Japan Aerospace Exploration Agency

Model-Based IV&V for an Operation Procedure

ADCSS2010@ESA ESTEC

New Approaches for Verification and Validation of Avionics

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)

November 02, 2010

Contents

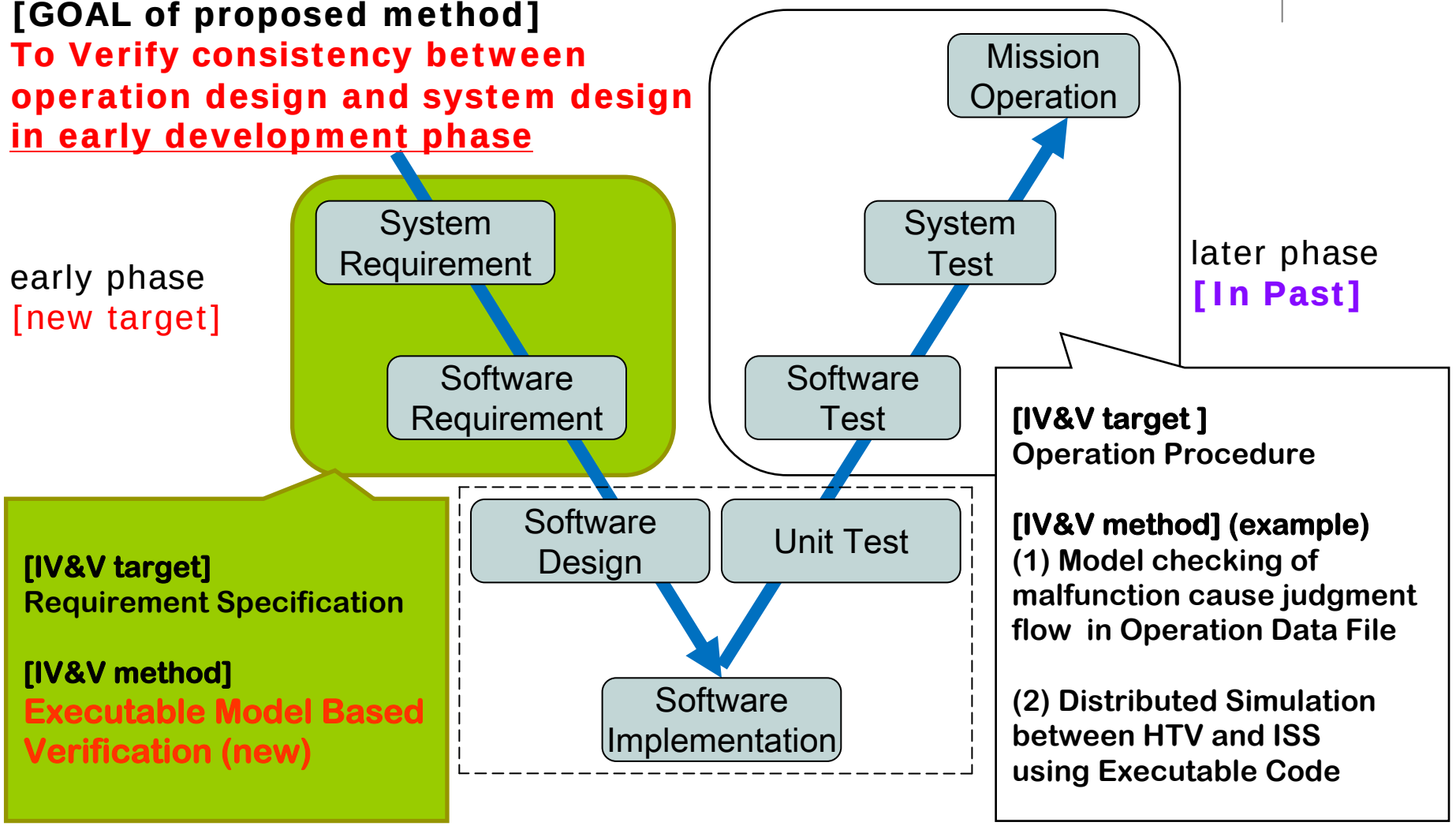
- Background
- Target System
- Modeling
- Simulation
- Lessons Learned
- Conclusion and Future Work

Background

IV&V for an Operation Procedure in JAXA

[GOAL of proposed method]

To Verify consistency between operation design and system design in early development phase

