MODEL-BASED TECHNIQUES FOR SPACE MICROCONTROLLER APPLICATIONS

Steve Duncan

MBSE 2020

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

INTRODUCTION

- Rad-hard mixed-signal microcontrollers promise to have the same effect on the space industry as their predecessors did on terrestrial industries
- Component count, board space, power consumption, cost are all improved
- Microcontroller code is usually simple and repetitive, but the complexity of the interaction between the increased number of devices creates a new challenge
- Failure rates that are acceptable in terrestrial applications are unacceptable in avionics and space
- This is especially true of command & control protocols, which may contain hidden defects
- A way is needed to analyse and manage complexity through the design, development and qualification process

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

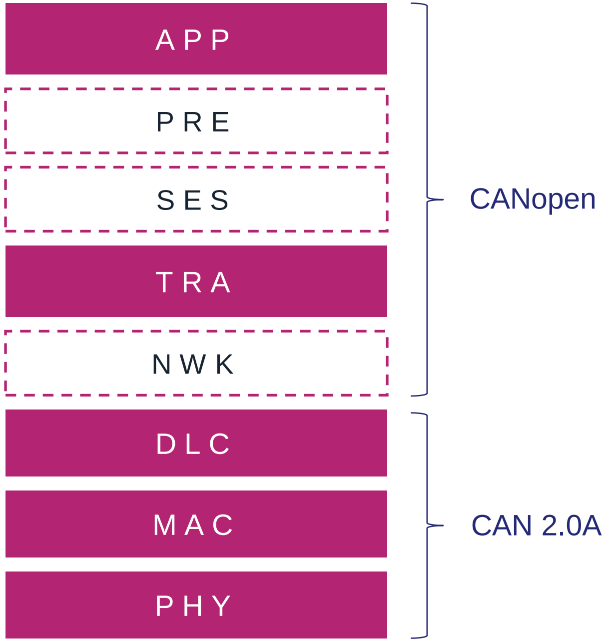
MIXED-SIGNAL MICROCONTROLLERS

	GR716	DPC	SAMV71Q21RT
Manufacturer	Cobham Gaisler	Thales Alenia Space	Microchip
CPU	LEON	MSP430	Cortex M7
Word size	32	16	32
Clock	50 MHz	40 MHz	300 MHz
Cores	1	3	1
Endianism	big	little	little
Program/Data RAM (kB)	128 / 64	28 / 14	384
PROM	-	-	2MB
ADC	2 x 11 bit	4 x 13 bit	2 x 12 bit
DAC	4 x 12 bit	3 x 12 bit	2 x 12 bit
Mil-1553B	✓	✓	✗
CANbus	✓	✓	✓
SpaceWire	✓	✗	✗
Radiation class	Rad-hard	Rad-hard	Rad-tolerant
FM availability	TBC	✓	✓

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

CANOPEN

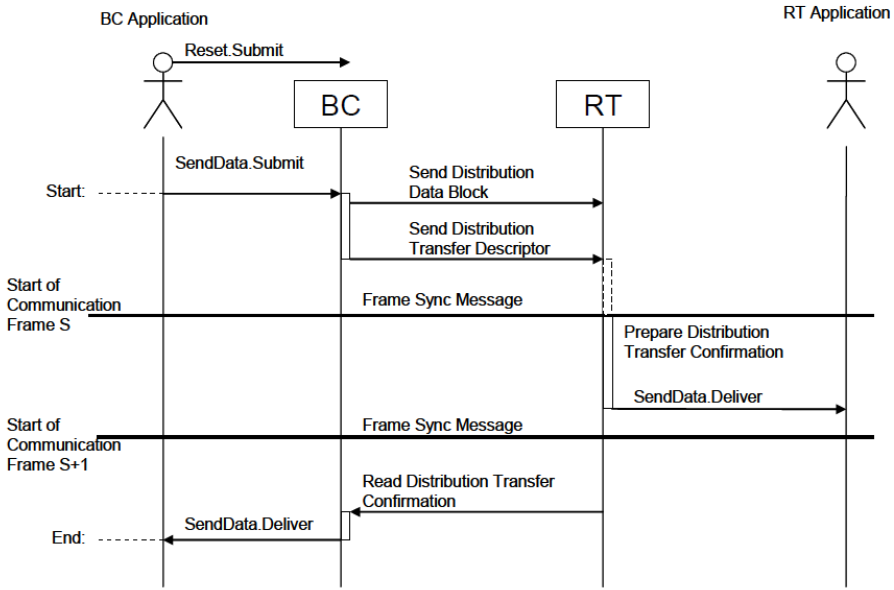
- CANopen is a higher layer protocol for CANbus
  - **Based on CAN 2.0A media layers**
- Transport Layer
  - **Segmented message transfer (SDO)**
- Application Layer
  - **Object Dictionary**
- Tailored for space applications in ECSS-E-ST-50-15C
  - **Redundant bus management**
  - **Optional subset for simple terminals**
- Implements a Master-servant communication model
  - **One node is in control of the bus (usually the OBC)**



