Hi-Lite project

ASTRIUM Space Transportation

Presented by David LESENS

29 May 2012

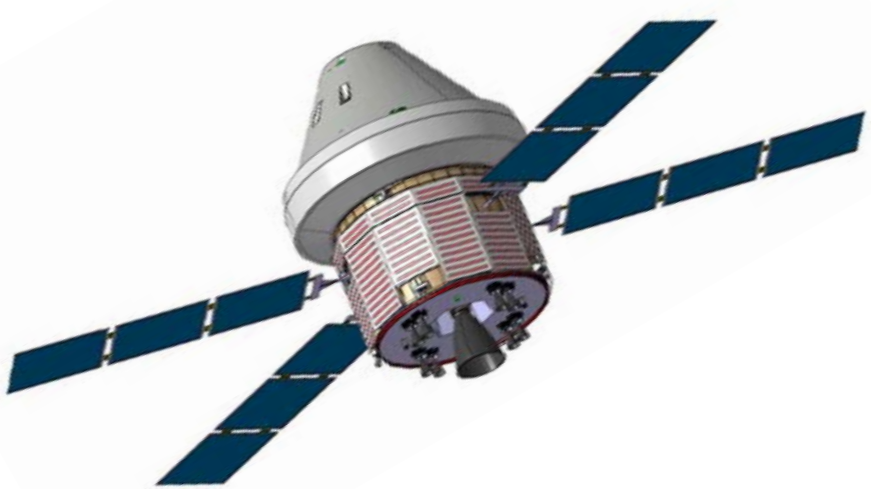
All the space you need

ASTRIUM
AN EADS COMPANY

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Astrium products



ASTRIUM
AN EADS COMPANY

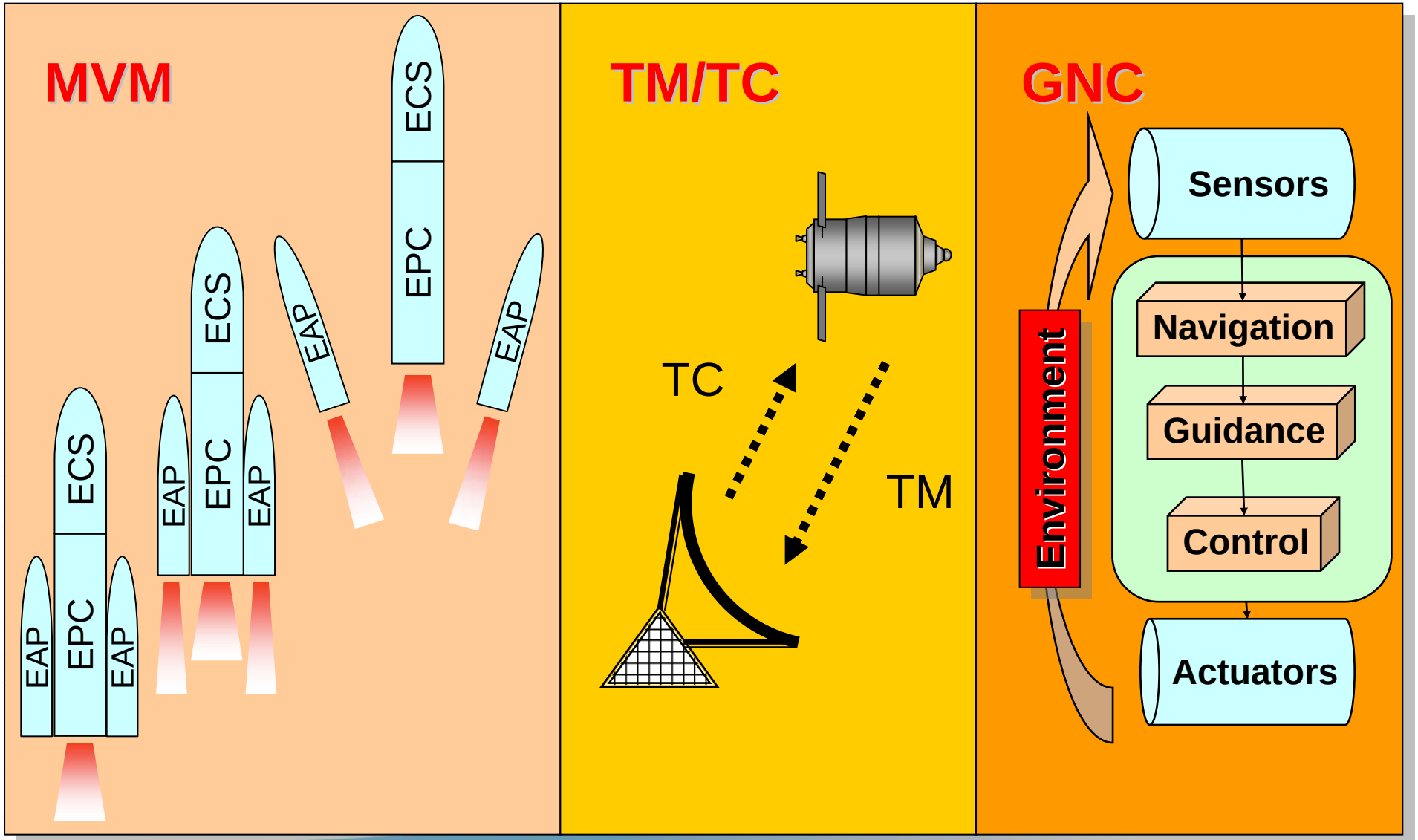
Tools

- GNAT
  - gnatpro-7.1.0w-20120514-45-i686-pc-mingw32-bin.exe
- gnatprove
  - hilite-0.2w-20120514-i686-pc-mingw32-bin.exe
- GPS
  - gps-5.2.0w-20120514-i686-pc-mingw32.exe
- SCADE Suite
  - 6.3.1

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Technical scope of the case study



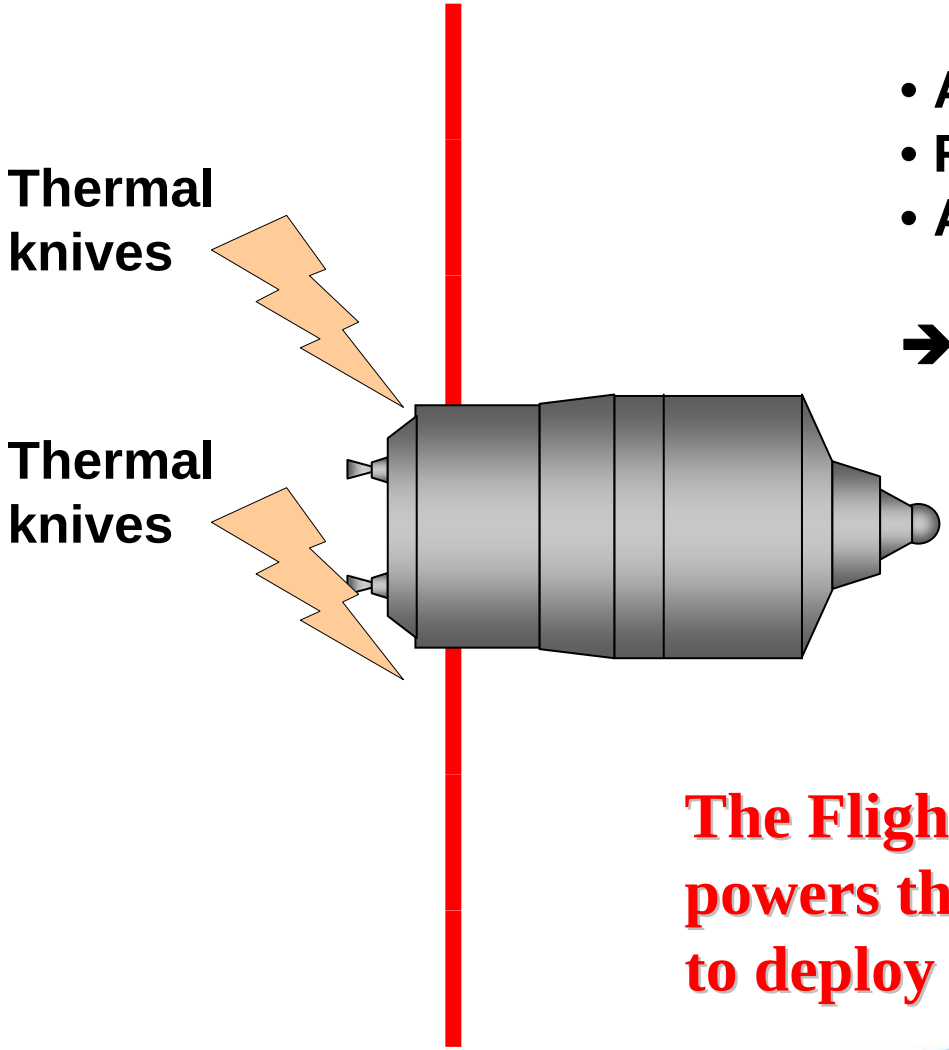
Size of the Astrium case study

```
/HiLite/CASE_STUDY/TMTC/ADA/src
$ find . -name "*.ad[bs]" -exec cat {} \; | wc -l
54610

/HiLite/CASE_STUDY/TMTC/ADA/src
$ find . -name "*.ad[bs]" -exec grep "\;" {} \; | wc -l
12543

/HiLite/CASE_STUDY/TMTC/ADA/testing
$ find . -name "*.ad[bs]" -exec cat {} \; | wc -l
17738

/HiLite/CASE_STUDY/TMTC/ADA/testing
$ find . -name "*.ad[bs]" -exec grep "\;" {} \; | wc -l
5524
```

