Japan Aerospace Exploration Agency

Model-Based IV&V for an Operation Procedure

2010 Validation and Verification Workshop@NASA IV&V Facility

Tsutomu MATSUMOTO*1,
Masakazu TAKASE*2, Yuko MIYAMOTO*1, Masa KATAHIRA*1
*1 Japan Aerospace Exploration Agency (JAXA)
*2 Mitsubishi Space Software Co.,Ltd. (MSS)

September 17, 2010

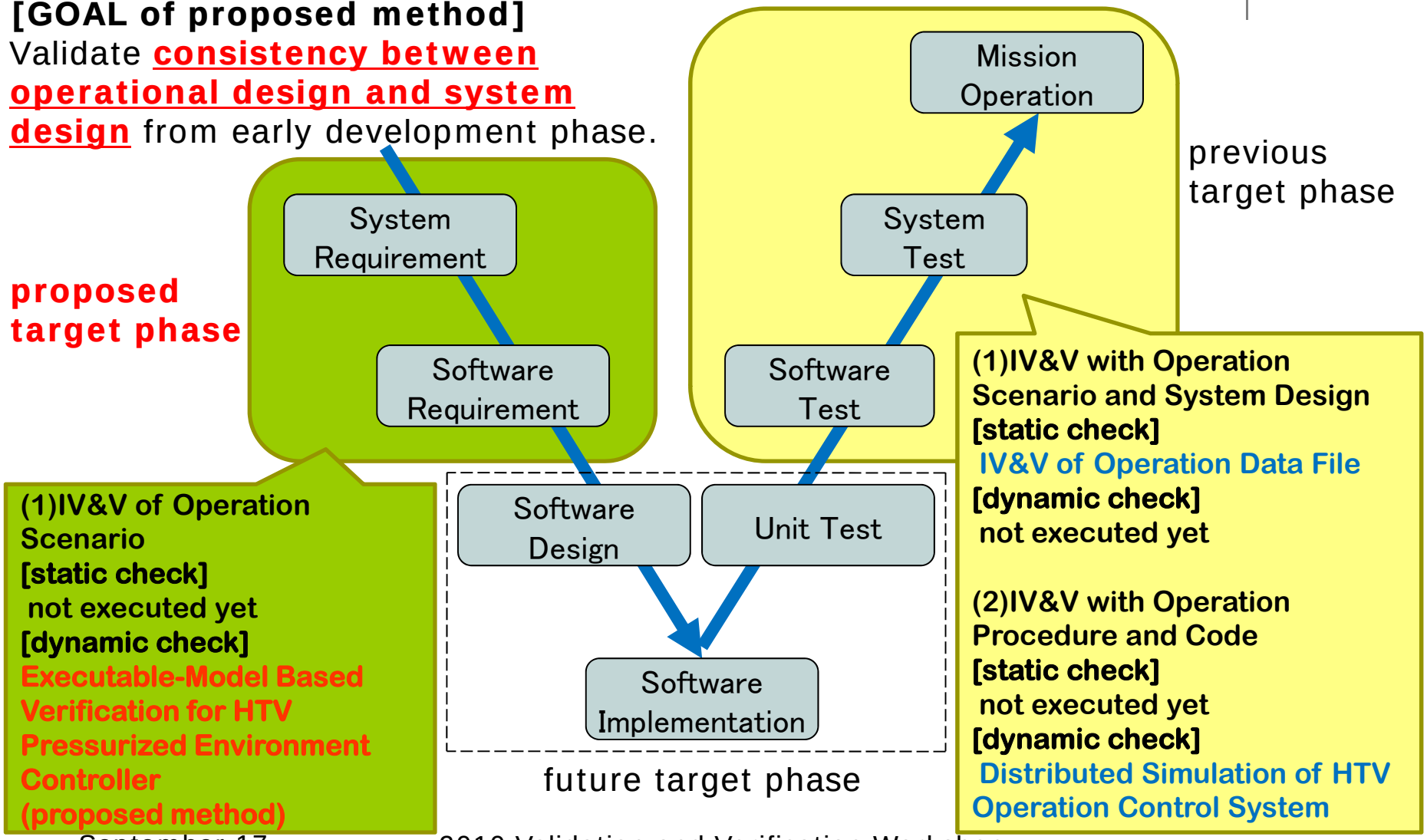
Contents

- Background
  - IV&V for an Operation Procedure in JAXA
- Target System
- Activity execution
  - Work Sequence
  - Modeling and Simulation
  - Case Example
- Lessons Learned
- Conclusion and Future Work

Background

IV&V for an Operation Procedure in JAXA

[GOAL of proposed method]
Validate **consistency between operational design and system design** from early development phase.