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

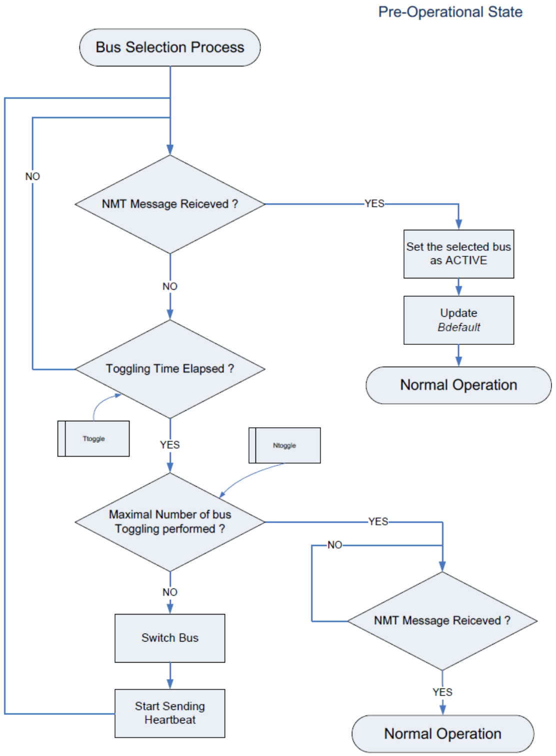
DESCRIBING PROTOCOLS

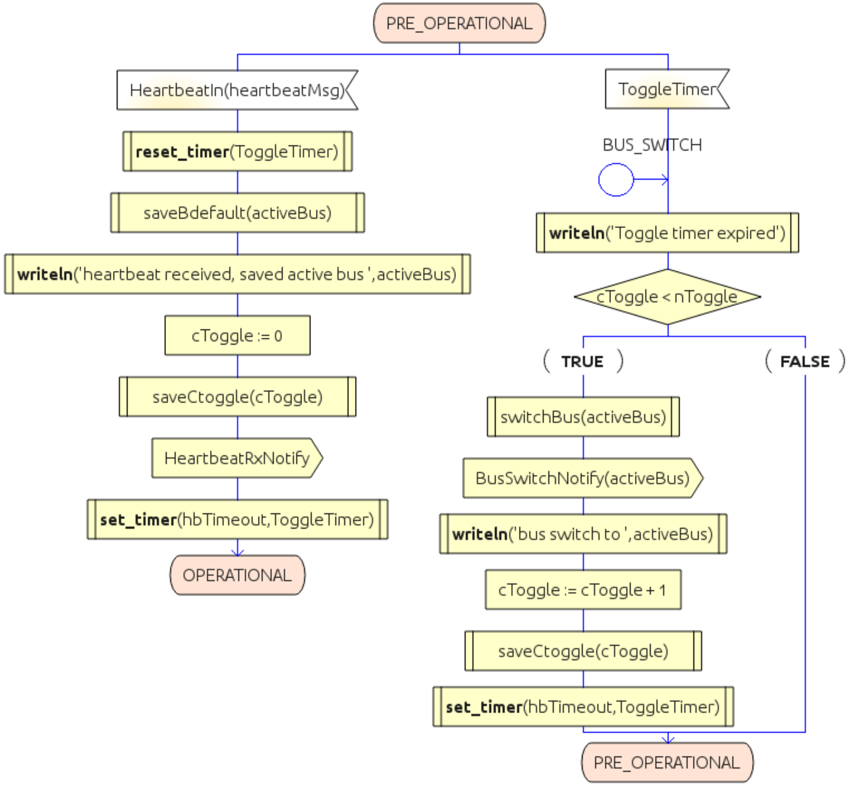
- Onboard protocol specifications are generally expressed in natural language
  - **ECSS series**
  - **CANopen**
  - **Mil-1553B**
- Augmented by MSCs
  - **Good for showing nominal path**
  - **Poor at showing recovery paths**
  - **Poor at exposing protocol flaws**
- Considerable scope for differences in interpretation of the specification
  - **Often discovered late in the cycle**



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

BEHAVIOURAL MODELLING IN SDL



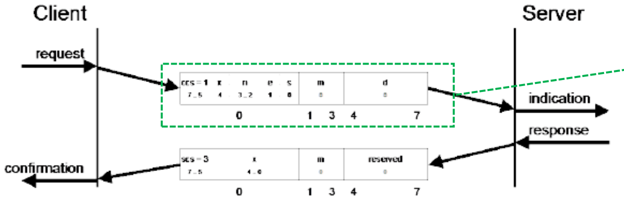


Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

DATA MODELLING IN ASN.1

7.2.4.3.3 Protocol SDO download initiate

The protocol as defined in Figure 21 shall be used to implement the SDO download initiate service.



- **ccs: client command specifier**
  1: initiate download request
- **scs**: server command specifier
  3: initiate download response
- **n**: Only valid if e = 1 and s = 1, otherwise 0. If valid it indicates the number of bytes in d that do not contain data. Bytes [8-n, 7] do not contain data.
- **e**: transfer type
  0: normal transfer
  1: expedited transfer
- **s**: size indicator
  0: data set size is not indicated
  1: data set size is indicated
- **m**: multiplexer. It represents the index/sub-index of the data to be transfer by the SDO.
- **d**: data
  e = 0, s = 0: d is reserved for further use.
  e = 0, s = 1: d contains the number of bytes to be downloaded.
  Byte 4 contains the LSB and byte 7 contains the MSB.
  e = 1, s = 1: d contains the data of length 4-n to be downloaded,
  the encoding depends on the type of the data referenced by index and sub-index
  e = 1, s = 0: d contains unspecified number of bytes to be downloaded
- **x**: not used, always 0
- **reserved**: reserved for further use, always 0

