

A Tool Set for Integrated Software and Hardware Dependability Analysis Using the Architecture Analysis and Design Language (AADL) and Error Model Annex

Myron Hecht, Alex Lam, Chris Vogl,

Presented to 2011 UML/AADL Workshop Las Vegas, NV

April, 2011

## Outline

- AADL vs. UML for Stochastic Analysis of Risk and Reliability
- AADL Error Annex
- Tool Set for Analyzing Risk and Reliability/Availability
- Satellite Example
- FMEA Generation
- Conclusions



# AADL vs. UML for Stochastic Analysis of Risk and Reliability

- Advantages
  - Objects directly represent real-time system hardware and software
  - Standard method for incorporation of quantitative attributes
    - Failure and Recovery Probabilistic Distributions
    - Parameters of those distributions
    - Probabilities and rates for individual transitions
  - Standard methods for representing propagation of failures across multiple components
    - Event ports for failure propagations
    - Guards to enable conditional propagations (important for abstractions and reuse)
- Drawbacks
  - No commercial quality tools
    - Public domain tools are available and usable but not bug free

## AADL Error Annex

- AADL annex that supports stochastic analysis
- Defines error model
  - State transition diagram that represents normal and failed states
  - Error models can be associated with hardware components, software components, connections, and "system" (composite) components
- Error model consists of
  - State definitions
  - Propagations from and to other components
  - Probability distribution and parameter definitions
  - Allowed state transitions and probabilities





## AADL Tool Set

- Eclipse Development Environment (Ganymede) and Eclipse Modeling Framework (EMF)
- Component plug-ins
  - TopCASED graphical editor to create AADL architecture diagrams (SEI, Aerospace modifications)
  - Error Model Editor graphical editor to create AADL error model diagrams (Aerospace)
  - **OSATE** AADL generator (SEI, Aerospace modifications)
  - ADAPT-M Stochastic Petri net to MoBIUS stochastic analysis network tool ((SEI/LAAS Toulouse and Aerospace)
  - MoBIUS Quantitative Dependability modeling and prediction tool (University of Illinois, Champaign Urbana)
  - FMEAGEN FMEA Generator (Aerospace)

### AADL Modeling Tool Set Data Flow



#### **Tool Set Screen Shot**



# AADL Components (graphical representation)



# Simple Satellite Hardware/Software Architecture Representation



# Simple Satellite MDDA Representation

- Bus and Payload Computers
  - Object names:
    - SBCU (Spacecraft Bus Computer Unit
    - SPCU (Spacecraft Payload Computer Unit)
  - Payload relies on the Bus, thus whenever the Bus is in Standby, the Payload goes to Standby.



# Spacecraft Bus Control Unit (SBCU)

- Architecture Description
  - Dual redundant Bus Control Processors (BCP)
  - Each runs identical copy of bus control software (BCS)
- Failure Behavior
  - Permanent Failures (primarily hardware)
    - A hardware failure results in loss of a processor
    - Two permanent failures result in a mission loss
  - Transient Failures (primarily software)
    - Once BCP is active, when it fails control immediately switches to other processor (hot standby)
    - Switching is not always successful ("imperfect switching)
      - If successful, then a short ("minor failure") occurs
      - If not successful, then a longer ("major failure") occurs