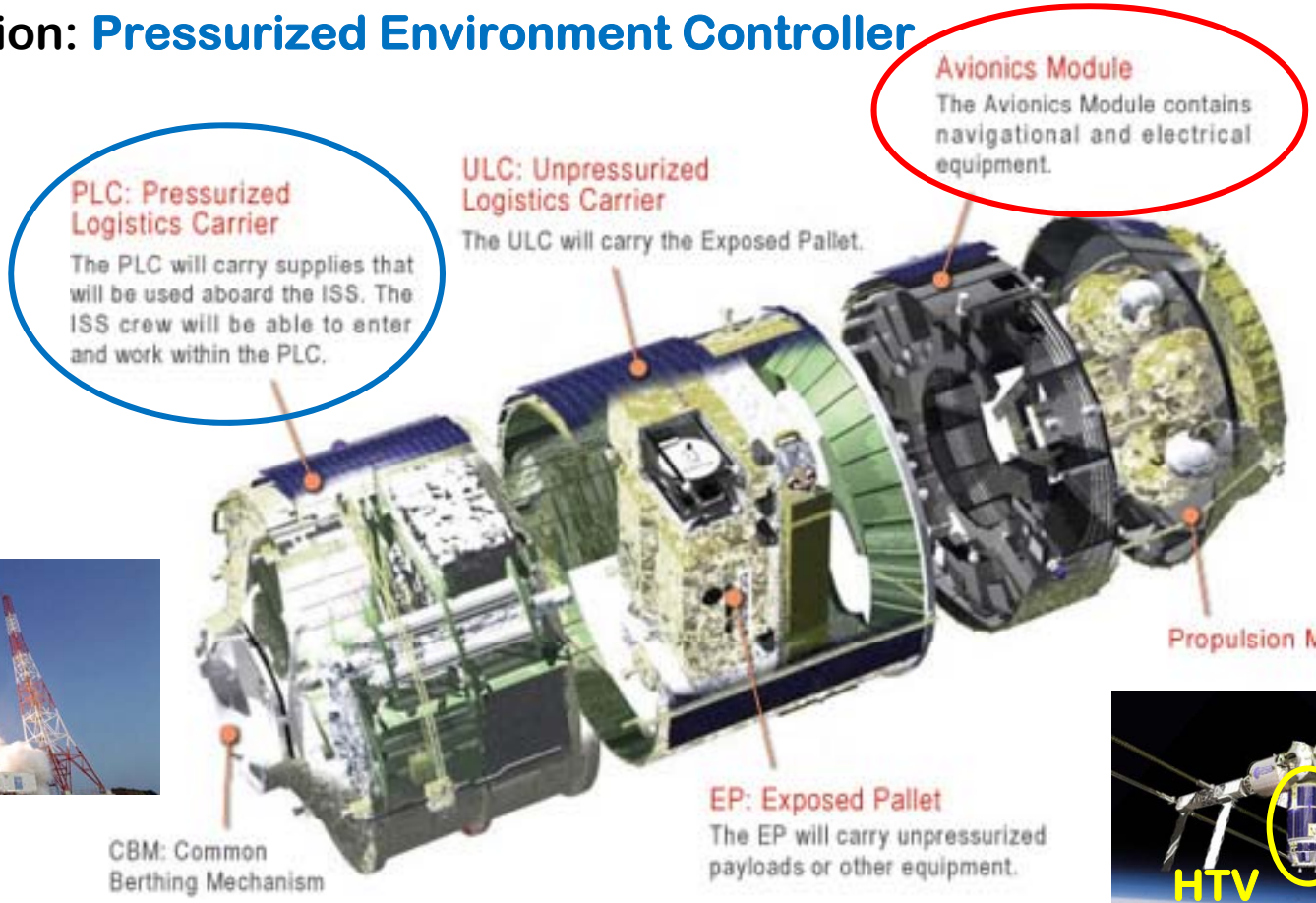


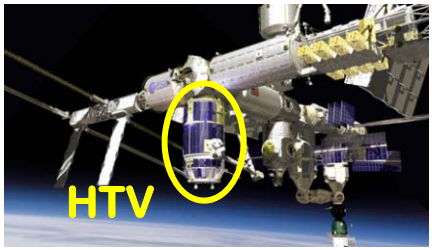
Target System (1/2)