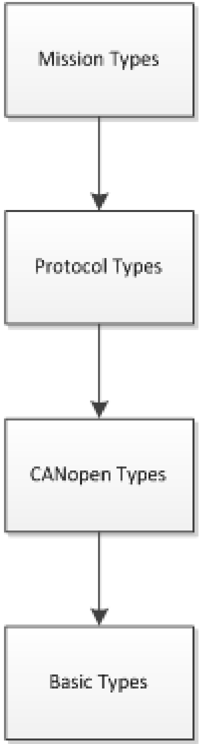
```
T-CANopen-SDO-DownloadInitiate ::= SEQUENCE {
    commandByte    T-CANopen-SDO-DownloadInitiateCommandByte,
    odIndex        T-CANopen-ObjectDictionary-Index,
    odSubIndex     T-CANopen-ObjectDictionary-SubIndex,
    payload        T-CANopen-SDO-DownloadInitiate-Payload
}
```

```
T-CANopen-SDO-DownloadInitiateCommandByte ::= SEQUENCE {
    ccs            T-CANopen-SDO-ClientCommandSpecifier (download-initiate),
    x              UINT1   (0),
    n              UINT2      ,
    e              UINT1      ,
    s              UINT1
}

T-CANopen-SDO-ClientCommandSpecifier ::= ENUMERATED {
    download-segment  (0),
    download-initiate (1),
    upload-initiate   (2),
    upload-segment    (3),
    transfer-abort    (4),
    block-upload      (5),
    block-download    (6),
    reserved          (7)
}
```

```
T-CANopen-SDO-DownloadInitiate-Payload ::= CHOICE {
    segmentedDownloadSize      T-CANopen-ObjectRawDataSize,
    expeditedData              T-CANopen-SDO-GenericPayload
}
```


Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

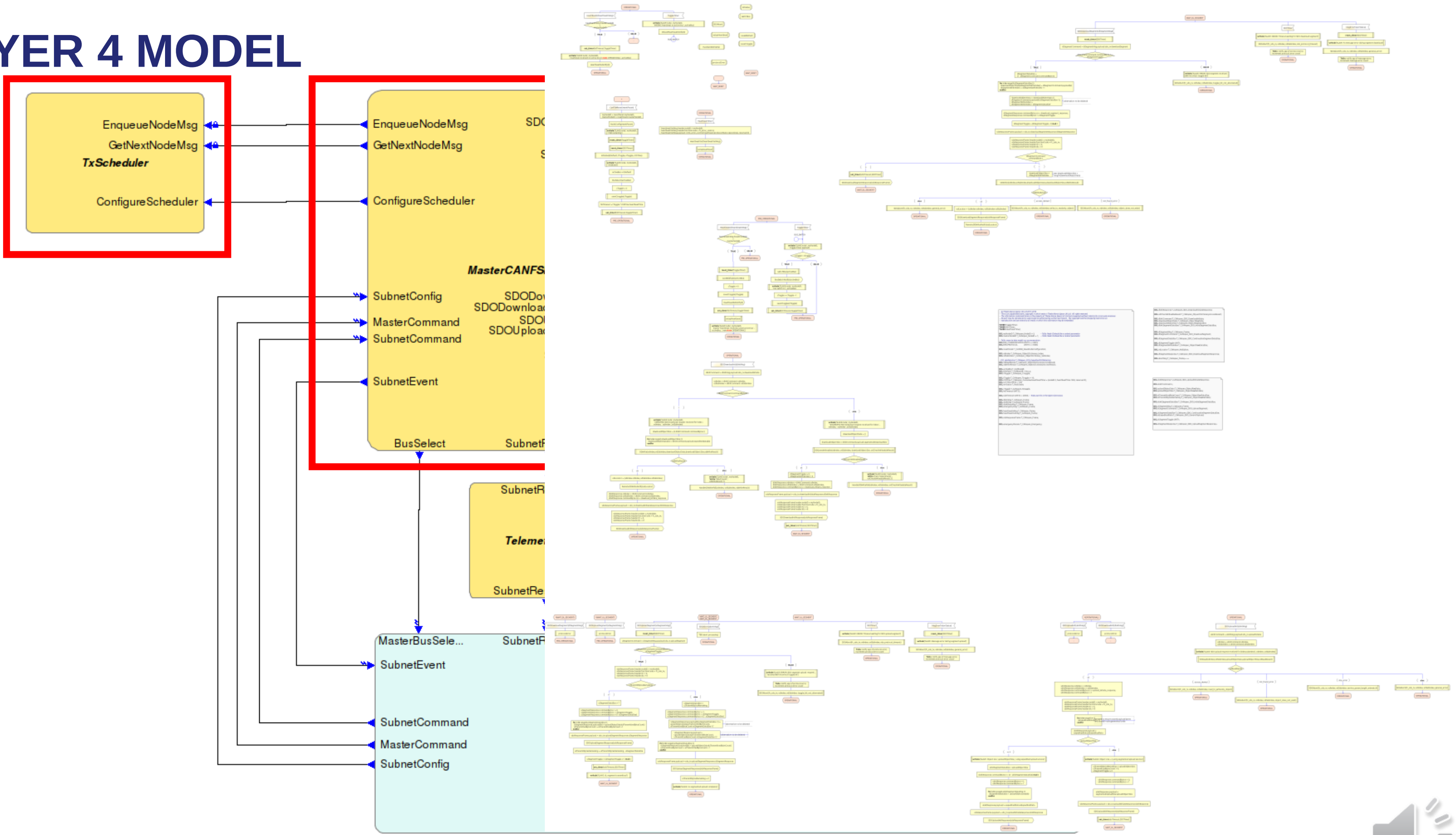
HIERARCHICAL DATA MODEL




```
T-MTCS-ADCToVoltageCalibration         ::= REAL32 (0.0 .. 1000.0)

T-MTCS-ThermistorSteinhartCoefficientA ::= REAL32 (0.0 .. 1.0)
T-MTCS-ThermistorSteinhartCoefficientB ::= REAL32 (0.0 .. 1.0)
T-MTCS-ThermistorSteinhartCoefficientC ::= REAL32 (0.0 .. 1.0)

T-MTCS-ThermistorCalibrationPolynomialCoefficient  ::= REAL32 (-10.0 .. 10.0)

T-MTCS-ThermistorCalibrationPolynomial ::= SEQUENCE (SIZE(3)) OF T-MTCS-ThermistorCalibrationPolynomialCoefficient

T-MTCS-ThermistorReferenceVoltage  ::= REAL32(1.0 .. 12.0)
T-MTCS-ThermistorBridgeResistance  ::= REAL32(1.0 .. 100000.0)

c-MTCS-THERMISTOR-REFERENCE-VOLTAGE REAL ::= 5.0
c-MTCS-THERMISTOR-BRIDGE-RESISTANCE REAL ::= 18000.0

T-MTCS-ThermistorCalibration ::= SEQUENCE {
  adcToVoltage       T-MTCS-ADCToVoltageCalibration,
  refVoltage         T-MTCS-ThermistorReferenceVoltage,
  bridgeResistance   T-MTCS-ThermistorBridgeResistance,
  steinhartA         T-MTCS-ThermistorSteinhartCoefficientA,
  steinhartB         T-MTCS-ThermistorSteinhartCoefficientB,
  steinhartC         T-MTCS-ThermistorSteinhartCoefficientC,
  polynomial         T-MTCS-ThermistorCalibrationPolynomial
}
```

```
T-CANopen-SDO-DownloadInitiate ::= SEQUENCE {
  commandByte    T-CANopen-SDO-DownloadInitiateCommandByte,
  odIndex        T-CANopen-ObjectDictionary-Index,
  odSubIndex     T-CANopen-ObjectDictionary-SubIndex,
  payload        T-CANopen-SDO-DownloadInitiate-Payload
}

T-CANopen-SDO-DownloadInitiateResponse ::= SEQUENCE {
  commandByte    T-CANopen-SDO-DownloadInitiateResponseCommandByte,
  odIndex        T-CANopen-ObjectDictionary-Index,
  odSubIndex     T-CANopen-ObjectDictionary-SubIndex,
  payload        T-CANopen-SDO-GenericPayload
}
```