# SBCU AADL Architecture Graphical Representation

#### SBCU Top Level Diagram



#### **Reusable AADL Representation of SBCU**



# SBCU Error Model Representation using Graphical Editor



# Stochastic Analysis Representation (product of ADAPT-M conversion)

		<u> </u>		·····		
SBCU_Pri	maryChannel_BCP_Normal_Fail_default	SBCU_PrimaryCh	annel BCP_Eailed	SBC PrimaryChan	el_BCP_Norma	_Fall
SBCU_Prima	Channel_BCE_Failed_out_CPUFail_default			SBCU_P <mark>_haryChannel</mark>	BCP_Failed_out	CPUFail
3BCU_PrimaryChannel_BCS_CPUFail_from	ILSS SpaceV bicle SV Instance SBCU PrimaryCh	anner BERCH Remain/Cha	nnel_BCB_Normal SBCU_PrimaryChar	nnel_BCS_CPUFail_romLSS_Spa	e <mark>eVehicle<u>i</u>s∨_in</mark>	stance_SBCU_PrimaryChannel_BCP_1
SBCU_PrimaryChannel_BCS_CPUFail_from	ILSS Space V bicle_SV_Instance_SBCU_PrimaryCh	annel BCP 2 default	HELACP Stead In Brienary Char	ppet_BCS_CPUFaiteromLSS_Spa	e <mark>e∀ehicle_S∀_ln</mark>	stance_SBCU_PrimaryChannel_BCP_2
3BCU_PrimaryChannel_BCS_CPUFail_from	ILSS Space bicle SV Instance SBC& PrimaryCh	nannel_B6R_3_default	SBCU PrimaryChar	nnel_BCS_CPUFaiteromLSS_Spa	é <mark>eVehicle_S∨_in</mark>	stance_SBCU_PrimaryChannel_BCP_3
SBCU_PrimaryChannel_BCS_CPUFail_from	ILSS Space v nicle SV Instance SBCU Primary Ch		nnel BCP Standby SBCU_PrimaryChar	anel_BC <u>8_CPU5ail_romLS8_Spa</u>	evehicle_SV_In	stance_SBCU_PrimaryChannel_BCP_4
SBCU_Pri	anyChanner S Active Failing default	SBSU_PrimaryChanne	BCP CPUFail Failed	SBCU	E <u>BCSLActive</u> l	Failing
SBCU_F	ImaryChanne ECS_Bown Eall-Level2		abnel Bits Artive	SBC PrimaryCha	nel_BCS_Down	Fail
SBCU_PrimaryCha	nnel_BCS_Drive_bevel1_Level4_Repair_default			SBCU_Primate Channel_BCS	Down_Level1_L	evel1_Repair
SBCU_PrimaryCha	nnel_BCS_Dave_Devel2_Level2_Repair_default	SBCU PRImary Chapnel	BCS Report Terminated	8BCU_Primatehannel_BCS	Down_Level2_L	evel2_Repair
SBCU_PrimaryCrla	annel_BCS_B_pontBown_out_BCSDown_default	SBCU Primarystann	el BOS Dawn Level	SBCU_Primatchannel_BC	<mark>_ReportDown_c</mark>	út_BCSDown
SBCU_PrimaryChan	iel_BCS_Rep_dStandby_out_BCSStandby_defaults		$\nabla X X / $	8BCU_Primaty annel_BCS_I	ReportStandby_c	ut_BCSStandby
SBC⊍_PrimaryChannel_	BCS_Report Perminated_out_BCSTenninated_defa	ultSBCV_PrimaryCharl	nel BCS Terminated	SBCU_PrimaryChatel_BCS_Re	rtTerminated_c	ut_BCSTerminated
SBCU_Ba	ckupChannel BCP_Normal_Pail_default	SBCU_PrimaryChann	el_BCS_Down_Level2	980	<mark>r</mark> el_BCP_Norma	Fail
SBCU_Backug	Channel_BCP_Failed_but_CPUFail_default			SECU_E	BCP_Failed_out	CPUFail
SBCU_BackupChannel_BCS_CPUFall_from	<u>ILSS_Space</u>	ianner_BOPdevallit		nnel_BC8_CPUF/alteromLSS_Spa	<mark>e</mark> ∋∀ehicle_S∀_ln	stance_SBCU_BackupChannel_BCP_1
SBCU_BackupChannel_BCS_CPUFail_from	ILSS_Space/pide_SV_Instance_SBCU_BackupCh		el_CS_BBOOMBARhupChar	nnel_BCS_CPUFzile_romLSS_Spa	s <mark>eVehicle_SV_In</mark>	tance_SBCU_BackupChannel_BCP_2
SBCU_BackupChannel_BCS_CPUFail_from	ILSS_SpaceVostance_SBCU_BackupCh	iange/ BCR & deisult		ynel_BCS_CPVFan <mark>romLSS_Spa</mark>	<mark>e</mark> ≥Vehicle_SV_In	tance_SBCU_BackupChannel_BCP_3
SBCU_BackupChannel_BCS_CPUFail_from	ILSS_Space/picke_SV_Instance_SBCU_BackupCV	langel_BCF_4_default *	SBOU_BackupChar	nnél_BCS_CPUF# <b></b>	é <mark>∛Vehícíe<u>`</u>SV_in</mark>	tance_SBCU_BackupChannel_BCP_4
SBCU_Bae	kupChannel S. Abtive Failing default	SBC/0_PhrafaryChanne	L_BCS_ReportStandby	/ /sßCuterackupChar	T_BCS_Active_I	Failing
	ŧsknikchanne Ekszkniktéan-fekelt	SBCU Rrimary Channel, BC	S_BCSDown Report Down	/// SBC BackupCha	r <mark>iel_BCS_Down</mark>	Fail
SBCU_BackupCha	nnel_BCS_Depril_Level1_Level1_Repair_default/			SPCV_Backuthannel_BCS	Down_Level1_L	evel1_Repair
SBCU_BackupCha	nnel BCS Dimn Level2 Cevel2 Repair default25		BCSStarudy_Reportstatud	V//SBCU_Backuthannel_BC9	Down_Level2_L	evel2_Repair
SBCU_BackupCha	annel_BCS_EPPORTDovin_out_BCSDown_derout_	PrimaryShannel_BCS_BC	STerminated_ReportTermin	aled /SBCU_Back	<mark>6</mark> _ReportDown_c	ut_BCSDown
SBCU_BackupChan	<u>iel_BCS_Reput</u> Standby_out_BCSStandby_default	SBCU BackunCh			R <mark>eportStandby_</mark> c	ut_BCSStandby
SBCU_BackupChannel	-BCS_Report Printated out BCSTerminated defai			3800XBackupChatel_BCS_Re	Terminated_c	ut_BCSTerminated
SBC	HTMS_SWILL BUPTOR SWITCH Kairs	SBCU_BackupGha	innel_BCP_Normal		ChingPtoB_Swite	h
	U_FMS_SWIE CONTOP_SWICH CAN	SBQU BackupChan	nel BCR Terminated	K // K Strategy	<mark>ŧ</mark> :hingBtoP_Swite	þ
SBCU_Fv	<u>AS_SWITCHFalled</u> out SwitchFall default		• _X / _//X		Failed_out_Swite	hFall
SBCU_BackupChannel_BCS_Switch	IF all_tromLS_Space vehicle/SY_Instance_SBC0_F	-мз_х анаштваскирста	nnei BUP-Standard (U_Back	xpChannel_609_	E <mark>SS_SpaceVehic</mark>	le_SV_instance_SBCU_FMS_1
SBCU_PrimaryChannel_BCS_Switch	IFail from LS Space vertice By Apetance SBCUAF	-MS 1 gerault SBCO Backupchanne	LBCP_CPUFail Bared Prim	arXChannel_BCS_ <b>4</b> itchFail_from	<mark>l SS_Space∀ehic</mark>	le_SV_Instance_SBCU_FMS_1
					CP_Normal_Fa	1
SPCU_Phi	mary PCP Epido out XCPUKar aerault	X Specification			Failed_out_CP	ÚFail.
SPCU_Primary_PCS_CPUFail_from	ILSS_Space_price_SV/Instance_SPON_Primary_R	KrsBederanter	BCS_ReportTernanBated	nary_PC6_QPU#4	e <mark>eVehicle_</mark> SV_In	stance_SPCU_Primary_PCP_1
SPCU_Primary_PCS_CPUFail_from	ILSS Space Primary P		BOS DOWD LEVEL	vary_PCS_CAUF01_romLSS_Spa	eVehicle_SV_In	stance_SPCU_Primary_PCP_2
SPCL	<u>7. Primary PP</u> Active Pail_default	X = 11 =			CS_Active_Fai	