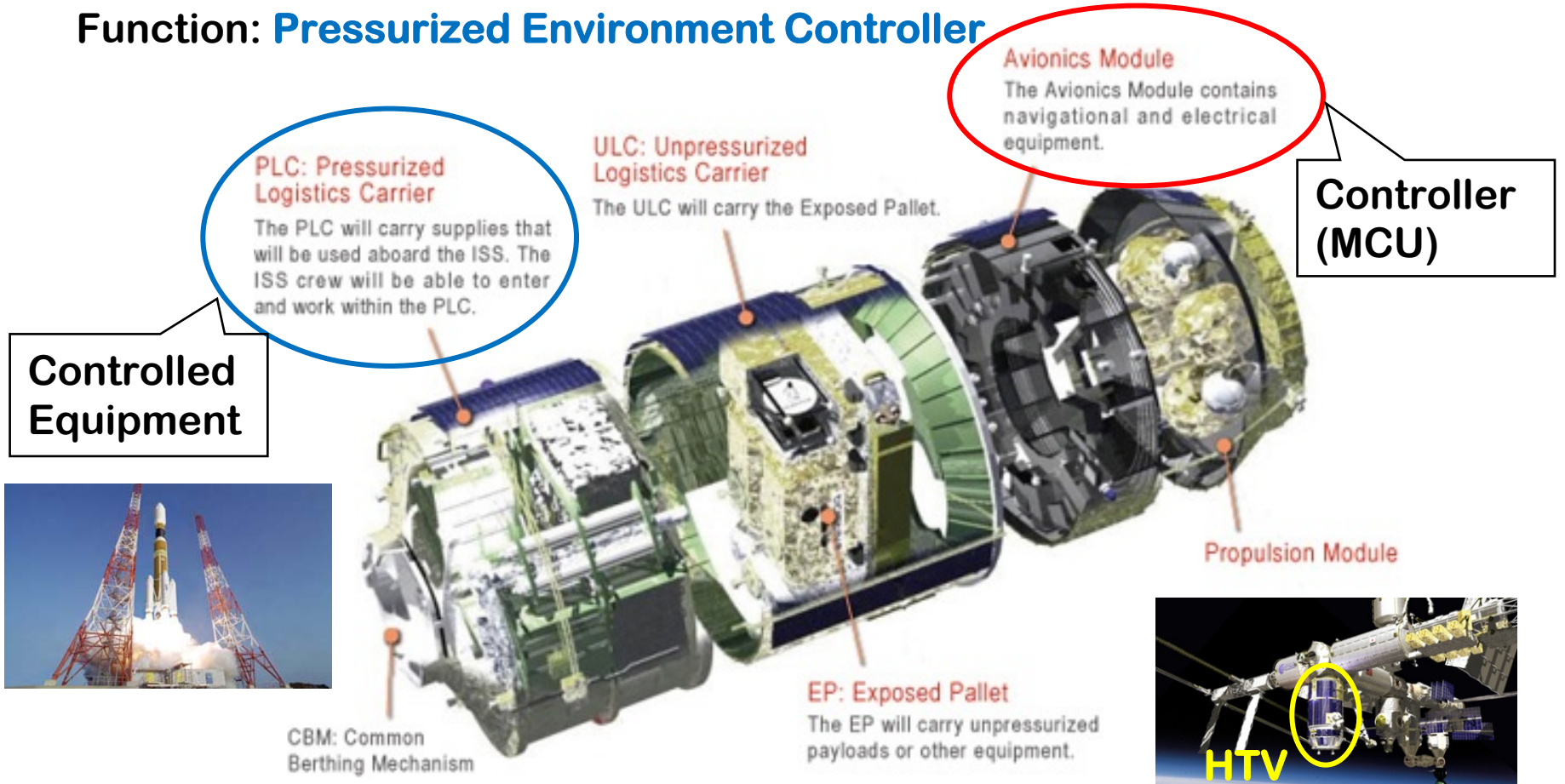


Target System

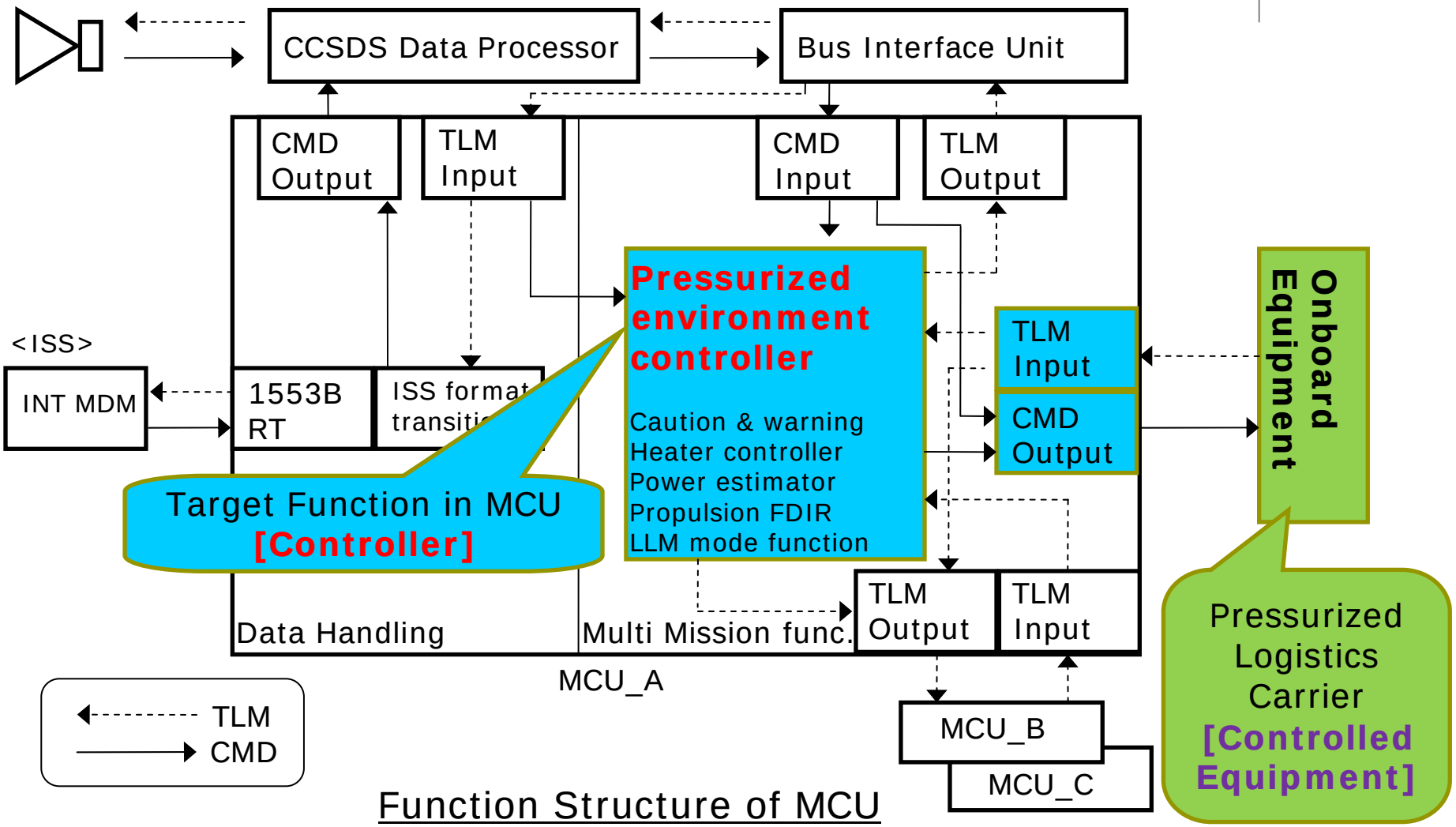
Spacecraft : **H-II Transfer Vehicle (HTV)**