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Solar wing deployment

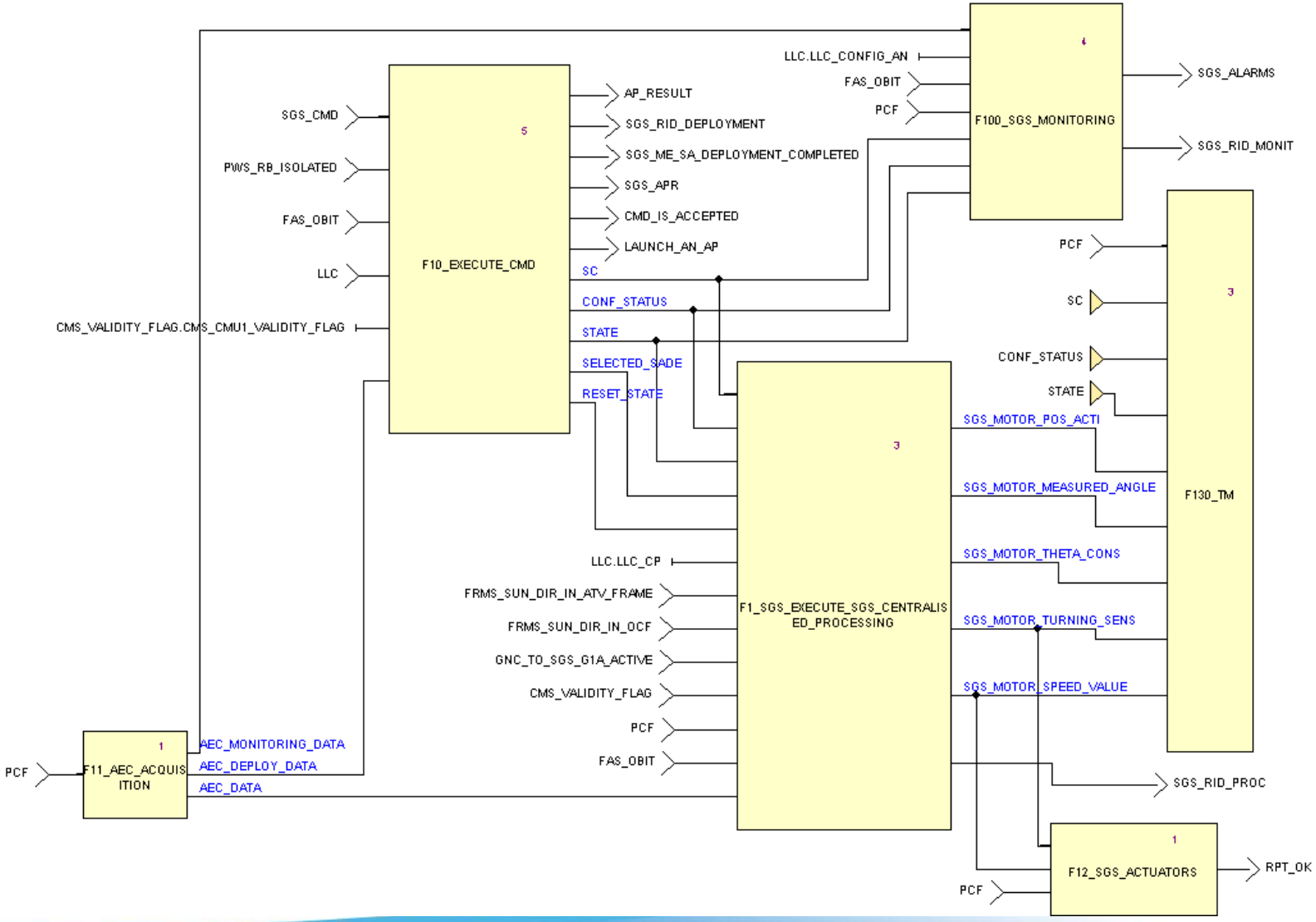


- Acyclic events
- Redundancy (FDIR)
- Automaton oriented

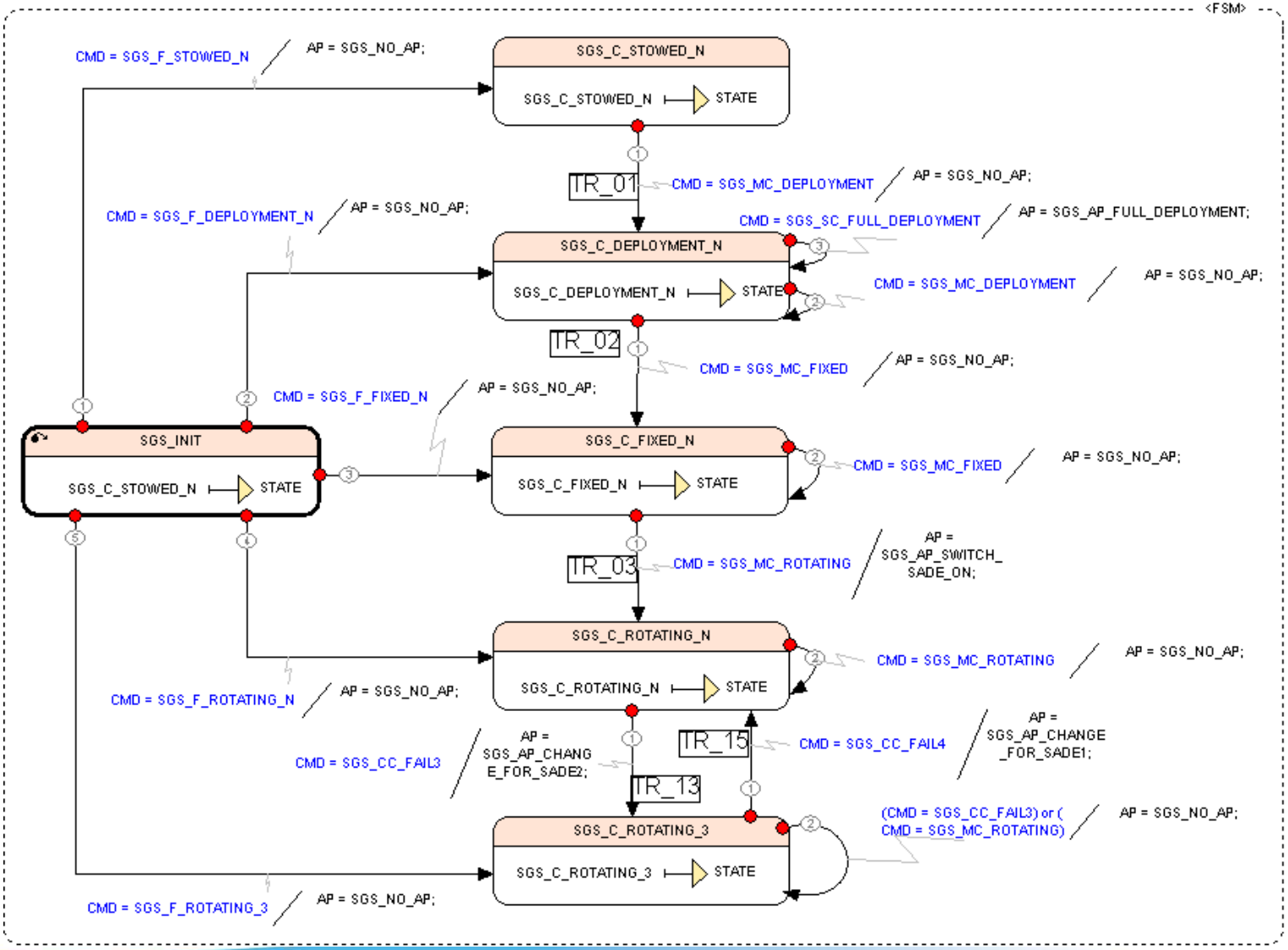
➔ Software part modelled in SCADE

The Flight Application Software powers thermal knives in order to deploy the solar wings

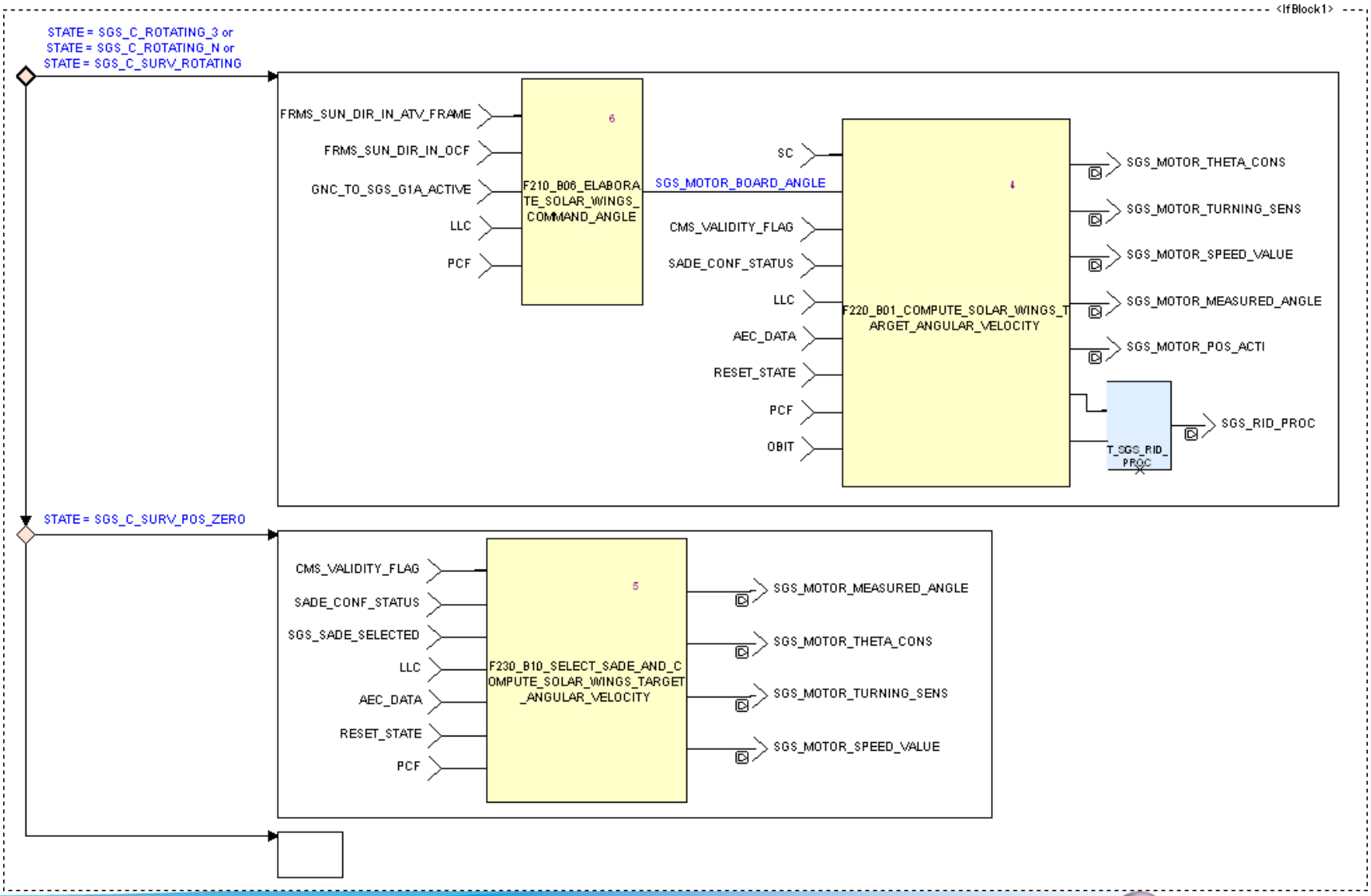
Software architecture in SCADE



Mode automaton



Activation conditions



Automatic generated code

```
begin
  if(Ctx.init_5) then
    SM_FSM_state_sel_1_1 := Kcg_Types.SSM_st_SURVIVAL;
    SM_AP_state_sel_1_1 := Kcg_Types.SSM_st_INIT_2;
    SC_t1_1_1 := P5_SGS_LIB_TYPES.IMPORTED_CONSTANTS.C_D_SC;
    last_RT_INHIBIT_TABLE_1_1 :=
      P5_SGS_LIB_TYPES.MAIN.C_D_SGS_RT_INHIBIT_TABLE;
    last_RT_INHIBIT_EQPT_1_1 := P5_SGS_LIB_TYPES.MAIN.C_D_RT_INHIBIT_EQPT;
    last_ALARM_ID_1_1 := Kcg_Types.NO_ALARM;
  else
    SM_FSM_state_sel_1_1 := Ctx.SM_FSM_state_nxt_1_1;
    SM_AP_state_sel_1_1 := Ctx.SM_AP_state_nxt_1_1;
    SC_t1_1_1 := Ctx.rem_SC;
    last_RT_INHIBIT_TABLE_1_1 := Ctx.RT_INHIBIT_TABLE_1_1;
    last_RT_INHIBIT_EQPT_1_1 := Ctx.RT_INHIBIT_EQPT_1_1;
    last_ALARM_ID_1_1 := Ctx.ALARM_ID_1_1;
  end if;
  case (SM_FSM_state_sel_1_1) is
    when Kcg_Types.SSM_st_SURVIVAL =>
      SM_SGS_SC_FULL_DEPLOYMENT_reset_act_1_1 := ((((SGS_CMD.CMD =
        Kcg_Types.SGS_F_DEPLOYMENT_N) or (SGS_CMD.CMD =
        Kcg_Types.SGS_F_FIXED_N)) or (SGS_CMD.CMD =
        Kcg_Types.SGS_F_ROTATING_3)) or (SGS_CMD.CMD =
        Kcg_Types.SGS_F_ROTATING_N)) or (SGS_CMD.CMD =
        Kcg_Types.SGS_F_STOWED_N);
      tmp_1_4_2 := (((SGS_CMD.CMD = Kcg_Types.SGS_F_SURV_INIT) or
        (SGS_CMD.CMD = Kcg_Types.SGS_F_SURV_ROTATING)) or (SGS_CMD.CMD =
        Kcg_Types.SGS_F_SURV_POS_ZERO)) or (SGS_CMD.CMD =
        Kcg_Types.SGS_F_SURV_FIXED);
      if(SM_SGS_SC_FULL_DEPLOYMENT_reset_act_1_1) then
        SM_FSM_state_act_1_1 := Kcg_Types.SSM_st_NOMINAL;
        L17_2_1_1 := True;
      else
```