LAYER 4 MODEL



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

OBJECT DICTIONARY REPRESENTATION

- OD contains three classes of object
  - **CANopen mandatory elements**
    - Heartbeat parameters
    - ST-50-15C extensions
      - Bus selection parameters
  - **Additional protocol elements**
    - Onboard protocol extensions
  - **Mission-specific protocol elements**
    - TM/TC parameters
- OD also serves as the data pool for the unit

```
T-CANopen-ObjectDescriptor ::= SEQUENCE {
  objectName     T-CANopen-ObjectName                     OPTIONAL,
  odIndex        T-CANopen-ObjectDictionary-Index,
  odSubIndex     T-CANopen-ObjectDictionary-SubIndex,
  objectCode     T-CANopen-ObjectCode                     DEFAULT var,
  dataType       T-CANopen-ObjectDictionary-DataType      OPTIONAL,
  category       T-CANopen-ObjectDictionary-Category      OPTIONAL,
  accessType     T-CANopen-ObjectDictionary-Access        OPTIONAL
}
```

```
T-CANopen-ObjectDictionary-ObjectDataType ::= CHOICE {
  arrayHeader                        T-CANopen-ArrayHeader,
  recordHeader                       T-CANopen-RecordHeader,
  chbTime                            T-CANopen-ConsumerHeartbeatTime,
  phbTime                            T-CANopen-ProducerHeartbeatTime,
  bDefault                           T-CANopen-Bdefault,
  tToggle                            T-CANopen-Ttoggle,
  nToggle                            T-CANopen-Ntoggle,
  cToggle                            T-CANopen-Ctoggle
}
```

```
T-Node-ObjectDictionary-ObjectDataType ::= CHOICE {
  canopenObject      T-CANopen-ObjectDictionary-ObjectDataType,
  protocolObject     T-CANOB-ObjectDictionary-ObjectDataType,
  applicationObject  T-MySubsystem-ObjectDictionary-ObjectDataType
}
```

```
T-Node-ObjectDictionary-Entry ::= SEQUENCE {
    descriptor       T-CANopen-ObjectDescriptor,
    objectData       T-Node-ObjectDictionary-ObjectDataType OPTIONAL
}
```


Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

OBJECT DICTIONARY INSTANTIATION

```
c-MTCS-ObjectDictionary T-MTCS-ObjectDictionary ::= {

-- CANopen mandatory entries
  {descriptor {odIndex 4118, odSubIndex 0,  accessType rw, objectCode array,  objectName "{CANopen Consumer Heartbeart Management}"},
   objectData canopenObject:arrayHeader:{dataType unsigned32, numElements 1}},
  {descriptor {odIndex 4118, odSubIndex 1,  accessType rw, objectCode var, dataType unsigned32},
   objectData canopenObject:chbTime:{nodeID 1, heartbeatTime 5000}},
  {descriptor {odIndex 4119, odSubIndex 0,  accessType rw, objectCode var, dataType unsigned16, objectName "{CANopen Producer Heartbeart Management}"},
   objectData canopenObject:phbTime:5000},
```

```
-- Manufacturer-specific area (0x2000 = 8192, first index reserved by ST-50-15C
  {descriptor {odIndex 8192, odSubIndex 0,  accessType ro, objectCode record, objectName "{ECSS E-ST-50-15C Redundancy Management}"},
   objectData canopenObject:recordHeader:{numElements 4}},
  {descriptor {odIndex 8192, odSubIndex 1,  accessType rw, objectCode var, dataType unsigned8},
   objectData canopenObject:bDefault:bus-a},
  {descriptor {odIndex 8192, odSubIndex 2,  accessType rw, objectCode var, dataType unsigned8},
   objectData canopenObject:tToggle:10},
  {descriptor {odIndex 8192, odSubIndex 3,  accessType rw, objectCode var, dataType unsigned8},
   objectData canopenObject:nToggle:10},
  {descriptor {odIndex 8192, odSubIndex 4,  accessType rw, objectCode var, dataType unsigned8},
   objectData canopenObject:cToggle:0},
```

```
-- Protocol counters
  {descriptor {odIndex 8193, odSubIndex 0,  accessType ro, objectCode record, objectName "{Protocol Packet and Error Counters}"},
   objectData canopenObject:recordHeader:{numElements 10}},
  {descriptor {odIndex 8193, odSubIndex 1,  accessType ro, objectCode var, dataType unsigned32},   objectData protocolObject:rxSDOCounter:0},
  {descriptor {odIndex 8193, odSubIndex 2,  accessType ro, objectCode var, dataType unsigned32},   objectData protocolObject:txSDOCounter:0},
  {descriptor {odIndex 8193, odSubIndex 3,  accessType ro, objectCode var, dataType unsigned32},   objectData protocolObject:rxSyncCounter:0},
  {descriptor {odIndex 8193, odSubIndex 4,  accessType ro, objectCode var, dataType unsigned32},   objectData protocolObject:rxHeartbeatCounter:0},
  {descriptor {odIndex 8193, odSubIndex 5,  accessType ro, objectCode var, dataType unsigned32},   objectData protocolObject:txHeartbeatCounter:0},
```

```
-- Application-specific area
  {descriptor {odIndex c-MTCS-ODINDEX-NODETEMP, odSubIndex 0, accessType ro, objectCode array, objectName "{Thermal Node Temperature}"},
   objectData canopenObject:arrayHeader:{dataType real32, numElements c-MTCS-NUM-THERMAL-NODES-PER-MICRONODE}},
  {descriptor {odIndex c-MTCS-ODINDEX-NODETEMP, odSubIndex 1, accessType ro, objectCode var,  dataType real32},
   objectData applicationObject:thermalNodeTemperature:0.0},
  {descriptor {odIndex c-MTCS-ODINDEX-NODETEMP, odSubIndex 2, accessType ro, objectCode var,  dataType real32},
   objectData applicationObject:thermalNodeTemperature:0.0},
  {descriptor {odIndex c-MTCS-ODINDEX-NODETEMP, odSubIndex 3, accessType ro, objectCode var,  dataType real32},
   objectData applicationObject:thermalNodeTemperature:0.0},
```


Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

TELEMETRY DEFINITIONS

```
-- Telemetry Object 1  Structure Definition
{descriptor {odIndex 9100, odSubIndex 0,  accessType rw, objectCode array, objectName "TM1 Structure Definition"},
 objectData canopenObject:arrayHeader:{dataType unsigned24, numElements 7}},
{descriptor {odIndex 9100, odSubIndex 1,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 9000, odSubIndex 1}},
{descriptor {odIndex 9100, odSubIndex 2,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 9000, odSubIndex 2}},
{descriptor {odIndex 9100, odSubIndex 3,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 9000, odSubIndex 3}},
{descriptor {odIndex 9100, odSubIndex 4,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 8200, odSubIndex 1}},
{descriptor {odIndex 9100, odSubIndex 5,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 8200, odSubIndex 2}},
{descriptor {odIndex 9100, odSubIndex 6,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 8200, odSubIndex 8}},
{descriptor {odIndex 9100, odSubIndex 7,  accessType rw, dataType unsigned24}, objectData applicationObject:multiplex:{odIndex 8200, odSubIndex 9}},

-- Telemetry Object 1 contents
{descriptor {odIndex 9101, odSubIndex 0,  accessType ro, objectCode domain, dataType octet-string, objectName "TM1 Data"},
 objectData applicationObject:telemetryObject:{maxSizeBytes 1024, definitionIndex 9100}},
```

○ TM structure defined in Object Dictionary

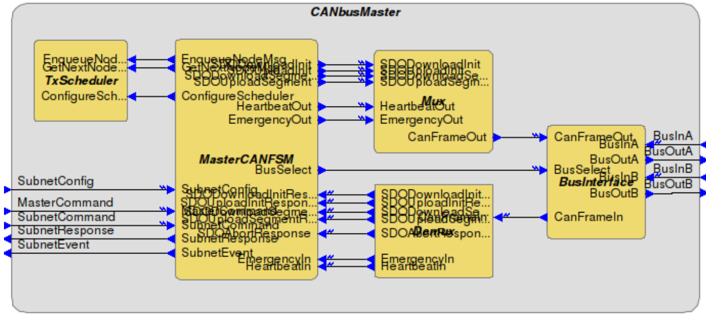
- **Expressed as a combination of other OD entries**
- **Definition is accessible via SDO access**
- **Read-write or read-only**