Spacecraft : H-II Transfer Vehicle (HTV)

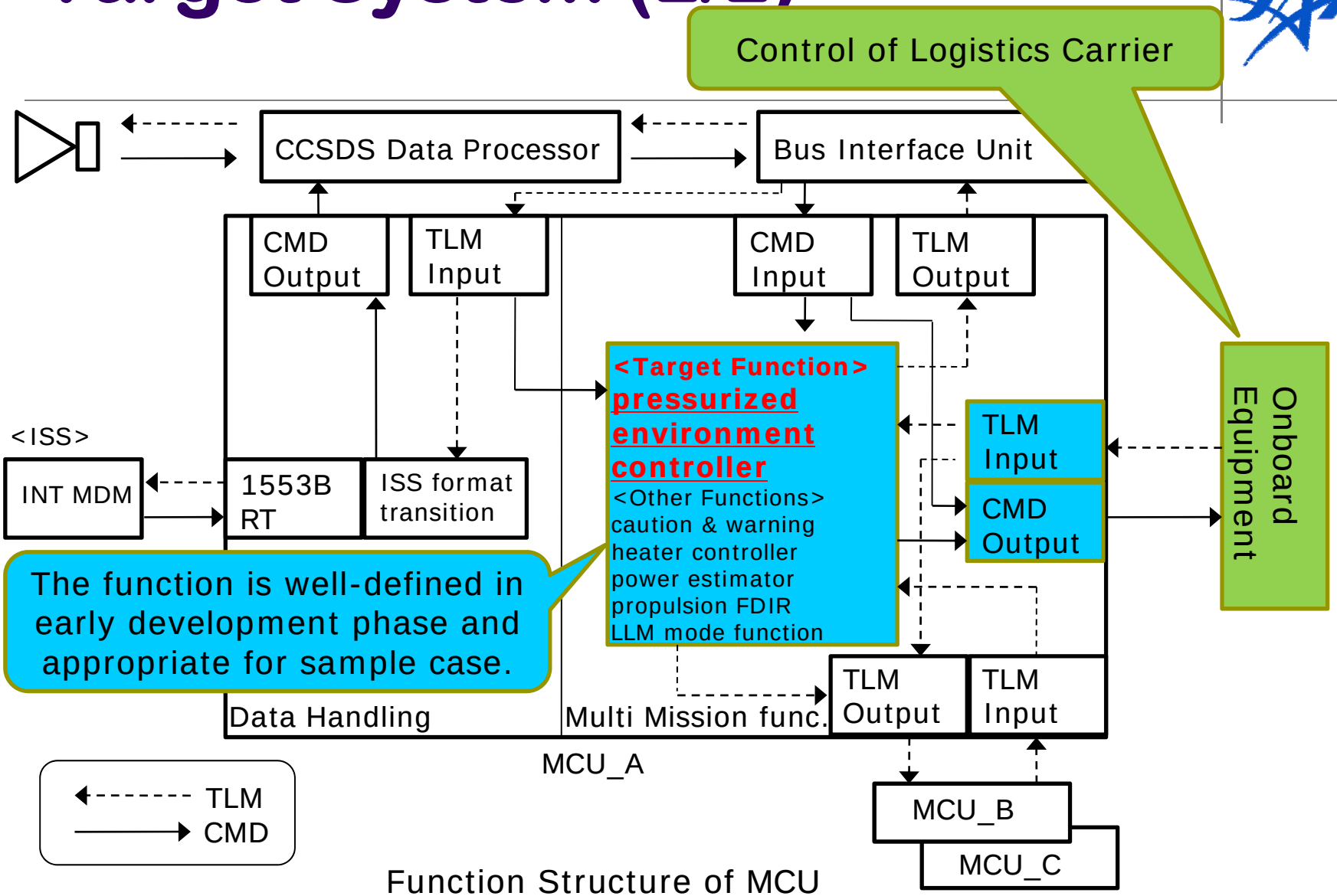
Component : Avionics Module / Multi-mission Control Unit (MCU)

Function: Pressurized Environment Controller





Target System (2/2)



