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 DPU 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)

Processor
Harris RTX 2010RH

FPGA
Actel A1280RH

Latching
Current
Limiter

PROM
16k x 16
Harris HS-16K43RH

RAM
128k x 24
Honeywell HX6656

EEPROM
128k x 24
Atmel AT28C010

EDAC

INTERFACES
Interrupt Controller
Watch dog Timer
Memory I/F
Umbilical I/F
TX/RX I/F
Mass Memory I/F
HW TC Decoder

To Mass Memory
To CIU
Subsystems' & Instruments' I/F

+5 V

Umbilical
TX/RX
RTC
Oscillators

Rosetta Lander CDMS
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 Modes
- 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

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

Latching Current Limiter (LCL)

CDMS Mode
- Nominal
- Low-power
- Quiet
- Degraded
- Off

Primary DPU Speed
- Full
- Reduced

Secondary DPU Speed
- Full
- Reduced
- Off

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

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

Latching Current Limiter (LCL)

CDMS Mode
- Nominal
- Low-power
- Quiet
- Degraded
- Off

Primary DPU Speed
- Full
- Reduced

Secondary DPU Speed
- Full
- Reduced
- 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)

<table>
<thead>
<tr>
<th>SSADR</th>
<th>Subsystem Address Word</th>
<th>(CDMS Subsystem, Instrument)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>14</td>
<td>13 12 11 10 9 8 7 6 5 4 3 2 1 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSADR</th>
<th>T/R</th>
<th>ACTC / Subaddress</th>
<th>WRDC</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>SSCMD</th>
<th>Subsystem Command Word(s)</th>
<th>(CDMS Subsystem, Instrument)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>14</td>
<td>13 12 11 10 9 8 7 6 5 4 3 2 1 0</td>
</tr>
</tbody>
</table>

| 16 bit DATA |

<table>
<thead>
<tr>
<th>SSTS</th>
<th>Subsystem Status Word</th>
<th>(CDMS Subsystem, Instrument)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>14</td>
<td>13 12 11 10 9 8 7 6 5 4 3 2 1 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSADR</th>
<th>ME</th>
<th>CE</th>
<th>SR</th>
<th>BSY</th>
<th>SM</th>
<th>0 0</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>SSDAT</th>
<th>Subsystem Data Word(s)</th>
<th>(CDMS Subsystem, Instrument)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>14</td>
<td>13 12 11 10 9 8 7 6 5 4 3 2 1 0</td>
</tr>
</tbody>
</table>

| 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)
- Active 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)