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

Function: **Pressurized Environment Controller**

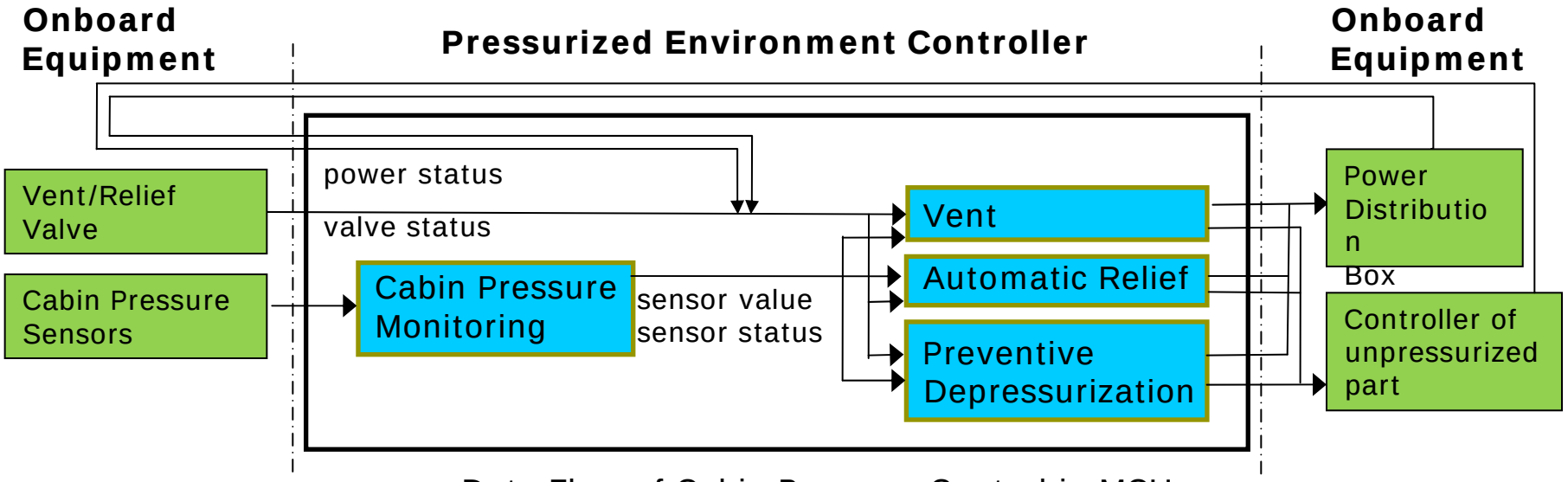


Target System (2/2)