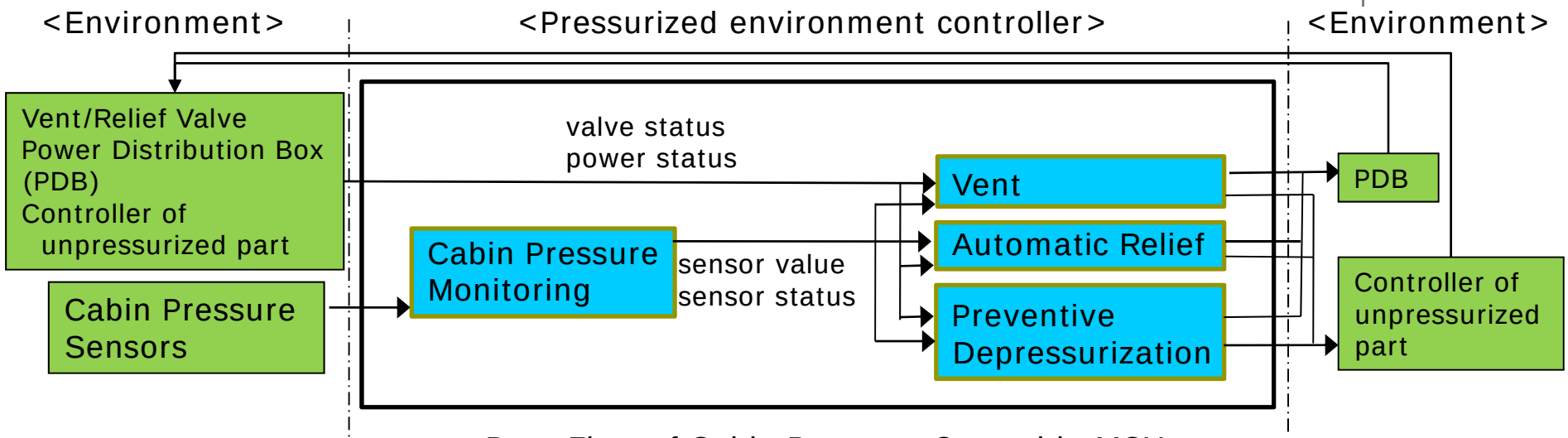
Function Structure of MCU

Activity Execution (1/6)
Work Sequence

Perform model-based simulation of targeted system behavior to validate operation procedure regarding HTV MCU

- **Step1: Modeling of target system and its environment**
  - System model is constructed based on system specification defined in system requirement phase.
    - ✓ System behavior is statically simulated according to the command input and the state of environmental model.
  - Environmental model associated with cabin pressure is virtually constructed.
    - ✓ If all two switches of valves are "open", pressure value is decreased by 1kPa/sec.
    - ✓ If one of two switches of valves is "close", pressure value remains the same.
- **Step2: Simulation with executable models**
  - [input] sequence of commands based on operation procedure
  - [output] telemetry
- **step3: Analyze the result of the simulation recorded in log file**

Activity Execution (2/6)
Modeling and Simulation



Data Flow of Cabin Pressure Control in MCU

Environmental Model <sample>

```
if ( (MainPowerSourceOnOffStatus == ON)
     && (SwitchOfVentReliefValve1 == OPEN)
     && (SwitchOfVentReliefValve2 == OPEN) )
{
      ValueOfCabinPressureSensor1--;
      ValueOfCabinPressureSensor2--;
      ValueOfCabinPressureSensor3--;
}
```

System Model <sample>

```
if( (ValueOfCabinPressureSensor1 > UpperLimit)
    && (ValueOfCabinPressureSensor2 > UpperLimit) )
{
     PressureValue = ValueOfCabinPressureSensor3;
}
else {
     AutomaticReliefFlag = NonExecutable;
}
```