<table>
<thead>
<tr>
<th>Code</th>
<th>Mnemo</th>
<th>Action Code / Subaddress</th>
<th>BRD</th>
<th>T/R</th>
<th>WRDC</th>
<th>CMD Word(s)</th>
<th>DATA Word(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000</td>
<td>TRSW</td>
<td>Trm Status Word</td>
<td>No</td>
<td>1</td>
<td>void</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00001</td>
<td>TRCC</td>
<td>Trm Request Code Word</td>
<td>No</td>
<td>1</td>
<td></td>
<td>Request Code</td>
<td></td>
</tr>
<tr>
<td>00010</td>
<td>STBY</td>
<td>Standby Mode / Power Down</td>
<td>Yes</td>
<td>0</td>
<td>TBD</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>00011</td>
<td>RMOD</td>
<td>Rcv Current CDMS Mode</td>
<td>Yes</td>
<td>0</td>
<td>1</td>
<td>CDMS Mode: SSCLK</td>
<td></td>
</tr>
<tr>
<td>00100</td>
<td>RTIM</td>
<td>Rcv On-Board Time</td>
<td>Yes</td>
<td>0</td>
<td>2</td>
<td>On-Board Time Code</td>
<td></td>
</tr>
<tr>
<td>00101</td>
<td>HSST</td>
<td>Hrv Service System Status</td>
<td>Yes</td>
<td>0</td>
<td>TBD</td>
<td>Service Sys. Status</td>
<td></td>
</tr>
<tr>
<td>00110</td>
<td>RAXT</td>
<td>Rcv Action Code / Subaddress Extension</td>
<td>Yes</td>
<td>0</td>
<td>1</td>
<td>ACTG / Subaddress</td>
<td></td>
</tr>
<tr>
<td>00111</td>
<td>HRFM</td>
<td>Hrv Housekeeping Data Format Count</td>
<td>Yes</td>
<td>0</td>
<td>1</td>
<td>HK Format Count</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TKD</td>
<td>Trm Housekeeping Data Word</td>
<td>No</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01000</td>
<td>HCMU</td>
<td>Rcv Telecommand Sequence</td>
<td>No</td>
<td>1</td>
<td>n</td>
<td>Command Sequence</td>
<td></td>
</tr>
<tr>
<td>01001</td>
<td>TCMD</td>
<td>Trm Offset/Length of Stored Tcmd. Buffer Section</td>
<td>No</td>
<td>1</td>
<td>2</td>
<td>Offset: Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HCMS</td>
<td>Rcv Stored Telecommand Buffer Section</td>
<td>No</td>
<td>1</td>
<td>3</td>
<td>Buffer Section</td>
<td></td>
</tr>
<tr>
<td>01101</td>
<td>HASV</td>
<td>Hrv Allocated Science Data Volume</td>
<td>No</td>
<td>1</td>
<td>2</td>
<td>Packet counts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR</td>
<td>Trm Science Data Burst</td>
<td>No</td>
<td>1</td>
<td>4, 32</td>
<td>Science Data burst</td>
<td></td>
</tr>
<tr>
<td>01111</td>
<td>RCS</td>
<td>Receive Science Data Packet Checksum</td>
<td>No</td>
<td>1</td>
<td>1</td>
<td>Check Sum</td>
<td></td>
</tr>
<tr>
<td>01111</td>
<td>HBUS</td>
<td>Rcv Allocated Backup RAM Buffer Size</td>
<td>No</td>
<td>1</td>
<td>1</td>
<td>Record count</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IBUP</td>
<td>Trm Pointer of Backup RAM Buffer Record</td>
<td>No</td>
<td>1</td>
<td>1</td>
<td>Unit, Pointer</td>
<td></td>
</tr>
<tr>
<td>01100</td>
<td>TBUF</td>
<td>Trm Backup RAM Buffer Record</td>
<td>No</td>
<td>1</td>
<td>32</td>
<td>Data Record</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HBUF</td>
<td>Rcv Backup RAM Buffer Record</td>
<td>No</td>
<td>1</td>
<td>32</td>
<td>Data Record</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TRG</td>
<td>Trm Trigger Word</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>Source &amp; Trigger</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTRG</td>
<td>Rcv Trigger Word</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>Destination &amp; Trigger</td>
<td></td>
</tr>
<tr>
<td>01101</td>
<td>HERE</td>
<td>Hrv Error Code Word</td>
<td>No</td>
<td>1</td>
<td>1</td>
<td>Error Code Word</td>
<td></td>
</tr>
</tbody>
</table>

---

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

**Request Code**

<table>
<thead>
<tr>
<th>Code</th>
<th>Mnemo</th>
<th>Request Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>SSST</td>
<td>Send Service System Status</td>
</tr>
<tr>
<td>0010</td>
<td>SCMD</td>
<td>Send Stored Tcmd. Buffer Section</td>
</tr>
<tr>
<td>0010</td>
<td>SAV</td>
<td>Send Allocated Science Data Volume</td>
</tr>
<tr>
<td>0110</td>
<td>SADY</td>
<td>Science Data Ready</td>
</tr>
<tr>
<td>0111</td>
<td>SBUS</td>
<td>Send Allocated Backup RAM Buffer Size</td>
</tr>
<tr>
<td>0110</td>
<td>WRBF</td>
<td>Write Backup RAM Buffer Record</td>
</tr>
<tr>
<td>0111</td>
<td>RDBF</td>
<td>Read Backup RAM Buffer Record</td>
</tr>
<tr>
<td>1000</td>
<td>PTRG</td>
<td>Pass Trigger Word</td>
</tr>
<tr>
<td>1001</td>
<td>FLSP</td>
<td>Flush Last Science Data Packet</td>
</tr>
<tr>
<td>1010</td>
<td>OCPL</td>
<td>Operation Completed</td>
</tr>
</tbody>
</table>

*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

***Bits 15..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

<table>
<thead>
<tr>
<th>Packet ID</th>
<th>Packet Seq;Cntrl</th>
<th>Packet Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

### Data Field
- **Packet ID**: 1
- **Packet Seq;Cntrl**: 2
- **Packet Length**: 3

### Packet Data Field
- **Data Field Header**
  - Packet Type (192d)
  - Version Number
  - Packet Category
  - Private = 12 (dCH)
</no-stage>