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Telemetry / Telecommand

TMTC

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION

ECSS

Space engineering

ECSS-E-70-41A

30 January 2003

Ground systems and operations — Telemetry and telecommand packet utilization

Packet Header (48 Bits)							Packet Data Field (Variable)			
Packet ID				Packet Sequence Control		Packet Length	Data Field Header (Optional) (see Note 1)	Application Data	Spare	Packet Error Control (see Note 2)
Version Number (=0)	Type (=1)	Data Field Header Flag	Applica-tion Process ID	Sequence Flags	Sequence Count					
3	1	1	11	2	14					
16				16		16	Variable	Variable	Variable	16

ASTRIUM AN EADS COMPANY

Structure of telemetry / telecommand packets

```
type T_Packet_ID is
   record
      Version_Number          : T_Version_Number;
      Packet_Type             : T_Packet_Type;
      Data_Field_Header_Flag  : T_Data_Field_Header_Flag;
      Application_Process_Id  : Tmtc.Entities.T_Application_Process_Id;
   end record;
for T_Packet_ID use
   record
      Version_Number          at 0 range 0 .. 2;
      Packet_Type             at 0 range 3 .. 3;
      Data_Field_Header_Flag  at 0 range 4 .. 4;
      Application_Process_Id  at 0 range 5 .. 15;
   end record;
for T_Packet_ID'Size use 16;
```

```
type T_Packet_Header is
   record
      Packet_ID               : T_Packet_ID;
      Packet_Sequence_Control : T_Packet_Sequence_Control;
      Packet_Length           : T_Packet_Length;
   end record;
for T_Packet_Header use
   record
      Packet_ID               at 0 range 0 .. 15;
      Packet_Sequence_Control at 0 range 16 .. 31;
      Packet_Length           at 0 range 32 .. 47;
   end record;
for T_Packet_Header'Size use 48;
```

Verification of telecommand packets

```
procedure Check_Telecommand
  (
   Packet_Header      : in Tmtc.Packet.T_Packet_Header;
   Data_Field_Header  : in T_Data_Field_Header;
   Tc_Error           : out T_Tc_Error
  )
is
   Sequence_Count : Tmtc.Packet.T_Sequence_Count;
begin
   if not Packet_Header.Packet_ID.Version_Number'Valid then
      Tc_Error := Invalid_Version_Number;
   elsif not Packet_Header.Packet_ID.Packet_Type'Valid then
      Tc_Error := Invalid_Packet_Type;
   elsif not ( Packet_Header.Packet_ID.Packet_Type = Tmtc.Packet.Tc_Packet )
   then
      Tc_Error := Invalid_Packet_Type;
   elsif not Packet_Header.Packet_ID.Data_Field_Header_Flag'Valid then
      Tc_Error := Invalid_Data_Field_Header_Flag;
   elsif not          ( Packet_Header.Packet_ID.Data_Field_Header_Flag =
                         Tmtc.Packet.Field_Header_Present ) then
      Tc_Error := Invalid_Data_Field_Header_Flag;
   elsif not Packet_Header.Packet_ID.Application_Process_Id'Valid then
      Tc_Error := Invalid_Application_Process_Id ;
   elsif not Packet_Header.Packet_Sequence_Control.Sequence_Flags'Valid then
      Tc_Error := Invalid_Sequence_Flags;
   elsif not Packet_Header.Packet_Sequence_Control.Sequence_Count'Valid then
      Tc_Error := Invalid_Sequence_Count;
   elsif not Packet_Header.Packet_Length'Valid then
      Tc_Error := Invalid_Packet_Length;
   elsif not
```

Definition of data bus

```
type T_SADE_MOTOR_MOVEMENT_COMMAND is --     5       BC-RT
   record
      MOTOR1_TURNING_SENS : Ml.Bits.T_1Bit;-- MOTOR1_DATA    7       1
      MOTOR1_SPEED_VALUE  : Ml.Bits.T_5Bit;-- MOTOR1_DATA    11      5
      MOTOR2_TURNING_SENS : Ml.Bits.T_1Bit;-- MOTOR2_DATA    23      1
      MOTOR2_SPEED_VALUE  : Ml.Bits.T_5Bit;-- MOTOR2_DATA    27      5
      MOTOR3_TURNING_SENS : Ml.Bits.T_1Bit;-- MOTOR3_DATA    39      1
      MOTOR3_SPEED_VALUE  : Ml.Bits.T_5Bit;-- MOTOR3_DATA    43      5
      MOTOR4_TURNING_SENS : Ml.Bits.T_1Bit;-- MOTOR4_DATA    55      1
      MOTOR4_SPEED_VALUE  : Ml.Bits.T_5Bit;-- MOTOR4_DATA    59      5
   end record;
for T_SADE_MOTOR_MOVEMENT_COMMAND use
   record
      MOTOR1_TURNING_SENS at 0 range 7 .. 7;-- MOTOR1_DATA   7       1
      MOTOR1_SPEED_VALUE  at 1 range 3 .. 7;-- MOTOR1_DATA   11      5
      MOTOR2_TURNING_SENS at 2 range 7 .. 7;-- MOTOR2_DATA   23      1
      MOTOR2_SPEED_VALUE  at 3 range 3 .. 7;-- MOTOR2_DATA   27      5
      MOTOR3_TURNING_SENS at 4 range 7 .. 7;-- MOTOR3_DATA   39      1
      MOTOR3_SPEED_VALUE  at 5 range 3 .. 7;-- MOTOR3_DATA   43      5
      MOTOR4_TURNING_SENS at 6 range 7 .. 7;-- MOTOR4_DATA   55      1
      MOTOR4_SPEED_VALUE  at 7 range 3 .. 7;-- MOTOR4_DATA   59      5
   end record;
```

Access to the data bus

```
-- Access to the bus frame with a Boolean result
procedure Read_Data_Pool_Boolean
  (
   Parameter_Id : in     T_Parameter_Id;
   Read_Value   :    out Boolean;
   Is_Ok        :    out Boolean
  )
with
  Post =>
    ( Is_Ok = ( Parameter_Id = Id_SGS_MOTOR_POS_ACTI_0_POS_ACTI or else
                Parameter_Id = Id_SGS_MOTOR_POS_ACTI_1_POS_ACTI or else
                  Parameter_Id = Id_SGS_MOTOR_POS_ACTI_2_POS_ACTI or else
                    Parameter_Id = Id_SGS_MOTOR_POS_ACTI_3_POS_ACTI )
    )
  and then
    ( if Parameter_Id = Id_SGS_MOTOR_POS_ACTI_0_POS_ACTI then
     Read_Value = DP.Engineering_Data.SGS_MOTOR_POS_ACTI(0).POS_ACTI )
  and then
    ( if Parameter_Id = Id_SGS_MOTOR_POS_ACTI_1_POS_ACTI then
     Read_Value = DP.Engineering_Data.SGS_MOTOR_POS_ACTI(1).POS_ACTI )
  and then
    ( if Parameter_Id = Id_SGS_MOTOR_POS_ACTI_2_POS_ACTI then
     Read_Value = DP.Engineering_Data.SGS_MOTOR_POS_ACTI(2).POS_ACTI )
  and then
    ( if Parameter_Id = Id_SGS_MOTOR_POS_ACTI_3_POS_ACTI then
     Read_Value = DP.Engineering_Data.SGS_MOTOR_POS_ACTI(3).POS_ACTI );
```

Monitoring list

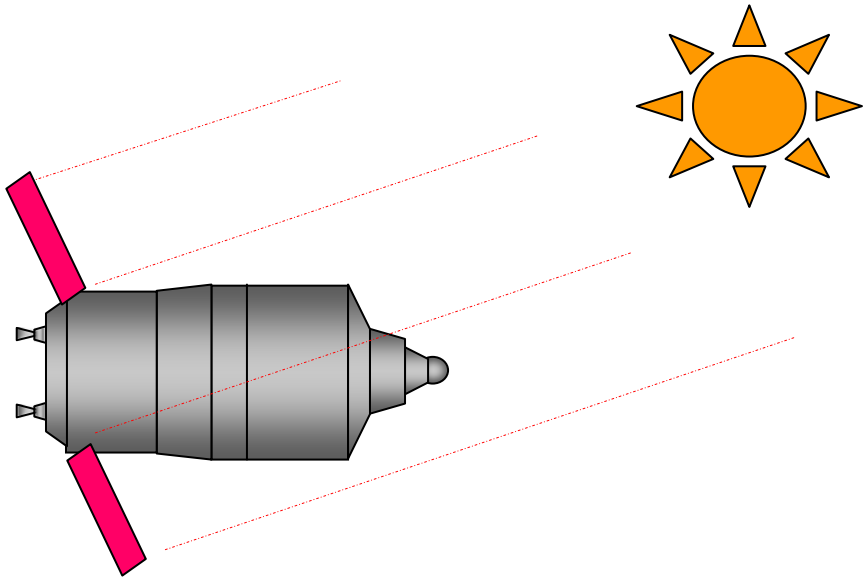
```
type T_Monitored_Parameter
  (Check_Type : T_Check_Type := Limit_Check;
   Parameter_Data_Type : Tmtc.Data_Pool.T_Parameter_Data_Type
   := Tmtc.Data_Pool.Nat32_Type ) is
   record
      -- The identification of the on-board parameter to be monitored
      Parameter_Id : Tmtc.Data_Pool.T_Parameter_Id;
      -- Is the monitoring of the parameter enabled or disabled
      Is_Enabled : Boolean;
      -- The monitoring interval for the parameter
      Monitoring_Interval : T_Monitoring_Interval;
      -- A counter allowing decieding if it is time to monitor the parameter
      -- (depending of the value of Monitoring_Interval)
      Monitoring_Counter : Ml.T_Nat32;
      -- Depending if the nature of the check to be performed
      case Check_Type is
      when Limit_Check =>
         case Parameter_Data_Type is
            when Tmtc.Data_Pool.Boolean_Type =>
               null;
            when Tmtc.Data_Pool.Nat32_Type =>
               Low_Limit_Nat32_Value : Ml.T_Nat32;
               High_Limit_Nat32_Value : Ml.T_Nat32;
            when Tmtc.Data_Pool.Int32_Type =>
               Low_Limit_Int32_Value : Ml.T_Int32;
               High_Limit_Int32_Value : Ml.T_Int32;
            when Tmtc.Data_Pool.Nat64_Type =>
               Low_Limit_Nat64_Value : Ml.T_Nat64;
               High_Limit_Nat64_Value : Ml.T_Nat64;
            when Tmtc.Data_Pool.Int64_Type =>
               Low_Limit_Int64_Value : Ml.T_Int64;
               High_Limit_Int64_Value : Ml.T_Int64;
```

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Algorithms

- Orientation of the ATV solar wings
  - Optimisation of energy



- From SPARK to Alfa

Mathematical library

```
function Sin32 (X : T_Float32) return T_Float32
with
  Pre => ( X >= - C_2Pi32 ) and then
  ( X <= C_2Pi32 ),
Post => ( Sin32'Result >= -1.0 ) and then
  ( Sin32'Result <= 1.0),
Test_Case => (Name     => "-2Pi .. -3Pi/2",
              Mode     => Nominal,
              Requires => X >= -C_2Pi32 and X < -C_3Halfpi32,
              Ensures  => Sin32'Result >= 0.0 and Sin32'Result <= 1.0),
Test_Case => (Name     => "-3Pi/2 .. -Pi",
              Mode     => Nominal,
              Requires => X >= -C_3Halfpi32 and X < -C_Pi,
              Ensures  => Sin32'Result >= 0.0 and Sin32'Result <= 1.0),
Test_Case => (Name     => "-Pi .. -Pi/2",
              Mode     => Nominal,
              Requires => X >= -C_Pi32 and X < -C_HalfPi,
              Ensures  => Sin32'Result >= -1.0 and Sin32'Result <= 0.0),
Test_Case => (Name     => "-Pi/2 .. 0",
              Mode     => Nominal,
              Requires => X >= -C_HalfPi32 and X < 0.0,
```