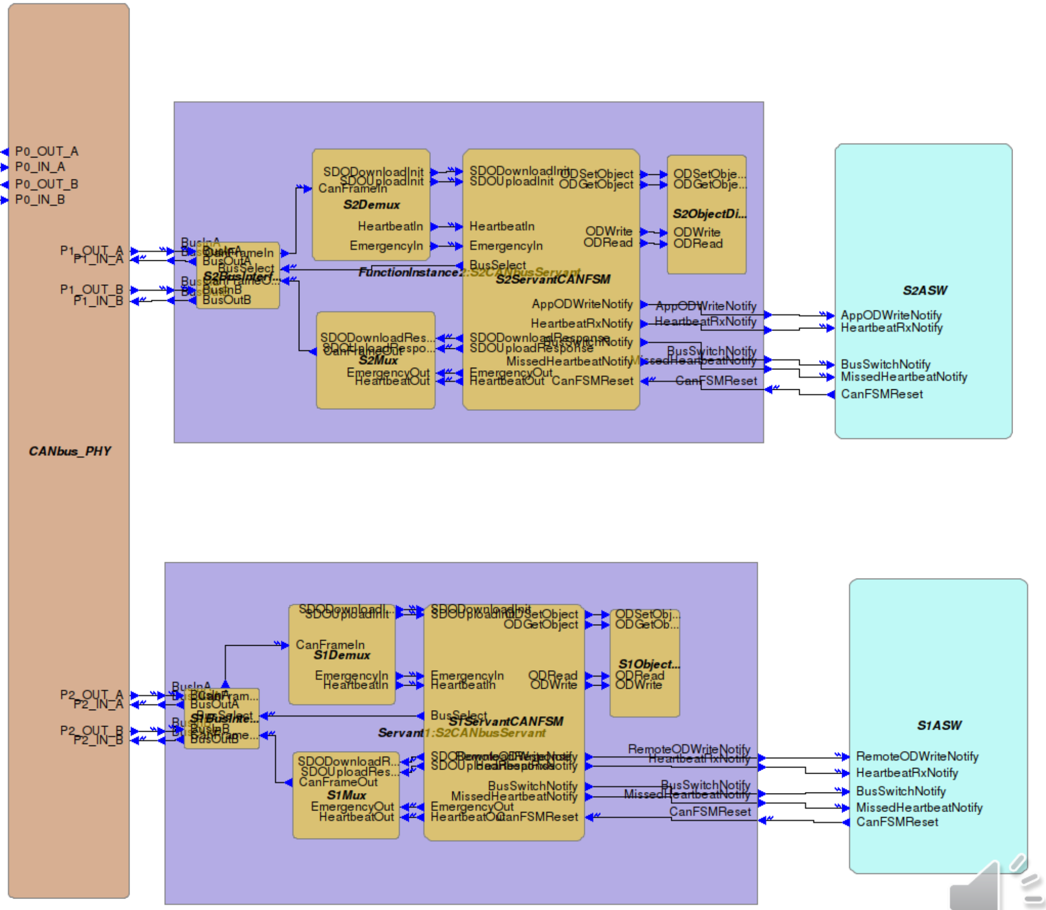
○ TM compiled dynamically when TM object requested

- **OD knows all data types**
- **Optimal packing (e.g. UPER) possible**

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

SYSTEM / LAYER 2 MODEL





- CANbus PHY modelled as TASTE process
  - **Can introduce message errors under control of the test system**
  - **Message loss**
  - **Message corruption / permutation**
- Forthcoming TASTE improvements will facilitate this
  - **Multiple instantiation of servant nodes**

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

ThalesAlenia Space
a Thales / Leonardo company

MODEL EXECUTION

- Model executed in TASTE VM
  - **Inputs provided via GUI**
  - **Message sequences recorded by TASTE**
  - **Including internal signals**
  - **MSC is editable and executable**

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

SCRIPTING

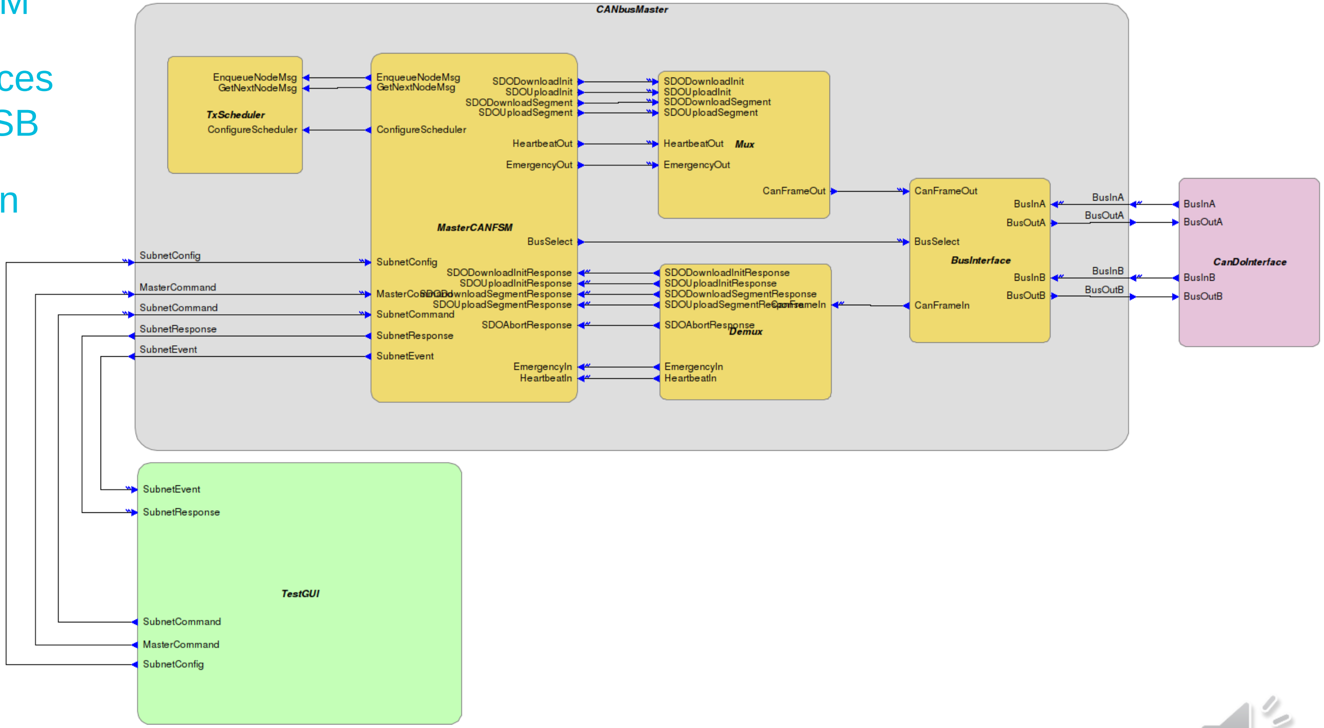
```
@Scenario
def Exercise_startup(queue):
    queue.sendMsg('SubnetConfig', '{nodeCount 1, nodeIDList {5}}', lineNo=24)
    queue.sendMsg('MasterCommand', 'master-reset', lineNo=25)
    try:
        queue.expectMsg('SubnetEvent', 'master-startup', lineNo=26, ignoreOther=False)
    except TypeError as err:
        raise
    try:
        queue.expectMsg('MasterBusSelect', 'bus-a', lineNo=27, ignoreOther=False)
    except TypeError as err:
        raise
    try:
        queue.expectMsg('SubnetEvent', 'master-bus-select', lineNo=28, ignoreOther=False)
    except TypeError as err:
        raise
    queue.sendMsg('CanFSMReset', 'FALSE', lineNo=29)
    try:
        queue.expectMsg('SlaveBusSelect', 'bus-a', lineNo=30, ignoreOther=False)
    except TypeError as err:
        raise
    return 0
```