Function Structure of MCU

Modeling
- Controller and Equipment Model -



Data Flow of Cabin Pressure Control in MCU

Onboard Equipment Model <sample>

If power status of the valve is "ON" and valve status is "OPEN", **then** Cabin Pressure decreases 1 unit value per second.

Controller Model <sample>

If sensor value 1 is over upper threshold and sensor value 2 is over upper threshold, **then** sensor value 3 becomes representative value, **else** Automatic Relief becomes non-executable.

Modeling Environment : **Microsoft Visual C++**

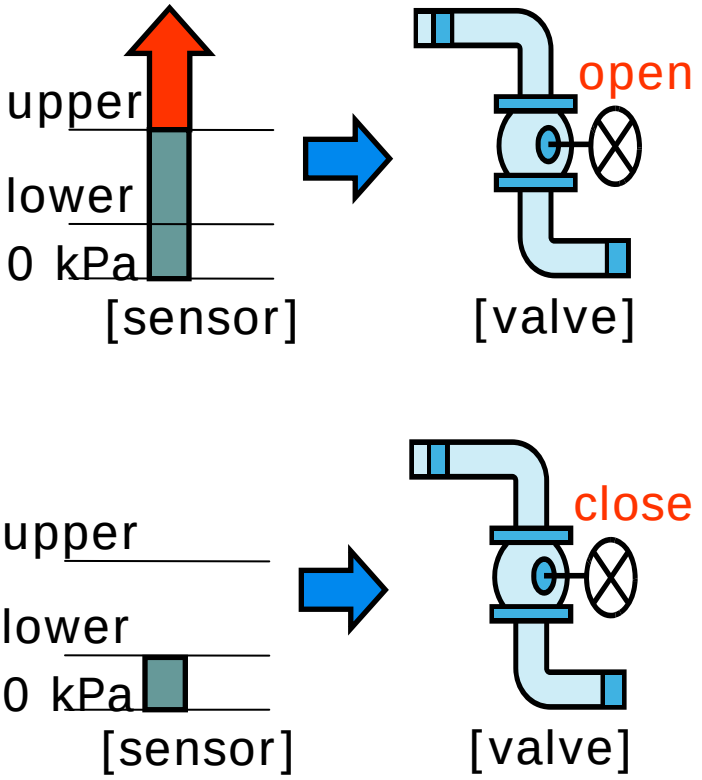
Simulation(1/3)
- Case Example -

- **Automatic Cabin Air Relief**

If cabin pressure goes over upper threshold,
cabin air is released for depressurization by opening relief valves
until cabin pressure falls down below lower threshold.

[Abstract of Operation Procedure]

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



Simulation(2/3)
- Result -

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		R=6
34	MCU1_At_Relf_Exe_Ena						
35	MCU2_At_Relf_Exe_Ena						
36			MCU1_AutoRlf_ExecSt	ON	ON		
37			MCU2_AutoRlf_ExecSt	ON	ON		R=6
38							

cabin pressure monitoring : ENA

cabin pressure sensor : NORMAL

automatic cabin air relief : ENA

automatic cabin air relief : ON

Simulation(3/3)
- Result (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 threshold, valves are closed.

Remarks about the simulation result

- Static system behavior such as state transitions can be verified by comparing simulation output with expectation value.

- Continuous system behavior can't be evaluated with only these static models. (e.g. software processing time)

Lessons Learned

- **Modeling**
  - **Setting of Abstraction Level**
    - In order to verify consistency between Operation Design and System Design, abstraction level of system models should be adjusted according to the Operation Design.
      (In the case example, Controller model was partly complemented by Detailed Design.)
- **Simulation**
  - **Setting of Execution Conditions**
    - Defined carefully about input/output timing of parameters
      (e.g. cabin pressure changes, status changes, etc.)
    - More advanced Conditions could be defined
      (e.g. Multiple Failure Conditions during Operation)

Conclusion and Future Work

- **Conclusion**
  - **Executable Model Based method was shown to be effective for IV&V in early development phase.**
    - **Consistency check between Operation and System Design with simply constructed models**
    - **Correction of ambiguity description in the Requirement Specification through Modeling**

- **Future Work**
  - **Feasibility research with other case examples**
    - **Interactive system behavior with multiple functions**
    - **Applying the method to other subsystems and projects**

Thank you for your attention!