From SPARK to Ada 2012

```
procedure S_CONV_AND_INCREMENT_ANGLE(INPUT_XSUN    : in  M1.T_FLOAT32;
                                     Angle_Radian : in  M1.T_Angle_HalfPi;
                                     Angle_Degree : out M1.T_Angle_360)
  --# derives Angle_Degree from Angle_Radian,
  --#                           INPUT_XSUN;
  --# pre ( Angle_Radian >= -M1.C_Halfpi32 ) and
  --#     ( Angle_Radian <= M1.C_Halfpi32 );
with Pre =>
  ( Angle_Radian >= -M1.C_Halfpi32 ) and then
  ( Angle_Radian <= M1.C_Halfpi32 );
```

```
function S_COMP_MOTORJ_THETA_POINT_COM_M (SADM_J              : in T_SGS_SADM_ID;
                                          THETA_POINT_COM     : in T_MOTOR_THETA_POINT_Com)
                                          return T_MOTOR_THETA_POINT_Com
--# return MOTJ_THETA_POINT_COM_M => ( ( MOTJ_THETA_POINT_COM_M >= -0.5 ) and
--#                                   ( MOTJ_THETA_POINT_COM_M <= 0.5 ) );
with Post =>
  ( S_COMP_MOTORJ_THETA_POINT_COM_M'Result >= -0.5 ) and
  ( S_COMP_MOTORJ_THETA_POINT_COM_M'Result <= 0.5 );
```

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Mission & Vehicle Management

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

5.2.8 Waits

a. It shall be possible to specify the following types of wait statement within the main body of an OBCP:

1. wait until a given on-board time;
2. wait for a given interval of time to elapse;
3. wait until a given condition becomes true;
4. wait until a given event occurs;
5. wait until any event from a specified list of events occurs.

b. It shall be possible to specify a combination of conditions within a wait statement.

c. The conditions specified for an OBCP precondition or confirmation shall be any combination of the following:

1. wait until a given absolute time;
2. wait for a given interval of time to elapse;
3. wait until a given condition becomes true;
4. wait until a given event occurs;
5. wait until any event from a specified list of events occurs;
6. test whether a given condition is true.

d. It shall be possible to define timeout conditions for wait statements and the behaviour if the timeout is exceeded.

ECSS-E-ST-70-01C
16 April 2010

Space engineering

Spacecraft on-board control procedures

MVM

ASTRIUM
AN EADS COMPANY

Features

- Events
  - Detection, timed windows
- Variables
- Expressions
  - +, -, comparisons…
- Automated procedure
- Onboard mission plan
  - Loop, conditions…
- (Fault Detection) Isolation and Recovery

Example of contract

Example:

- ✓ A list of event detection statuses
- ✓ Request to reset the detection status for Event

```
procedure Reset_Event_Status (Event : in T_Event) with
Post =>
   not Event_Status(Event).Detection and
   (for all Other_Event in T_Event =>
    ( if Other_Event /= Event then
      Event_Status( Other_Event ) = Event_Status'Old( Other_Event ) ));
```

Post-condition

The detection of event is reset

For all other events

The detection status is unchanged

Event1	Event	Event3
Not detected	Not detected	Detected

GPS - (Tmtc project) - mvm-events.ads

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

Scenario
Runtime full

Project
- src\ml
- src\mvm
  - mvm-events.adb
  - mvm-events.ads
  - mvm-expression.a
  - mvm-expression.a
  - mvm-fdir.ads
  - mvm-functional_u
  - mvm-functional_u
  - mvm-obit.adb
  - mvm-obit.ads
  - mvm-omp.adb
  - mvm-omp.ads
  - mvm-types.ads
  - mvm-variable.ads
  - mvm-variables.ad
  - mvm-variables.ad
  - mvm-vehicle_ap.a
  - mvm-vehicle_ap.a
  - mvm.ads

Project | Outline

Y:\HiLite\ADA\src\mvm\mvm-events.ads

```
32
33  generic
34     type T_Event_Id is (<>);
35
36  package Mvm_Events is
37
38     -- The type defining the number of times an event can be detected
39     subtype T_Number_Of_Detection is Ml.T_Nat64;
40
41     type T_Type_Of_Monitoring is
42        (No_Window,
43         Time_Window,
44         Protected_Window);
45
46     type T_Type_Of_Time is
47        (-- The time of the window is in OBIT
48         Absolute_Time,
49         -- The time of the window is relative to an event
50         Relative_To_Event);
51
52     -- The detection status of an event
53     type T_Event_Status
54        (Is_Active          : Ml.T_Boolean          := False;
55         Type_Of_Monitoring : T_Type_Of_Monitoring  := No_Window;
56         Type_Of_Time       : T_Type_Of_Time        := Absolute_Time)
57     is
58        record
59           case Is_Active is
60              when False =>
61                 null;
62              when True =>
63                 -- The number of times the event has been detected
64                 -- in the time window
```

Generic

Discriminant

Insert | Writable | Unmodified | 1:1

Messages | Locations | Call Trees

Contract can be quite big

```
-- Update the status of an event following its detection
procedure Set_Event_Detection (Event_Id      : in     T_Event_Id;
                               Events_Status : in out T_Ev
                               Obit          : in     Mvm

  Post =>
    (case Get_Event_Status(Event_Id,Events_Status).Is_Acti
     when True =>
       (Get_Event_Status(Event_Id,Events_Status).Threshold
          Get_Event_Status(Event_Id,Events_Status'Old).Thr
       (case Get_Event_Status(Event_Id,Events_Status).Type
        when No_Window | Protected_Window =>
        Get_Event_Status(Event_Id,Events_Status).Total_Num
          Get_Event_Status(Event_Id,Events_Status).Total_N
        when Time_Window =>
          (if Is_In_Time_Window(Event_Id,Obit,Events_Statu
           Get_Event_Status(Event_Id,Events_Status).Total_
             Get_Event_Status(Event_Id,Events_Status).Tota
           else
           Get_Event_Status(Event_Id,Events_Status).Total_
             Get_Event_Status(Event_Id,Events_Status).Tota
          )
       ) and then
       (if not Get_Event_Status(Event_Id,Events_Status'Old
          (case Get_Event_Status(Event_Id,Events_Status).T
           when No_Window | Time_Window =>
           Get_Event_Status(Event_Id,Events_Status).Is_Det
           Status(Event_Id,Events_Status).Total
           Status(Event_Id,Events_Status).T
           dow =>
           Obit) < Get_Event_Status(Eve
           Status(Event_Id,Events_Statu
           .Get(Obit) >= Get_Event_Status
           nt_Status(Event_Id,Events_Status).
           Get_Event_Status(Event_Id,Events_Status).
           (Get_Event_Status(Event_Id,Events_Status)
             Get_Event_Status(Event_Id,Events_Sta
          )) and then
       (if not Get_Event_Status(Event_Id,Events_Status'Old
        Get_Event_Status(Event_Id,Events_Status).Is_Detect
        Get_Event_Status(Event_Id,Events_Status).Detection
        Get_Event_Status(Event_Id,Events_Status).Is_Detect
     and then
       (for all Other_Event_Id in T_Event_Id =>
          ( if Other_Event_Id /= Event_Id then
           Get_Event_Status(Other_Event_Id,Events_Status)
             Get_Event_Status(Other_Event_Id,Events_Status
     when False =>
       (for all Other_Event_Id in T_Event_Id =>
        Get_Event_Status(Other_Event_Id,Events_Status) =
          Get_Event_Status(Other_Event_Id,Events_Status'Old) ));
```

spec

```
procedure Set_Event_Detection (Event_Id      : in     T_Event_Id;
                               Events_Status : in out T_Events_Status;
                               Obit          : in     Mvm.Obit.T_Obit) is
   Status : T_Event_Status;
   Numerical_Obit : Mvm.Obit.T_Numerical_Obit;
begin
   Status := Events_Status(Event_Id);
   if Status.Is_Active then
      Numerical_Obit := Mvm.Obit.Get(Obit);
      case Events_Status(Event_Id).Type_Of_Monitoring is
         when No_Window =>
            Status.Total_Number_Of_Detection := Status.Total_Number_Of_Detection + 1;
            if Status.Total_Number_Of_Detection = Status.Threshold_Of_Number_Of_Detection then
               Status.Is_Detected := True;
               Status.Detection_Time := Numerical_Obit;
            end if;
         when Time_Window =>
            if Numerical_Obit >= Status.Start_Window and then
              Numerical_Obit <= Status.End_Window then
               Status.Total_Number_Of_Detection := Status.Total_Number_Of_Detection + 1;
               if Status.Total_Number_Of_Detection = Status.Threshold_Of_Number_Of_Detection then
                  Status.Is_Detected := True;
                  Status.Detection_Time := Numerical_Obit;
               end if;
            end if;
         when Protected_Window =>
            Status.Total_Number_Of_Detection := Status.Total_Number_O
            if Numerical_Obit >= Status.End_Window then
               if not Status.Is_Detected then
                  Status.Is_Detected := True;
                  Status.Detection_Time := Numerical_Obit;
               end if;
            else
               if Numerical_Obit >= Status.Start_Window then
                  if Status.Total_Number_Of_Detection >= Status.Threshold_Of_Number_Of_Detection  and then
                    not Status.Is_Detected then
                     Status.Is_Detected := True;
                     Status.Detection_Time := Numerical_Obit;
                  end if;
               end if;
            end if;
      end case;
      Events_Status(Event_Id) := Status;
   end if;
end Set_Event_Detection;
```

body

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Features not yet supported

```
tmtc-types.ads:35:04: info: enumeration representation clause is not yet supported
...
tmtc-data_pool.adb:394:24: info: attribute is not yet supported
...
tmtc.ads:34:09: info: discriminant is not yet supported
...
ml-bits.adb:25004:44: info: type conversion not between scalar types is not yet supported
...
ml.adb:688:04: warning: in instantiation at a-ngelfu.adb:943
...
sgs-basic_types.ads:108:09: info: array type is not yet supported
...
```

Subprograms in Alfa : 92% (618/669)
... already supported : 88% (586/669)
... not yet supported : 5% (32/669)
Subprograms not in Alfa : 8% (51/669)

Subprograms not in Alfa due to (possibly more than one reason):
exception : 6% (40/669)
unchecked conversion : 1% (10/669)
impure function : 0% (1/669)

Subprograms not yet supported due to (possibly more than one reason):
attribute : 6% (39/669)
conversion : 2% (11/669)
multi dim array : 1% (4/669)
discriminant : 0% (3/669)

Units with the largest number of subprograms in Alfa:
ml-bits : 98% (388/396)
ml : 78% (140/180)
tmtc-data_pool : 96% (47/49)
sgs-main : 100% (14/14)
scade-ln1 : 100% (11/11)
scade-p5_sgs_lib_types-im: 100% (3/3)
(...)