- Recorded MSCs are available in Python
  - **Converted automatically by TASTE**
  - **Has symbolic access to ASN.1 data model**

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

HARDWARE IN THE LOOP

- CANopen master model executed within TASTE VM
- TASTE component interfaces to physical CANbus via USB
- Basis of phased integration testing
- Also could be used for compliance testing



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

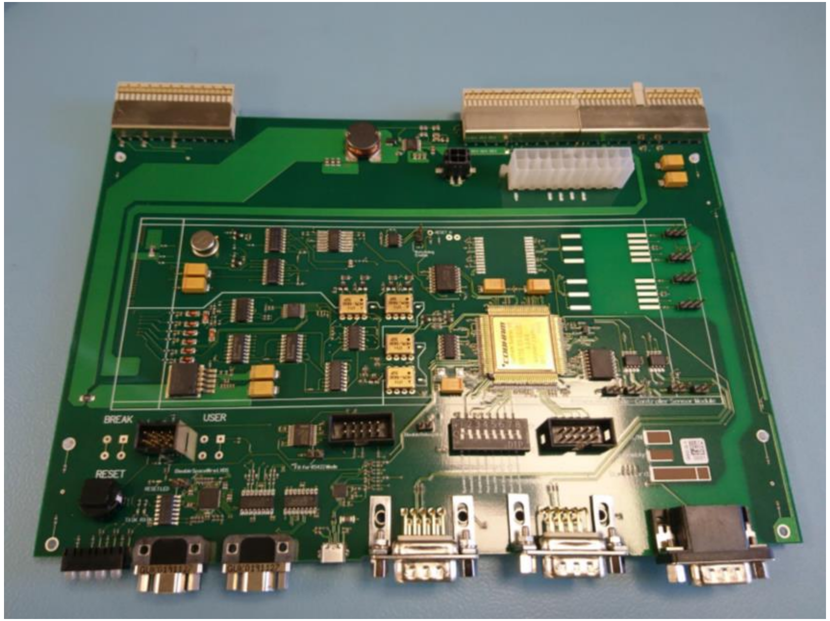
NANOSAT BACKPLANE DEMONSTRATOR

- 2017 UKSA-funded technology fast track project in conjunction with Bright Ascension
  - **CANbus master based on GR712**
  - **Running GenerationOne OBSW**
  - **TMTC interface to mission control SW**
  - **Payload modules based on DPC**
- Heterogeneous architecture
  - **32-bit big-endian (GR712)**
  - **16-bit little-endian (DPC)**
- Thermal control demo application
- Bus redundancy demonstrated
- Object dictionary autogenerated from ASN.1 model
- Simple CANopen stack autogenerated from SDL

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

MICRONODES

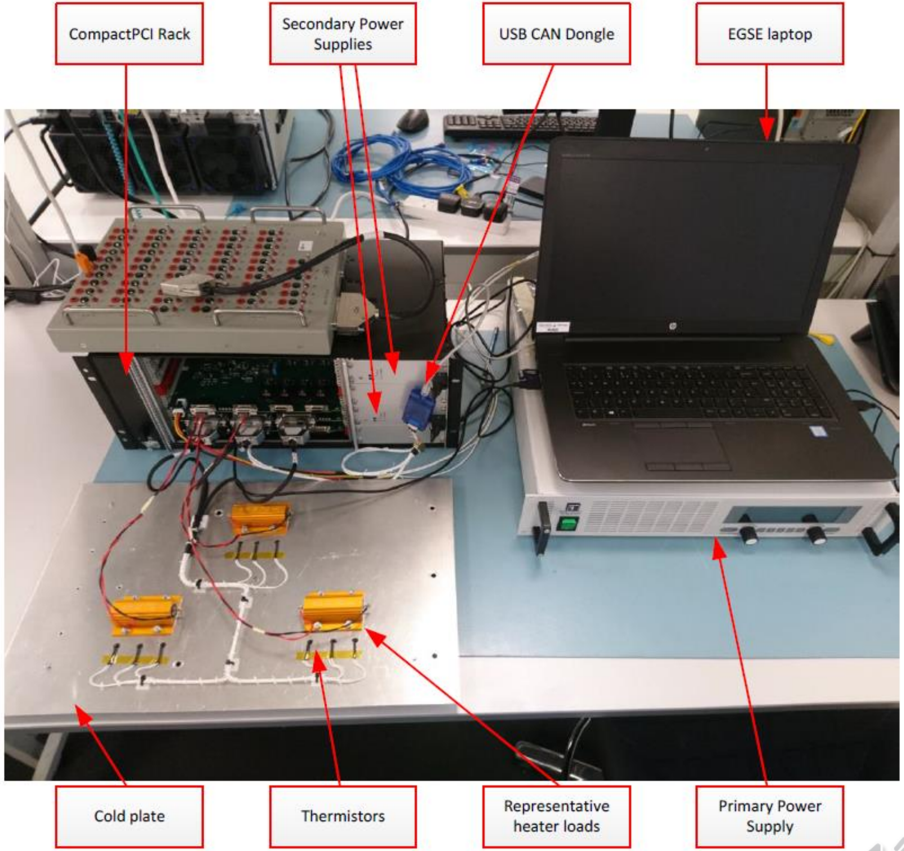
- Breadboard processing module based on Cobham Gaisler GR716
- Separate boards for thermistor acquisition and heater power switching
- CANbus protocol autogenerated from SDL
- Object Dictionary autogenerated from ASN.1
- Thermal control application written in C using structures from ASN.1 data model