### Format ID 1
- **Packet ID**: 6
- **Packet Seq;Cntrl**: 7
- **Packet Length**: 8

### Format ID 2
- **Packet ID**: 8
- **Packet Seq;Cntrl**: 45
- **Packet Length**: 46

### User Command Field
- User Command Field (≤38 words)

### Application Data
- User Command Word Count
- Visible flag
- Extension flag
- Visible flag
- Extension flag
- Visible flag
- Extension flag
- Visible flag
- Extension flag
- Visible flag
- Extension flag
- Visible flag
- Extension flag

### ESS generated CRC
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)
    (RelTtagTCs -> AbsTtagTCs for Lander)
Parameter Tables structures and links

CDMS Parameter Tables
- CDMS HW Config. Table
- Basic Mission Prms.
- Units Admin. Prms.
- Units Priority Order Tbl.
- PSS/TCU Prms.
- TCUs Set-points

AMSTs List
- AMST-0 / Item1 Points to AMDT-0
  Termination: TC
- AMST- x / Item1 Points to AMDT- k
  Termination: Time|Even|TC
- AMST- x / Item2 Points to AMDT- l
  Termination: Time|Even|TC
- AMST- x / Item3 Points to AMDT- m
  Termination: Time|Even|TC
- AMST- x / ItemN Points to AMDT- k
  Termination: Time|Even|TC
- AMST-y / Item1 Points to AMDT- z
  Termination: Time|Even|TC
- AMST-y / Item2 Points to AMDT- m
  Termination: Time|Even|TC
- AMST-z / Item1 Points to AMDT- z
  Termination: Time|Even|TC
- AMST-z / ItemS Points to AMDT-f
  Termination: Time|Event|TC

AMDTs List
- AMDT-0 Units on: TCU
- AMDT-k Units on: ....
- AMDT-l Units on: ....
- AMDT-m Units on: ....
- AMDT-z Units on: ....

RTTCs List
- Unit-a, Timing Contents: Pointer to STCB
  Attached to: AMDT-m
- Unit-a, Timing Contents: Pointer to STCB
  Attached to: AMDT-f
- Unit-c, Timing Contents: Pointer to STCB
  Attached to: AMDT-z
- Unit-c, Timing Contents: Pointer to STCB
  Attached to: AMDT-k
- Unit-b, Timing Contents: Pointer to STCB
  Attached to: AMDT-k
- Unit-b, Timing Contents: Pointer to STCB
  Attached to: AMDT-z
- Unit-b, Timing Contents: Pointer to STCB
  Attached to: AMDT-d

STCB Buffer
- For Unit-a
- For Unit-b
- For Unit-c
- For Unit-N
Multitasking CDMS SW

CDMS On-board Software Task Activation Flow

1. Boot Program
   - Code Source Selection: Code out of PROM
   - Code out of PROM-Patch(es)
   - Code out of EEPROM

2. TEST_Task
   - Code out of PROM
   - Code out of PROM-Patch(es)
   - Code out of EEPROM

3. AMST_Task
   - AMDT change ?
   - TC Time-tag queue ?
   - Flag ?
   - TCBUFRDY
   - True from Pre-separation to Post-landing

4. ADS_Task
   - Executive

5. PWTH_Task
   - Flag ?
   - ONOFFCHG
   - Battcharging ?
   - Conditioning ?

6. EXP_Task
   - Flag ?
   - UNA, TMA
   - TCB, BAK
   - SSS
   - HK ?
   - Science ?
   - ServiceRQ ?
   - OB Time ?

7. RDM_Task
   - Receive Context from Primary
   - Send Context to Secondary

8. TCTM_Task
   - TM (MM) Session ?

9. EXECUTOR
   - Executive

10. DPU Crash
    - True from Pre-separation to Post-landing

11. CPU Reset
    - SW Crash

12. Boot Program
    - Redundancy Manager Task

13. Priority?
    - Yes
    - Executive

14. irq
    - No
    - IRQ

15. Flag?
    - ONOFFCHG
    - True from Pre-separation to Post-landing

16. True from Pre-separation to Post-landing
    - Yes
    - Executive

17. True from Pre-separation to Post-landing
    - No
    - IRQ

18. Primary DPU?
    - No
    - IRQ
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 Sequences)** ... 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 question marks 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