Units with the largest number of subprograms not in Alfa:
ml : 22% (40/180)
ml-bits : 2% (8/396)
tmtc-data_pool : 4% (2/49)
util-time : 100% (1/1)

Warning
Some files are not in this statistic e.g. with discriminant

Compatibility of the case study with Alfa

- Two main features
  - Generic → Implemented
  - Discriminant → To be implemented

- + some other minor features not yet supported

Visibility problematic

- Visibility strategy and proof

```
with M1;
use type M1.T_Nat64;

package Mvm.Obit is

   subtype T_Numerical_Obit is M1.T_Nat64;

   type T_Obit is private;

   -- Return the current OBIT
   function Get(Obit : in T_Obit) return T_Numerical_Obit;

   -- Make the time running, i.e. increment the OBIT
   procedure Run_Time(Obit : in out T_Obit) with
     Post => Get(Obit) >= Get(Obit'Old),
     Test_Case => (Name     => "Test of Run_Time",
                   Mode     => Nominal,
                   Requires => Get(Obit) < T_Numerical_Obit'Last,
                   Ensures  => Get(Obit) = Get(Obit'Old) +1),
     Test_Case => (Name     => "Test of Run_Time with overflow",
                   Mode     => Nominal,
                   Requires => Get(Obit) = T_Numerical_Obit'Last,
                   Ensures  => Get(Obit) = Get(Obit'Old));

private

   type T_Obit is
      record
         Hidden_Obit : T_Numerical_Obit := 0;
      end record;

   -- Return the current OBIT
   function Get(Obit : in T_Obit) return T_Numerical_Obit is (Obit.Hidden_Obit);

end Mvm.Obit;
```

Reading right without writing right

Use in proof

Encapsulated private value

GPS - (Tmtc project) - mvm-events.ads

File Edit Navigate VCS Project Build Debu

Very efficient executable contracts

Scenario
Runtime full

Project

Y:\HiLite\ADA\src\mvm\mvm-ev

```
368   procedure Set_E
369
370
371     Post =>
372       ((Get_Event_Status(Event_Id,Events_Status).Is_Active = Get_Event_Status(Event_Id,Events_Status'Old).Is_Act
373          (Get_Event_Status(Event_Id,Events_Status).Type_Of_Monitoring = Get_Event_Status(Event_Id,Events_Status'
374          (Get_Event_Status(Event_Id,Events_Status).Type_Of_Time = Get_Event_Status(Event_Id,Events_Status'Old).T
375          (case Get_Event_Status(Event_Id,Events_Status).Is_Active is
376           when True =>
377             (Get_Event_Status(Event_Id,Events_Status).Threshold_Of_Number_Of_Detection =
378                Get_Event_Status(Event_Id,Events_Status'
379             (case Get_Event_Status(Event_Id,Events_Stat
380              when No_Window | Protected_Window =>
381              Get_Event_Status(Event_Id,Events_Status).Total_Number_Of_Detection =
382                Get_Event_Status(Event_Id,Events_Status'Old).Total_Number_Of_Detection+1,
383              when Time_Window =>
384                (if Is_In_Time_Window(Event_Id,Obit,Events_Status) then
385                 Get_Event_Status(Event_Id,Events_Status).Total_Number_Of_Detection =
386                   Get_Event_Status(Event_Id,Events_Status'Old).Total_Number_Of_Detection+1
387                 else
388                 Get_Event_Status(Event_Id,Events_Status).Total_Number_Of_Detection =
389                   Get_Event_Status(Event_Id,Events_Status'Old).Total_Number_Of_Detection
390                )
391             ) and then
```

Imprecision of the localisation

Set_Event_Detection | Unknown VCS (Modified) | Insert | Writable | Saved | 375:1

mvm-events.ads | mvm-events.adb | testing.adb | mvm-events_testing.adb

Run: run_tests

```
ERROR Mvm : Test case of Events
    SYSTEM.ASSERTIONS.ASSERT_FAILURE
    Exception Message: failed postcondition from mvm-events.ads:375 instantiated at mvm-events_testing.adb:48
    Traceback:
        0x004E0FC9 system.assertions.raise_assert_failure at s-assert.adb:46
        0x00456144 mvm.events_testing.p_events.set_event_detection at mvm-events.ads:375
        0x00457150 mvm.events_testing.p_events.set_event_detection at mvm-events.adb:102
```

Messages | Locations | Run: run_tests

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

GPS - (Tmtc project) - ml.ads

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.ads

```
58
59    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
60    with
61      Post  => ( ( Sign_Strict_Int32'Result = 1 ) or
62                 ( Sign_Strict_Int32'Result = -1 ) ) and then
63      (if X >= 0 then Sign_Strict_Int32'Result = 1) and then
64      (if X < 0 then Sign_Strict_Int32'Result = -1),
65      Test_Case => (Name     => "Negative input",
66                    Mode     => Nominal,
67                    Requires => X < 0,
68                    Ensures  => Sign_Strict_Int32'Result = -1),
69      Test_Case => (Name     => "Zero input",
70                    Mode     => Nominal,
71                    Requires => X = 0,
72                    Ensures  => Sign_Strict_Int32'Result = 1),
73      Test_Case => (Name     => "Positive input",
74                    Mode     => Nominal,
75                    Requires => X > 0,
76                    Ensures  => Sign_Strict_Int32'Result = 1);
77
78 end Ml;
```

Ml | Insert | Writable | Unmodified | 58:1

ml.ads ml.adb

Messages

Proj

Messages Locations Call Trees

GPS - (Tmtc project) - ml.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.adb

```
22
23    ------------------------------------------------------------------------
24    --
25    -- Integer operations
26    --
27    ------------------------------------------------------------------------
28
29    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
30    is
31       Result : T_Sign_Int32;
32    begin
33       if ( X > 0 ) then
34          Result := 1;
35       elsif ( X < 0 ) then
36          Result := -1;
37       end if;
38       return Result;
39    end Sign_Strict_Int32;
40
41 end ML;
```

ML | Unknown VCS (Modified) | Insert | Writable | Saved | 28:1

ml.ads ml.adb

Messages

```
gnatmake -ws -c -u -PY:\HiLite\TOY11\src\tmtc.gpr ml.adb
gcc -c -gnat12 -I- -gnatA Y:\HiLite\TOY11\src\ml.adb

[2012-05-03 14:45:47] process terminated successfully (elapsed time: 00.73s)
```

Proj

Messages Locations Call Trees

GPS - (Tmtc project) - ml.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Prove All
Prove Root Project
Prove File
Show Unprovable Code

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.adb

```
22
23    ------------------------------------------------------------------------
24    --
25    -- Integer operations
26    --
27    ------------------------------------------------------------------------
28
29    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
30    is
31       Result : T_Sign_Int32;
32    begin
33       if ( X > 0 ) then
34          Result := 1;
35       elsif ( X < 0 ) then
36          Result := -1;
37       end if;
38       return Result;
39    end Sign_Strict_Int32;
40
41 end ML;
```

ML | Unknown VCS (Modified) | Insert | Writable | Saved | 28:1

ml.ads ml.adb

Messages

```
gnatmake -ws -c -u -PY:\HiLite\TOY11\src\tmtc.gpr ml.adb
gcc -c -gnat12 -I- -gnatA Y:\HiLite\TOY11\src\ml.adb

[2012-05-03 14:45:47] process terminated successfully (elapsed time: 00.73s)
```

Proj

Messages Locations Call Trees

GPS - (Tmtc project) - ml.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.adb

```
22
23    ------------------------------------------------------------------------
24    --
25    -- Integer operations
26    --
27    ------------------------------------------------------------------------
28
29    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
30    is
31       Result : T_Sign_Int32;
32    begi
33       i
34
35       e
36
37       e
38       r
39    end
40
41 end ML;
```

ML

ml.ads ml.adb

sert Writable Saved 28:1

Prove File

Compilation

- [x] Force Recompilation
- [ ] Report Proved VCs

Proof

Prover Timeout 1

Alternate Prover

gnatprove -P%PP --mode=prove -u %fp -f

gnatprove -PY:\HiLite\TOY11\src\tmtc.gpr --mode=prove -u ml.adb -f

Execute Cancel

Messages

```
gnatmake -ws -c -u -PY:\HiLite\TOY11\src\tmtc.gpr ml.adb
gcc -c -gnat12 -I- -gnatA Y:\HiLite\TOY11\src\ml.adb

[2012-05-03 14:45:47] process terminated successfully (elapsed time: 00.73s)
```

Proj

Messages Locations Call Trees

GPS - (Tmtc project) - ml.ads

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.ads

```
58
59    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
60    with
61      Post  => ( ( Sign_Strict_Int32'Result = 1 ) or
62                 ( Sign_Strict_Int32'Result = -1 ) ) and then
63      (if X >= 0 then Sign_Strict_Int32'Result = 1) and then
64      (if X < 0 then Sign_Strict_Int32'Result = -1),
65      Test_Case => (Name     => "Negative input",
66                    Mode     => Nominal,
67                    Requires => X < 0,
68                    Ensures  => Sign_Strict_Int32'Result = -1),
69      Test_Case => (Name     => "Zero input",
70                    Mode     => Nominal,
71                    Requires => X = 0,
72                    Ensures  => Sign_Strict_Int32'Result = 1),
73      Test_Case => (Name     => "Positive input",
74                    Mode     => Nominal,
75                    Requires => X > 0,
76                    Ensures  => Sign_Strict_Int32'Result = 1);
77
78  end Ml;
```

Sign_Strict_Int32 | Insert | Writable | Unmodified | 64:7

ml.ads ml.adb

Locations

Builder results (1 item)

ml.ads (1 item)

64:7 postcondition not proved

Proj

Messages Locations Call Trees

GPS - (Tmtc project) - ml.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.adb

```
22
23    ------------------------------------------------------------------------
24    --
25    -- Integer operations
26    --
27    ------------------------------------------------------------------------
28
29    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
30    is
31       Result : T_Sign_Int32;
32    begin
33       if ( X >= 0 ) then
34          Result := 1;
35       else
36          Result := -1;
37       end if;
38       return Result;
39    end Sign_Strict_Int32;
40
41 end ML;
```

Sign_Strict_Int32 | Unknown VCS (Modified) | Insert | Writable | Modified | 33:1

ml.ads ml.adb

Locations

Builder results (1 item)

ml.ads (1 item)

64:7 postcondition not proved

Proj

Messages Locations Call Trees

GPS - (Tmtc project) - ml.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project conta

Project

Tmtc

.

..\OE

Y:\HiLite\TOY11\src\ml.adb

```
22
23    ------------------------------------------------------------------------
24    --
25    -- Integer operations
26    --
27    ------------------------------------------------------------------------
28
29    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
30    is
31       Result : T_Sign_Int32;
32    begin
33       if ( X >= 0 ) then
34          Result := 1;
35       else
36          Result := -1;
37       end if;
38       return Result;
39    end Sign_Strict_Int32;
40
41 end ML;
```

Sign_Strict_Int32 | Unknown VCS (Modified) | Insert | Writable | Saved | 33:1

ml.ads ml.adb

Messages

```
gnatprove -PY:\HiLite\TOY11\src\tmtc.gpr --mode=prove -u ml.adb -f
Phase 1 of 3: frame condition computation ...
Phase 2 of 3: translation to intermediate language ...

Statistics logged in gnatprove.out
(detailed info can be found in Y:\HiLite\TOY11\OBJ\gnatprove\*.alfa)
Phase 3 of 3: generation and proof of VCs ...

[2012-05-03 14:48:46] process terminated successfully (elapsed time: 03.12s)
```

Proj

Messages Locations Call Trees

Use of gnatprove – approach

- Use on the complete case study
  - Not yet supported
    (e.g. discriminant)

➔ Use on a restricted "SPARK" case study

GPS - (Tmtc project) - sgs.ads

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Y:\offline Folder\HiLite\CASE_STUDY\TMTC\SGS_SPARK\sgs.ads

```
113
114    -- Type defining 1553 report for SADEi_MOTORS_FPGA_STS_CMD transfer
115    type T_SGS_SADE_MOTOR_MOVE_RPT_OK is array (T_SGS_SADE_EQPT_ID) of BOOLEAN;
116
117    --  Type defining the turning sens of a MOTOR.
118    type T_SGS_MOTORJ_TURNING_SENS is (CLOCK_WISE, COUNTER_CLOCK_WISE);
119 --**>   for T_SGS_MOTORJ_TURNING_SENS'SIZE use 32;
120
121    --  Type defining transition sens of the wing switch.
122    type T_SGS_SWITCH_TRANSITION is (SGS_1_0_SWITCH_TRANSITION, SGS_0_1_SWITCH_TRANSITION);
123 --**>   for T_SGS_SWITCH_TRANSITION'SIZE use 32;
124
125    -- type defining the wing switch angle transitions in reference zone.
126    type T_SGS_WING_SWITCH_ANGLE_ARRAY is
127      array (T_SGS_SADM_ID, T_SGS_SWITCH_ID, T_SGS_MOTORJ_TURNING_SENS, T_SGS_SWITCH_TRANSITION) of M1.T_Angle_180;
128
129    -- This type is defined in order to create an Array of 8 Bits cells (with a BOOLEAN value) and to respect
130    -- the telemetry binding.
131    type T_MOTOR_POS_ACTI_CELL is
132       record
133          POS_ACTI : BOOLEAN;
```

Four dimension arrays not accepted

Sgs | Unknown VCS (Modified) | Insert | Writable | Saved | 126:9

sgs-s_sgs_b1_comp_sol_wing_ang_veloc.adb | sgs.adb | sgs.ads | m1.ads | sgs-s_rotate_data.adb | m1.adb | sgs-s_compute_reed_switch_angle.adb