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

MICRONODES II

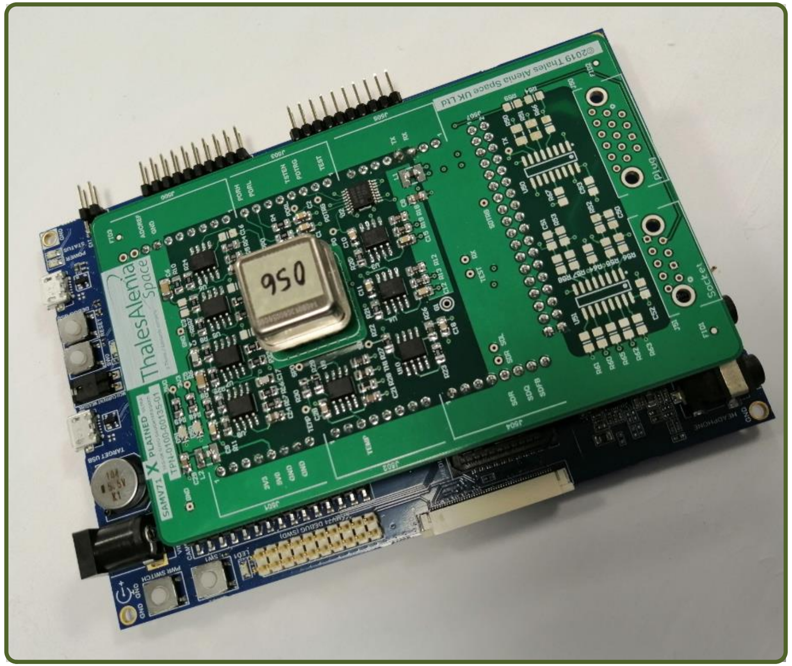
- Breadboard testing conducted using CANbus master SDL model running in TASTE VM on EGSE laptop.
- Suite of tests exercises all transition paths in the CANbus servant FSM
- Test coverage is currently verified manually, by inspection
- For more complex deployments, tool support for test generation is desirable



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

MEMS GYRO

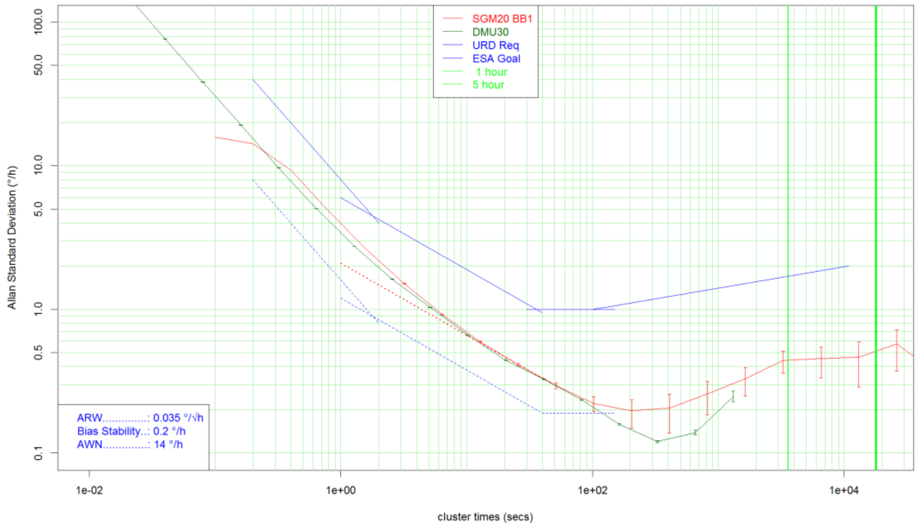
- Based on the Thales Alenia Space NG10 rate gyro
  - **Breadboard developed under ESA contract extension**
  - **Aim is cost reduction for LEO constellations**
- Based on Silicon Sensing SGH-03 MEMS gyro
  - **Operates by exciting the silicon ring with a drive signal coupled to the ring via magnetic actuators**
  - **Secondary vibration mode detected by magnetic pickoffs, proportional to rotation rate**
- Gyro daughterboard made for Atmel EVK.
  - **SAMV71 processor (ARM Cortex M7)**
- Gyro sensing/actuation performed using microcontroller PWM/DAC and ADCs



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

MEMS GYRO II

- Initial version duplicates UART TM/TC interface from NG10
  - **Allows reuse of existing EGSE**
  - **TM/TC and application data models defined in ASN.1**
- Performance closely matches that of the existing FPGA-based implementation
- An EM is in development
- Future EM variant will support CANbus
  - **Same data models and object dictionary used for both versions**
  - **TMs composed from descriptors defined in ASN.1 model**



Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

CONCLUSIONS

- MBSE is highly valuable for microcontroller SW design
- SDL behavioural modelling and ASN.1 data modelling used together give a verifiable route from specification through implementation to validation
- ASN.1 is applicable to the whole application data model, not just for message definitions
- The breadboarding results show us that investment in modularity pays off for models as well as code
- SDL reference models are far superior to paper specifications and indeed could one day replace them
- The analysis of model behaviour is still a manual process, would benefit from tool automation
- We expect to qualify and fly ASN.1 and SDL code derived from TASTE models

Date: 29/09/2020
Ref: TASUK/13679/PRS/007
Template: 83230347-DOC-TAS-EN-006

THANK YOU

stephen.duncan@thalesaleniaspace.com

Date: 29/09/2020
Ref:
Template: 83230347-DOC-TAS-EN-006