Modeling Language : **Microsoft Visual C++**

Activity Execution (3/6)
Simulation Result

	A	H	I	J	K	L	M	N
1	L/N						備考 ④	判定 ⑤
2		コマンド変数名 ①	設定値	テレメトリ変数名 ②	期待値	実際の値 ③		
3	1						予めキャビン圧力を記録する	
4	2			Cabin_Pressure_1	-		記録のみ	
5	3			Cabin_Pressure_2	-		記録のみ	
6	4			Cabin_Pressure_3	-		記録のみ	
7	5			WCU1_AutoRlf_EnaSt	-		記録のみ	
8	6			WCU2_AutoRlf_EnaSt	-		記録のみ	
9	7			WCU1_AutoRlf_ExecSt	-		記録のみ	
10	8	⑥		WCU2_AutoRlf_ExecSt	-		記録のみ	
11	9			VRY_A1_St	-		記録のみ	
12	10			VRY_B1_St	-		記録のみ	
13	11			VRY_A2_St	-		記録のみ	
14	12			VRY_B2_St	-		記録のみ	
15	13						予防減圧機能動作開始	
16	14	WCU_Pre-P_VALVE_SET_WCU1	220					
17	15	WCU_Pre-P_VALVE_SET_WCU2	220					
18	16	WCU1_PLC_Prc_Cab_Mon_Ena						
19	17	WCU2_PLC_Prc_Cab_Mon_Ena						
20	18			WCU1_PLC_Prc_Cab_Mon_st	ENA			
21	19			WCU2_PLC_Prc_Cab_Mon_st	ENA			
22	20			WCU1_Press_Snsr1_St	NORM			
23	21			WCU2_Press_Snsr1_St	NORM			
24	22			WCU1_Press_Snsr2_St	NORM			
25	23			WCU2_Press_Snsr2_St	NORM			
26	24			WCU1_Press_Snsr3_St	NORM			
27	25			WCU2_Press_Snsr3_St	NORM			
28	26			WCU1_PLC_Htr_St	-		記録のみ	
29	27			WCU2_PLC_Htr_St	-		記録のみ	
30	28	WCU1_PLC_Htr_Flt_Sel						
31	29	WCU2_PLC_Htr_Flt_Sel						
32	30			WCU1_PLC_Htr_St	FLT			
33	31			WCU2_PLC_Htr_St	FLT			
34	32							

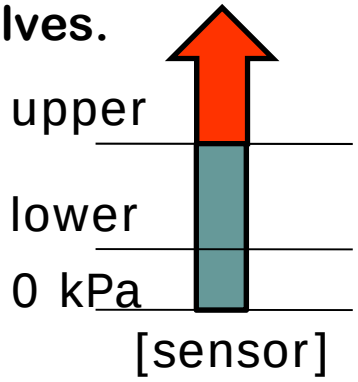
⑦

① Command Sequences
② Telemetry to be checked
③ Simulation Output
④ Comment on the Procedure
⑤ Comment on the Result
⑥ Setting Value
⑦ Expectation Value

Activity Execution (4/6)
Case Example

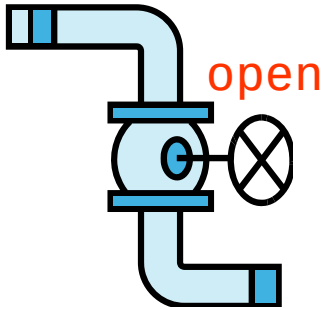
- Automatic Cabin Air Relief

If cabin pressure goes over upper threshold,
cabin air is released for depressurization by opening relief valves.



[Abstract of Operation Procedure]

Set "Status of Cabin Pressure Monitoring (ENA/INH)" to ENA
Set "Status of Cabin Pressure Sensor" to NORMAL
Set "Status of Automatic Cabin Air Relief (ENA/INH)" to ENA
Execute "Automatic Cabin Air Relief"
Monitor "Value of Air Pressure Sensor"
Monitor "Status of Air Pressure Sensor"
Monitor "Status of Valve (OPEN/CLOSE)"



[valve]

Activity Execution (5/6)