Locations

- Builder results (19 items)
  - sgs.ads (3 items)
    - 126:9 info: array type is not yet supported
    - 273:7 info: type of formal is not yet supported
    - 752:7 info: type of formal is not yet supported
  - sgs-s_compute_reed_switch_angle.adb (3 items)
  - sgs-s_sgs_b1_comp_sol_wing_ang_veloc.adb (3 items)

Messages | Locations

GPS - (Tmtc project) - sgs.ads

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Y:\offline Folder\HiLite\CASE_STUDY\TMTC\SGS_SPARK\sgs.ads

```
116
117     --  Type defining the turning sens of a MOTOR.
118     type T_SGS_MOTORJ_TURNING_SENS is (CLOCK_WISE, COUNTER_CLOCK_WISE);
119  --**>   for T_SGS_MOTORJ_TURNING_SENS'SIZE use 32;
120
121     --  Type defining transition sens of the wing switch.
122     type T_SGS_SWITCH_TRANSITION is (SGS_1_0_SWITCH_TRANSITION, SGS_0_1_SWITCH_T
123  --**>   for T_SGS_SWITCH_TRANSITION'SIZE use 32;
124
125     -- type defining the wing switch angle transitions in reference zone.
126  --**>   type T_SGS_WING_SWITCH_ANGLE_ARRAY is
127  --**>     array (T_SGS_SADM_ID, T_SGS_SWITCH_ID, T_SGS_MOTORJ_TURNING_SENS, T_SGS_SWITCH_TRANSITION) of M1.T_Angle_180;
128     type T_SGS_WING_SWITCH_ANGLE_ARRAY_1 is
129       array (T_SGS_MOTORJ_TURNING_SENS, T_SGS_SWITCH_TRANSITION) of M1.T_Angle_180;
130     type T_SGS_WING_SWITCH_ANGLE_ARRAY is
131       array (T_SGS_SADM_ID, T_SGS_SWITCH_ID) of T_SGS_WING_SWITCH_ANGLE_ARRAY_1;
132
133     -- This type is defined in order to create an Array of 8 Bits cells (with a BOOLEAN value) and to respect
134     -- the telemetry binding.
135     type T_MOTOR_POS_ACTI_CELL is
136       record
```

Sgs | Unknown VCS (Modified) | Insert | Writable | Saved | 132:1

sgs-s_sgs_b1_comp_sol_wing_ang_veloc.adb | sgs.adb | sgs.ads | m1.ads | sgs-s_rotate_data.adb | m1.adb

Locations

- Builder results (10 items)
  - m1.adb (10 items)
    - 121:4 warning: in instantiation at a-ngelfu.adb:90
    - 121:4 warning: raise statement is not in Alfa
    - 121:4 warning: handler is not in Alfa
    - 121:4 info: attribute is not yet supported
    - 121:4 warning: possible re-ordering due to missing parentheses

Messages | Locations

Adaptation of the case study

Subprograms in / not in Alfa (restricted case study)

Subprograms in Alfa : 76% (124/164)
... already supported : 74% (122/164)
... not yet supported : 1% (2/164)
Subprograms not in Alfa : 24% (40/164)

Subprograms not in Alfa due to (possibly more than one reason):
exception : 24% (40/164)

Subprograms not yet supported due to (possibly more than one reason):
attribute : 11% (18/164)

Units with the largest number of subprograms in Alfa:
ml : 73% (110/150)
sgs : 100% (14/14)

Units with the largest number of subprograms not in Alfa:
ml : 27% (40/150)

Application subprograms in Alfa

```
++ sgs__s_normalise_0_360 sgs.ads:636
++ sgs__s_normalise_minus_plus_180 sgs.ads:645
++ sgs__s_conv_and_increment_angle sgs.ads:659
++ sgs__s_comp_motorj_theta_point_com sgs.ads:672
++ sgs__s_comp_motorj_theta_point_com_m sgs.ads:694
++ sgs__s_store_theta_point_com_step sgs.ads:705
++ sgs__s_rotate_reed_switch_sequences sgs.ads:718
++ sgs__s_are_cms_switch_sts_available sgs.ads:729
++ sgs__s_compute_reed_switch_angle sgs.ads:749
++ sgs__s_rotate_data sgs.ads:795
++ sgs__s_sgs_b6_elab_sol_wing_cmd_angle sgs.ads:234
++ sgs__estimate_solar_wing_j_position sgs.ads:808
++ sgs__commanded_velocity_calculation sgs.ads:830
++ sgs__s_sgs_b1_comp_sol_wing_ang_veloc sgs.ads:259
```

Some library subprograms bodies not in Alfa

```
-+ ml__num32__OexponX a-ngelfu.ads:60 instantiated at ml.adb:121 (exception)
-+ ml__num32__arccosX a-ngelfu.ads:108 instantiated at ml.adb:121 (exception)
-+ ml__num32__arccos__2X a-ngelfu.ads:112 instantiated at ml.adb:121 (exception)
-+ ml__num32__arccoshX a-ngelfu.ads:168 instantiated at ml.adb:121 (exception)
-+ ml__num32__arccothX a-ngelfu.ads:177 instantiated at ml.adb:121 (exception)
-+ ml__num32__arcsinX a-ngelfu.ads:100 instantiated at ml.adb:121 (exception)
-+ ml__num32__arcsin__2X a-ngelfu.ads:104 instantiated at ml.adb:121 (exception)
-+ ml__num32__arctanX a-ngelfu.ads:116 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num32__arctan__2X a-ngelfu.ads:123 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num32__arctanhX a-ngelfu.ads:173 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num32__cotX a-ngelfu.ads:96 instantiated at ml.adb:121 (exception)
-+ ml__num32__cot__2X a-ngelfu.ads:98 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num32__cothX a-ngelfu.ads:160 instantiated at ml.adb:121 (exception)
-+ ml__num32__expX a-ngelfu.ads:56 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num32__exp_strictX a-ngelfu.adb:66 instantiated at ml.adb:121 (exception) [attribute]
*+ ml__num32__local_atanX a-ngelfu.adb:70 instantiated at ml.adb:121 [attribute]
-+ ml__num32__logX a-ngelfu.ads:48 instantiated at ml.adb:121 (exception)
-+ ml__num32__log__2X a-ngelfu.ads:52 instantiated at ml.adb:121 (exception)
-+ ml__num32__sin__2X a-ngelfu.ads:73 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num32__sqrtX a-ngelfu.ads:42 instantiated at ml.adb:121 (exception)
-+ ml__num32__tan__2X a-ngelfu.ads:92 instantiated at ml.adb:121 (exception) [attribute]
-+ ml__num64__OexponX a-ngelfu.ads:60 instantiated at ml.adb:688 (exception)
-+ ml__num64__arccosX a-ngelfu.ads:108 instantiated at ml.adb:688 (exception)
-+ ml__num64__arccos__2X a-ngelfu.ads:112 instantiated at ml.adb:688 (exception)
```

GPS - (Tmtc project) - Messages

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project contains no scenario var

Project

- Tmtc
  - .
    - ml.adb
    - ml.ads
    - sgs.adb
    - sgs.ads
    - OBJ
    - OBJ

Y:\offline Folder\HiLite\CASE_STUDY\TMTC\SGS_SPARK_NO_SEPARATE\sgs.adb

```
225  --  10) Reference SADM switch 1 status of the SADM  : it is available if it is TRUE
226  --  14) Reference SADM switch 2 status of the SADM  : it is available if it is TRUE
227
228  is
229
230     -- Returned value
231     REPORT_IS_OK : BOOLEAN;
232     --------        CODE      --------
233
234  begin
235
236     -- Return the logical "AND" between all data :
237     -- 1) CMS validity flag                          : it is available if it is OK
238     REPORT_IS_OK := ((CMS_VALIDITY_FLAG.CMS_CMU1_VALIDITY_FLAG = OK) and then
239
240                      -- 2) Canonic wing reed switch 1 status of the SADM  : it is available if it is T
241                        (WING_SWITCH_CANO_STS_RPT_OK(SADM_J,SGS_SWITCH_1)) and then
242
243                      -- 3) Canonic wing reed switch 2 status of the SADM  : it is available if it is T
244                        (WING_SWITCH_CANO_STS_RPT_OK(SADM_J,SGS_SWITCH_2)) and then
```

S_COMP_MOTORJ_THETA_POINT_COM Insert | Writable | Unmodified 298:14

sgs.adb sgs.ads ml.adb ml.ads

Messages

```
ml.adb:121:04: warning: in instantiation at a-ngelfu.adb:949
ml.adb:121:04: warning: possible re-ordering due to missing parentheses

Statistics logged in gnatprove.out
(detailed info can be found in Y:\offline Folder\HiLite\CASE_STUDY\TMTC\SGS_SPARK_NO_SEPARATE\OBJ\gnatprov
e\*.alfa)
Phase 3 of 3: generation and proof of VCs ...
Exception raise in Session.idle_handler: anomaly: Out of memory
Session.idle_handler stopped

[2012-05-24 11:07:05] process terminated successfully (elapsed time: 18:13.19s)
```

Project Outline

Messages Locations

Gestionnaire des tâches de Windows

Fichier Options Affichage ?

Applications | Processus | Performances | Mise en réseau

Nom de l'image	Nom de l'utilisateur	Processeur	Util. mémoire
gnatwhy3.exe	M023206	50	2 050 844 Ko
EngineServer.exe	SYSTEM	00	139 688 Ko
gps.exe	M023206	20	130 552 Ko
explorer.exe	M023206	00	113 268 Ko
svchost.exe	SYSTEM	00	102 600 Ko
Acrobat.exe	M023206	00	91 056 Ko
Mcshield.exe	SYSTEM	00	53 360 Ko
services.exe	SYSTEM	00	50 284 Ko
spoolsv.exe	SYSTEM	00	42 316 Ko
svchost.exe	SYSTEM	00	39 440 Ko
svchost.exe	SERVICE RÉSEAU	00	34 692 Ko
PPCNVCOM.EXE	M023206	00	32 616 Ko
svchost.exe	SYSTEM	00	32 088 Ko
WINWORD.EXE	M023206	00	31 780 Ko
CcmExec.exe	SYSTEM	00	29 872 Ko
svchost.exe	SERVICE LOCAL	00	29 336 Ko
POWERPNT.EXE	M023206	00	26 944 Ko
svchost.exe	SERVICE RÉSEAU	00	24 108 Ko
PolySpaceInOneClick.exe	M023206	00	15 656 Ko
OUTLOOK.EXE	M023206	00	13 912 Ko
FrameworkService.exe	SYSTEM	00	11 416 Ko
xemacs.exe	M023206	00	9 888 Ko
Acrotray.exe	M023206	00	9 708 Ko
EXCEL.EXE	M023206	00	9 140 Ko
winlogon.exe	SYSTEM	00	8 292 Ko
qttask.exe	M023206	00	7 744 Ko
SBKSRV.EXE	SYSTEM	00	7 600 Ko
wmiprvse.exe	SYSTEM	00	7 284 Ko
gprbuild.exe	M023206	00	6 856 Ko
dllhost.exe	SYSTEM	00	6 496 Ko
wmiprvse.exe	SYSTEM	00	5 928 Ko
gnatprove.exe	M023206	00	5 572 Ko
iss_acd.exe	SYSTEM	00	5 476 Ko
smax4pnp.exe	M023206	00	5 032 Ko
msiexec.exe	SYSTEM	00	4 928 Ko
Sbkrnl.exe	M023206	00	4 888 Ko
bash.exe	M023206	00	4 136 Ko
infxsrvc.exe	M023206	00	4 116 Ko

Afficher les processus de tous les utilisateurs

Terminer le processus

Processus : 67 | UC utilisée : 72% | Charge dédiée : 3347 Mo /

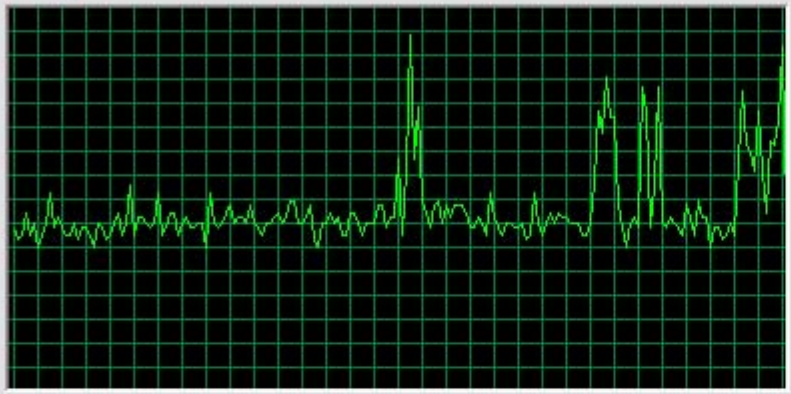
Gestionnaire des tâches de Windows

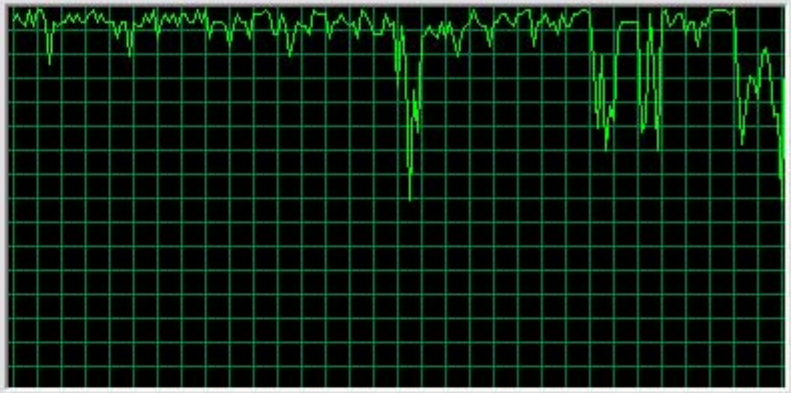
Fichier Options Affichage ?

