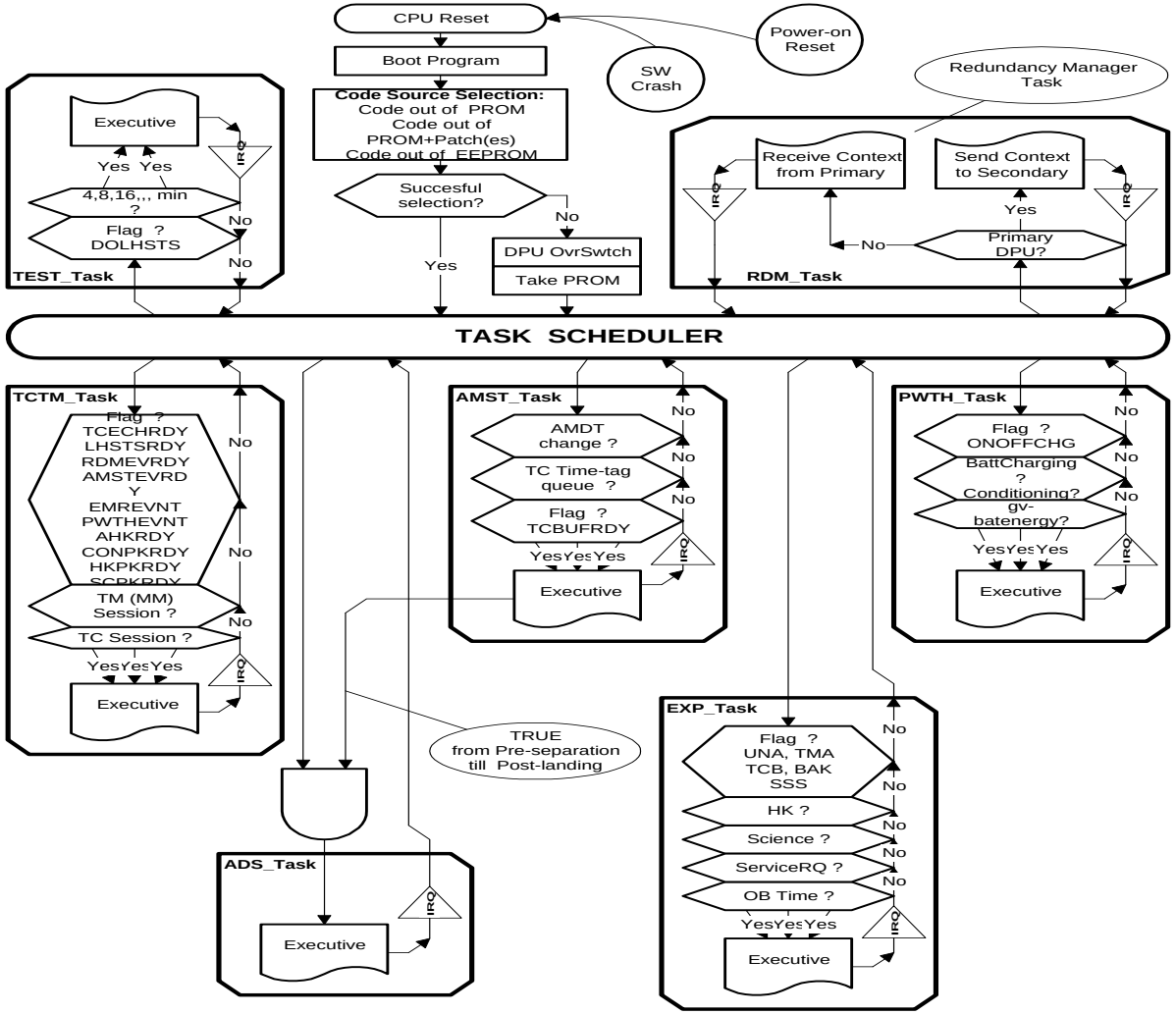
TC timing and execution mechanisms

- **Direct TCs, AbsTtagTCs, RelTtagTCs associated to AMDTs**
- **RelTtagTC List -> AbsTtagTC queue**
- **Timelines**
  - **Orbiter (MTL)**
    (AbsTtagTCs on MTL -> DirectTCs Or AbsTtagTCs for Lander)
  - **Lander internal (AMSTs)**
    (RelTttagTCs -> AbsTtagTCs for Lander)

Parameter Tables structures and links



Multitasking CDMS SW



CDMS On-board Software
Task Activation Flow

Mission Phases and Tasks

- Cruise …. 10 years
  - Routine activities, payload check-out, in-flight calibration
- SDL (Separation-Descent-Landing) … 0.5-1-2 hours
  - Critical phase
  - High data load on CDMS, active anchoring control
- FSS (First Science Seqences) … 4-5 days
  - Powered by the primary(1300) + secondary(140) Wh
- LTS (Long Term Science operations) … “N” months
  - Powered by the secondary batt. + solar power (~10W at 3AU)
  - Amount of solar cells turned out to have been “underdesigned”
  - Lot of questionmarks in terms of feasibility far from the sun
  - Complex temperature household and secondary battery charging control had to be implemented in/by CDMS

How to get the maximal solar power?

- Reconstruct the sun orbit wrt. lander, in-situ, from changing distribution of solar panels HK data collected during the first revolution of the comet after landing
- Afterwards rotate lander around its vertical axis into a from collected solar energy/orbit point of view optimal position