Case Example

expectation value

simulation output

L/N	コマンド変数名	設定値	テレメトリ変数名	期待値	実際の値	備考	補足
1						予めキャビン圧力を記録する	
2			Cabin_Pressure_1	-	226	記録のみ	
3			Cabin_Pressure_2	-	226	記録のみ	
4			Cabin_Pressure_3	-	226	記録のみ	
5			MCU1_AutoRlf_EnaSt	-	INH	記録のみ	
6			MCU2_AutoRlf_EnaSt	-	INH	記録のみ	
7			MCU1_AutoRlf_ExecSt	-	OFF	記録のみ	
8			MCU2_AutoRlf_ExecSt	-	OFF	記録のみ	
9			VRV_A1_St	-	Open	記録のみ	Openなのは初期設定のため。
10			VRV_B1_St	-	Open	記録のみ	Openなのは初期設定のため。
11			VRV_A2_St	-	Close	記録のみ	
12			VRV_B2_St	-	Close	記録のみ	
13							
14	MCU1_PLC_Prc_Cab_Mon_Ena						
15	MCU2_PLC_Prc_Cab_Mon_Ena						
16			MCU1_PLC_Prc_Cab_Mon_st	ENA	ENA		
17			MCU2_PLC_Prc_Cab_Mon_st	ENA	ENA		R=2, ENAからENAのためステータスの変化は判断できない。
18			MCU1_Press_Snsr1_St	NORM	NORM		
19			MCU2_Press_Snsr1_St	NORM	NORM		
20			MCU1_Press_Snsr2_St	NORM	NORM		
21			MCU2_Press_Snsr2_St	NORM	NORM		R=2
22			MCU1_Press_Snsr3_St	NORM	NORM		R=2
23			MCU2_Press_Snsr3_St	NORM	NORM		R=2
24			MCU1_PLC_Htr_St	-	0	記録のみ	R=2, 内部データの初期値が0。
25			MCU2_PLC_Htr_St	-	0	記録のみ	R=2, 内部データの初期値が0。
26	MCU1_PLC_Htr_Flt_Sel						
27	MCU2_PLC_Htr_Flt_Sel						
28			MCU1_PLC_Htr_St	FLT	FLT		R=4
29			MCU2_PLC_Htr_St	FLT	FLT		R=4
30	MCU1_At_Relf_EnaInh_Ena						
31	MCU2_At_Relf_EnaInh_Ena						
32			MCU1_AutoRlf_EnaSt	ENA	ENA		
33			MCU2_AutoRlf_EnaSt	ENA	ENA		
34	MCU1_At_Relf_Exe_Ena						
35	MCU2_At_Relf_Exe_Ena						
36			MCU1_AutoRlf_ExecSt	ON	ON		
37			MCU2_AutoRlf_ExecSt	ON	ON		
38							

cabin pressure monitoring : ENA

cabin pressure sensor : NORMAL

automatic cabin air relief : ENA

automatic cabin air relief : ON

Activity Execution (6/6)
Case Example (contd.)

expectation value

simulation output

L/N	コマンド変数名	設定値	テレメトリ変数名	期待値	実際の値	備考	補足
39			Cabin_Pressure_1	-	219→197		
40			Cabin_Pressure_2	-	219→197		
41			Cabin_Pressure_3	-	219→197	モニタ継続	R=8からR=21まで減少が続く。
42			MCU1_Press_Snsr1_St	-	NORM→MIN_ERR	モニタ継続	R=22
43			MCU2_Press_Snsr1_St	-	NORM→MIN_ERR	モニタ継続	R=22
44			MCU1_Press_Snsr2_St	-	NORM→MIN_ERR	モニタ継続	R=22
45			MCU2_Press_Snsr2_St	-	NORM→MIN_ERR	モニタ継続	R=22
46			MCU1_Press_Snsr3_St	-	NORM→MIN_ERR		
47			MCU2_Press_Snsr3_St	-	NORM→MIN_ERR		
48			VRV_A1_St	-	Open→Close		
49			VRV_B1_St	-	Open→Close		
50			VRV_A2_St	-	Close→Open→Close		
51			VRV_B2_St	-	Close→Open→Close	モニタ継続	R=13, R=22
52							

cabin pressure falls down continually.

If cabin pressure falls below lower limit, valves are closed.

Remarks about the simulation result

- In this case example, system model behaved as expected in the operation procedure.
- If there are some inconsistencies between system model and the operation procedure, simulation output would be different from expected values.

Lessons Learned

- **Modeling based on system specification**
  - Abstraction level of System Requirement Specification and Operation Procedure should be similar extent for modelling and integration.
  - Models are easy to build for those who can use C-language.
- **Validation of Operation Procedure**
  - Execution Conditions of the Simulation were defined as parameter changes with time.
  - Various failure conditions are possibly defined and Operation Procedure could be validated under the conditions.

Conclusion and Future Work

- **Conclusion**
  - Simulation with Executable Model was shown to be effective way to validate consistency between operational design and system/software design from early development phase.

- **Future Work**
  - Validation of Dynamic System Behaviour
    - Operational validation methodology should be developed with not only static model (status, command and telemetry) but also dynamic model.