Applications | Processus | Performances | Mise en réseau

Util. de l'UC

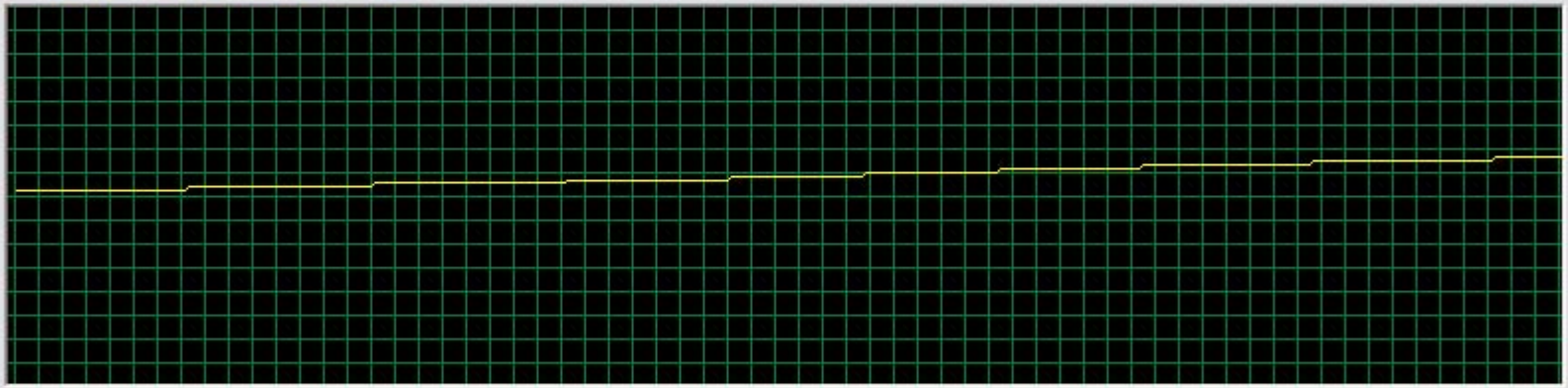
Historique de l'utilisation de l'UC





Util. du fichier

Historique d'utilisation du fichier d'échange



Totaux	
Handles	19962
Threads	653
Processus	67

Mémoire physique (Ko)	
Total	3632680
Disponible	314624
Cache système	464876

Charge dédiée (Ko)	
Total	3415792
Limite	5560284
Pic	3442176

Mémoire pour le noyau (Ko)	
Total	132344
Paginée	103704
Non paginée	28640

Processus : 67 | UC utilisée : 69% | Charge dédiée : 3335 Mo /

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

GPS - (Tmtc project) - Project

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project contains no scenario variables

Project

- Tmtc
  - .
    - ml.adb
    - ml.ads
  - ..\OBJ

Project | Outline

Y:\HiLite\TOY11\src\ml.ads

```
55    -- Integer operations
56    --
57    ---------------------------------------------------------------------
58
59    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
60    with
61      Post  => ( ( Sign_Strict_Int32'Result = 1 ) or
62                 ( Sign_Strict_Int32'Result = -1 ) ) and then
63      (if X >= 0 then Sign_Strict_Int32'Result = 1) and then
64      (if X < 0 then Sign_Strict_Int32'Result = -1),
65      Test_Case => (Name     => "Negative input",
66                    Mode     => Nominal,
67                    Requires => X < 0,
68                    Ensures  => Sign_Strict_Int32'Result = -1),
69      Test_Case => (Name     => "Zero input",
70                    Mode     => Nominal,
71                    Requires => X = 0,
72                    Ensures  => Sign_Strict_Int32'Result = 1),
73      Test_Case => (Name     => "Positive input",
74                    Mode     => Nominal,
75                    Requires => X > 0,
76                    Ensures  => Sign_Strict_Int32'Result = 1);
77
78  end Ml;
79
```

Ml | Insert | Writable | Unmodified | 58:1

ml.ads | ml.adb

Messages

```
Welcome to GPS 5.2.0w (20120405) hosted on i686-pc-mingw32
the GNAT Programming Studio
(c) 2001-2012 AdaCore
```

Messages | Locations | Call Trees

GPS - (Tmtc project) - Project

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

Tools:
- Views
- Browsers
- Coding Standard
- Compare
- Consoles
- Coverage
- Documentation
- GNATTest
- Macro
- Metrics
- Interrupt Shift+Ctrl+C
- Plug-ins

GNATTest:
- Generate unit test setup
- Generate unit test setup recursive
- Show not implemented tests
- Exit from harness project

Scenario

The project contains no scenario va

Project

Tmtc
- .
  - ml.adb
  - ml.ads
  - ..\OBJ

1\src\ml.ads

```
nteger operations
-----------------------------------------------------------------------

                                    Int32) return T_Sign_Int32

                                    lt = 1 ) or
                                    ult = -1 ) ) and then
                                    esult = 1) and then
f X < 0 then Sign_Strict_Int32'Result = -1),
    Test_Case => (Name     => "Negative input",
                  Mode     => Nominal,
                  Requires => X < 0,
                  Ensures  => Sign_Strict_Int32'Result = -1),
    Test_Case => (Name     => "Zero input",
                  Mode     => Nominal,
                  Requires => X = 0,
                  Ensures  => Sign_Strict_Int32'Result = 1),
    Test_Case => (Name     => "Positive input",
                  Mode     => Nominal,
                  Requires => X > 0,
                  Ensures  => Sign_Strict_Int32'Result = 1);

end Ml;
```

Ml | Insert | Writable | Unmodified | 58:1

ml.ads ml.adb

Messages

```
Welcome to GPS 5.2.0w (20120405) hosted on i686-pc-mingw32
the GNAT Programming Studio
(c) 2001-2012 AdaCore
```

Project Outline

Messages Locations Call Trees

GPS - (test_driver project)

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

- Test_Driver
  - .
  - .
  - AUnit
  - test_tmtc
    - ..\tests
      - ml-test_data-tests-test_sign_strict_int32_9f4b45
      - ml-test_data-tests-test_sign_strict_int32_9f4b45
      - ml-test_data-tests-test_sign_strict_int32_9f4b45
      - ml-test_data-tests.adb
      - ml-test_data-tests.ads
      - ml-test_data.adb
      - ml-test_data.ads
    - common
    - .
    - AUnit
    - Tmtc

Project | Outline

Y:\HiLite\TOY11\src\ml.ads

```
55    -- Integer operations
56    --
57    ------------------------------------------------------------------
58
59    function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
60    with
61      Post  => ( ( Sign_Strict_Int32'Result = 1 ) or
62                 ( Sign_Strict_Int32'Result = -1 ) ) and then
63      (if X >= 0 then Sign_Strict_Int32'Result = 1) and then
64      (if X < 0 then Sign_Strict_Int32'Result = -1),
65      Test_Case => (Name     => "Negative input",
66                    Mode     => Nominal,
67                    Requires => X < 0,
68                    Ensures  => Sign_Strict_Int32'Result = -1),
69      Test_Case => (Name     => "Zero input",
70                    Mode     => Nominal,
71                    Requires => X = 0,
72                    Ensures  => Sign_Strict_Int32'Result = 1),
73      Test_Case => (Name     => "Positive input",
74                    Mode     => Nominal,
75                    Requires => X > 0,
76                    Ensures  => Sign_Strict_Int32'Result = 1);
77
78  end Ml;
79
```

Ml | Insert | Writable | Unmodified | 58:1

ml.ads | ml.adb

Messages

Switched to harness project: Y:\HiLite\TOY11\OBJ\gnattest\harness\test_driver.gpr

Messages | Locations | Call Trees

GPS - (Test_Driver project) - Project

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

_0052bd.adb

_4fbf40.adb

_f98ele.adb

Proj

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Zero input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_0052bd (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int32_9f4b45_0052bd;
10 begin
11    AUnit.Assertions.Assert
12      (Gnattest_Generated.Default_Assert_Value,
13       "Test not implemented.");
14 end Test_Sign_Strict_Int32_9f4b45_0052bd;
```

Insert | Writable | Unmodified | 1:1

ml.ads | ml.adb | ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

Messages

Switched to harness project: Y:\HiLite\TOY11\OBJ\gnattest\harness\test_driver.gpr

Messages | Locations | Call Trees

GPS - (Test_Driver project) - ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

5_0052bd.adb
5_4fbf40.adb
5_f98ele.adb

Proj

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Zero input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_0052bd (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int32_9f4b45_0052bd;
10 begin
11    AUnit.Assertions.Assert
12      (Gnattest_Generated.Default_Assert_Value,
13       "Test not implemented.");
14 end Test_Sign_Strict_Int32_9f4b45_0052bd;
```

Unknown VCS (Modified) | Insert | Writable | Unmodified | 1:1

ml.ads | ml.adb | ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

Messages

```
gprbuild -d -PY:\HiLite\TOY11\OBJ\gnattest\harness\test_driver.gpr -XRUNTIME=full test_runner.adb
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 test_runner.adb
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 gnattest_generated.ads
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 gnattest_main_suite.adb
gcc -c -gnatl2 ml.adb
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 ml-test_data.adb
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 ml-test_data-tests.adb
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 ml-test_data-tests-suite.adb
gprbind test_runner.bexch
gnatbind test_runner.ali
gcc -c b__test_runner.adb
gcc test_runner.o -g -o test_runner.exe

[2012-05-03 14:37:33] process terminated successfully (elapsed time: 10.73s)
```

Messages | Locations | Call Trees

GPS - (Test_Driver project) - Run: test_runner

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

5_0052bd.adb

5_4fbf40.adb

5_f98ele.adb

Proj

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Zero input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_0052bd (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int32_9f4b45_0052bd;
10 begin
11    AUnit.Assertions.Assert
12      (Gnattest_Generated.Default_Assert_Value,
13       "Test not implemented.");
14 end Test_Sign_Strict_Int32_9f4b45_0052bd;
```

Unknown VCS (Modified) | Insert | Writable | Unmodified | 1:1

ml.ads | ml.adb | ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

Run: test_runner

```
FAIL Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_f98ele
    Test not implemented.
    at ml-test_data-tests-test_sign_strict_int32_9f4b45_f98ele.adb:11
FAIL Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_0052bd
    Test not implemented.
    at ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb:11
FAIL Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_4fbf40
    Test not implemented.
    at ml-test_data-tests-test_sign_strict_int32_9f4b45_4fbf40.adb:11

Total Tests Run:    3
Successful Tests:   0
Failed Assertions:  3
Unexpected Errors:  0
[2012-05-03 14:37:46] process terminated successfully (elapsed time: 00.97s)
```

Messages | Locations | Call Trees | Run: test_runner

GPS - (Test_Driver project) - ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

5_0052bd.adb

5_4fbf40.adb

5_f98ele.adb

Proj

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Zero input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_0052bd (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int32_9f4b45_0052bd;
10 begin
11    Assert( Sign_Strict_Int32(X => 0) = 1, "Zero input" );
12 end Test_Sign_Strict_Int32_9f4b45_0052bd;
```

Test_Sign_Strict_Int32_9f4b45_0052bd | Unknown VCS (Modified) | Insert | Writable | Saved | 11:1

ml.ads | ml.adb | ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

Messages

```
gprbuild -d -PY:\HiLite\TOY11\OBJ\gnattest\harness\test_driver.gpr -XRUNTIME=full test_runner.adb
gcc -c -g -O1 -gnat05 -gnatyM0 -gnata -gnatl2 ml-test_data-tests.adb
gprbind test_runner.bexch
gnatbind test_runner.ali
gcc -c b__test_runner.adb
gcc test_runner.o -g -o test_runner.exe

[2012-05-03 14:38:20] process terminated successfully (elapsed time: 08.45s)
```

Messages | Locations | Call Trees | Run: test_runner

GPS - (Test_Driver project) - Run: test_runner

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

5_0052bd.adb

5_4fbf40.adb

5_f98ele.adb

Proj

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Zero input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_0052bd (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int32_9f4b45_0052bd;
10 begin
11    Assert( Sign_Strict_Int32(X => 0) = 1, "Zero input" );
12 end Test_Sign_Strict_Int32_9f4b45_0052bd;
```

Test_Sign_Strict_Int32_9f4b45_0052bd | Unknown VCS (Modified) | Insert | Writable | Saved | 11:1

ml.ads | ml.adb | ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

Run: test_runner

```
OK Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_0052bd

FAIL Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_f98ele
    Test not implemented.
    at ml-test_data-tests-test_sign_strict_int32_9f4b45_f98ele.adb:11
FAIL Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_4fbf40
    Test not implemented.
    at ml-test_data-tests-test_sign_strict_int32_9f4b45_4fbf40.adb:11

Total Tests Run:    3
Successful Tests:   1
Failed Assertions:  2
Unexpected Errors:  0
[2012-05-03 14:38:31] process terminated successfully (elapsed time: 00.86s)
```

Messages | Locations | Call Trees | Run: test_runner

Positive points

- Easiness
  - Difficulty to manually write a test harness from scratch
  - Verification that the test case is satisfied

Points to be improved

- One file per test case
  - ➔ Huge number of files

    (one file is generally defined per package)
- Naming of files

GPS - (Test_Driver project) - Project

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

- Test_Driver
  - .
  - .
  - AUnit
  - test_tmtc
    - ..\tests
      - ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb
      - ml-test_data-tests-test_sign_strict_int32_9f4b45_4fbf40.adb
      - ml-test_data-tests-test_sign_strict_int32_9f4b45_f98ele.adb
      - ml-test_data-tests.adb
      - ml-test_data-tests.ads
      - ml-test_data.adb
      - ml-test_data.ads
    - common
    - .
    - AUnit
    - Tmtc

Project | Outline

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return
2  --  Test Case "Zero input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_0052bd (T : in
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T
10 begin
11    Assert( Sign_Strict_Int32(X => 0) = 1, "Zero input"
12 end Test_Sign_Strict_Int32_9f4b45_0052bd;
```

Test_Sign_Strict_Int32_9f4b45_0052bd | Insert | Writable | Unmodified | 12:1

ml-test_data-tests-test_sign_strict_int32_9f4b45_0052bd.adb

Locations

Messages | Locations

File name not linked to the test case

GPS - (Tmtc project) - ml.ads

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

Views
Browsers
Coding Standard
Compare
Consoles
Coverage
Documentation
GNATTest
Macro
Metrics
Interrupt Shift+Ctrl+C
Plug-ins

Generate unit test setup
Generate unit test setup recursive
Show not implemented tests
Exit from harness project

Scenario

The project contains no scenario variables

Project

Tmtc
.
..\OBJ

Y:\HiLite\T

```
58
59    fu                                  T_Int32) return T_Sign_Int32
60    wi
61                                        sult = 1 ) or
62
63
64
65
66
67
68                  Ensures  => Sign_Strict_Int32'Result = -1),
69      Test_Case => (Name     => "Zero input",
70                    Mode     => Nominal,
71                    Requires => X = 0,
72                    Ensures  => Sign_Strict_Int32'Result = 1),
73      Test_Case => (Name     => "Positive input",
74                    Mode     => Nominal,
75                    Requires => X > 0,
76                    Ensures  => Sign_Strict_Int32'Result = 1),
77      Test_Case => (Name     => "Big input",
78                    Mode     => Nominal,
79                    Requires => X > 10_000,
80                    Ensures  => Sign_Strict_Int32'Result = 1);
81
82  end Ml;
83
```

Addition of a new test case

Sign_Strict_Int32 | Unknown VCS (Modified) | Insert | Writable | Saved | 77:1

ml.ads ml.adb

Messages

```
gnatmake -q -c -gnatc -u -PY:\HiLite\TOY11\src\tmtc.gpr ml.ads -g

[2012-05-10 17:02:24] process terminated successfully (elapsed time: 00.42s)
```

Project Outline

Messages Locations

GPS - (Test_Driver project) - Run: test_runner

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

trict_int32_9f4b45_0052bd.adb

trict_int32_9f4b45_4fbf40.adb

trict_int32_9f4b45_e6d0ac.adb

trict_int32_9f4b45_f98ele.adb

Project Outline

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_e6d0ac.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Big input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_e6d0ac (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int3
10 begin
11    Assert( Sign_Strict_Int32(X => 20_000) = 1, "Big input" );
12 end Test_Sign_Strict_Int32_9f4b45_e6d0ac;
```

Previous file not impacted

Test_Sign_Strict_Int32_9f4b45_e6d0ac Unknown VCS (Modified) Insert Writable Saved 11:36

ml-test_data-tests-test_sign_strict_int32_9f4b45_e6d0ac.adb ml-test_data-tests-test_sign_strict_int32_9f4b45_f98e1e.adb

Run: test_runner

```
Y:\HiLite\TOY11\OBJ\gnattest\harness\test_runner

OK Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_f98ele
OK Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_0052bd
OK Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_4fbf40
OK Ml.Test_Data.Tests : Test_Sign_Strict_Int32_9f4b45_e6d0ac

Total Tests Run:    4
Successful Tests:   4
Failed Assertions:  0
Unexpected Errors:  0
[2012-05-10 17:04:40] process terminated successfully (elapsed time: 00.72s)
```

Messages Locations Run: test_runner

GPS - (tmtc project)

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

The project contains no scenario variables

Project

- Tmtc
  - .
  - ..\OBJ

Y:\HiLite\TOY11\src\ml.ads

```
56      --
57      ----------------------------------------------------------------------
58
59      function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
60      with
61        Post  => ( ( Sign_Strict_Int32'Result = 1 ) or
62                   ( Sign_Strict_Int32'Result = -1 ) ) and then
63        (if X >= 0 then Sign_Strict_Int32'Result = 1) and then
64        (if X < 0 then Sign_Strict_Int32'Result = -1),
65        Test_Case => (Name     => "Negative input",
66                      Mode     => Nominal,
67                      Requires => X < 0,
68                      Ensures  => Sign_Strict_Int32'Result = -1),
69        Test_Case => (Name     => "Zero input",
70                      Mode     => Nominal,
71                      Requires => X = 0,
72                      Ensures  => Sign_Strict_Int32'Result = 1),
73        Test_Case => (Name     => "Positive input",
74                      Mode     => Nominal,
75                      Requires => X > 0,
76                      Ensures  => Sign_Strict_Int32'Result = 1);
77
78  end Ml;
79
```

Suppression of a test case

Ml | Unknown VCS (Modified) | Insert | Writable | Saved | 58:1

ml.ads | ml.adb

Messages

```
gnatmake -q -c -gnatc -u -PY:\HiLite\TOY11\src\tmtc.gpr ml.ads -g

[2012-05-10 17:05:13] process terminated successfully (elapsed time: 00.37s)
```

Project | Outline

Messages | Locations

GPS - (tmtc project)

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

Views
Browsers
Coding Standard
Compare
Consoles
Coverage
Documentation
GNATTest
Macro
Metrics
Interrupt Shift+Ctrl+C
Plug-ins

Generate unit test setup
Generate unit test setup recursive
Show not implemented tests
Exit from harness project

Scenario

The project contains no scenario variables

Project

Tmtc
.
..\OBJ

Y:\HiLite\T

```
56      --
57      --
58
59      fu                                  T_Int32) return T_Sign_Int32
60      wi
61
62
63
64                                          Result = -1),
65                                          ve input",
66                          Mode     => Nominal,
67                          Requires => X < 0,
68                          Ensures  => Sign_Strict_Int32'Result = -1),
69        Test_Case => (Name     => "Zero input",
70                      Mode     => Nominal,
71                      Requires => X = 0,
72                      Ensures  => Sign_Strict_Int32'Result = 1),
73        Test_Case => (Name     => "Positive input",
74                      Mode     => Nominal,
75                      Requires => X > 0,
76                      Ensures  => Sign_Strict_Int32'Result = 1);
77
78  end M1;
79
```

M1 Unknown VCS (Modified) Insert Writable Saved 58:1

ml.ads ml.adb

Messages

```
gnatmake -q -c -gnatc -u -PY:\HiLite\TOY11\src\tmtc.gpr ml.ads -g

[2012-05-10 17:05:13] process terminated successfully (elapsed time: 00.37s)
```

Project Outline

Messages Locations

GPS - (Test_Driver project) - ml-test_data-tests-test_sign_strict_int32_9f4b45_e6d0ac.adb

File Edit Navigate VCS Project Build Debug Tools Prove Window Help

default

Scenario

Runtime full

Project

trict_int32_9f4b45_0052bd.adb
trict_int32_9f4b45_4fbf40.adb
trict_int32_9f4b45_e6d0ac.adb
trict_int32_9f4b45_f98e1e.adb

Project Outline

Y:\hilite\toy11\OBJ\gnattest\tests\ml-test_data-tests-test_sign_strict_int32_9f4b45_e6d0ac.adb

```
1  --  function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32
2  --  Test Case "Big input"
3
4  with Gnattest_Generated;
5
6  separate (Ml.Test_Data.Tests)
7  procedure Test_Sign_Strict_Int32_9f4b45_e6d0ac (T : in out Test) is
8     pragma Unreferenced (T);
9     function Sign_Strict_Int32 (X : in T_Int32) return T_Sign_Int32 renames Wrap_Test_Sign_Strict_Int3
10 begin
11    Assert( Sign_Strict_Int32(X => 20_000) = 1, "Big input" );
12 end Test_Sign_Strict_Int32_9f4b45_e6d0ac;
```

File not deleted

Unknown VCS (Modified) | Insert | Writable | Unmodified | 3:1

ml-test_data-tests-test_sign_strict_int32_9f4b45_f98e1e.adb | ml-test_data-tests-test_sign_strict_int32_9f4b45_e6d0ac.adb

Messages

Switched to harness project: Y:\HiLite\TOY11\OBJ\gnattest\harness\test_driver.gpr

Messages Locations

Overview

- Introduction
- Astrium Space Transportation Case study
  - SCADE modelling
  - Data handling
  - Numerical algorithm
  - Event driven
- Alfa
- Gnatprove
- Gnattest
- Conclusion

Conclusion

A lot of progress on all the subjects

- Alfa
  - A lot of features already implemented
  - A few are missing for the Astrium case study
- gnatprove
  - Performance issue
- gnattest
  - Very practical for small projects
  - Process issue for (normally) big projects
- Case study
  - Good process
  - Assessment of each new version of the tools

Always a great support from AdaCore

AdaCore
The GNAT Pro Company

ASTRIUM
AN EADS COMPANY