#### **Results: Mission Duration vs. Processor Reliability**



# Automatically Generated FMEA Features

- Automatically Generated
  - Utilizes information in petri nets and error models
  - Automation enables analyses to be performed repeatedly
    - Manual analyses are constrained because of cost (typically done only once)
- No limit to number of effect levels
  - Conventional manually generated FMEAs are done to 3 levels (immediate, next level, end effect)
  - Propagations are traced across components
- Editable
  - Output Generated in MS Excel

#### Example: Supplemental Restraint System



Generation of FMEA from Petri Net of Error Models



## Results: Automatically Generated FMEA

G	FI 1 2 3 7 SRS_FMEA3 [Compatibility Mode] - Microsoft Excel											
	Home Insert PageLayout Formulas Data Review View Developer Livelink											
	$\overline{K3}$ $\overline{f_x}$ $\overline{f_x}$											
	В	С	D	E	F	G	Н		J	K		
1												
2	SRS1	Project	Teset	Date:	2/3/2010							
4	SILOT	T TOJECI.	16361	Date.	2/3/2010							
5	ltem	Initial Failure Mode	1st Level Effect	Failure Mode	2nd Level Effect	Failure Mode	3rd Level Effect	Severity	Mitigation	Comments		
6	Accelerometer	Failure	Sensor.Accelerometer Failed	SensorFail from Accelerometer to ControlUnit	CPU.ControlUnit Failed	CPUFail from ControlUnit to Airbag	Actuator.Airbag NotReady	[State Property]	[Designer Input]	[Analyst Input]		
7	ControlUnit	Failure	CPU.ControlUnit Failed	CPUFail from ControlUnit to Airbag	Actuator.Airbag NotReady			[State Property]	[Designer Input]	[Analyst Input]		
			Actuator Airbag					[State				
8	Actuator	Failure	NotReady					- Property]	[Designer Input]	[Analyst Input]		

Enhanced formatting for presentation purposes

# Excerpt of Automatically Generated FMEA for 10-state

ID	ltem	Initial Failure Mode	1st Level Effect	Transition	2nd Level Effect	Transition	3rd Level Effect	Transition	4th Level Effect	Transition	5th Level Effect
1.1	SBCU.Primary_SU	Failure	SU.SBCU_Primary ReportDown	SBCUSdown from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_PrimaryDown	Failure_case_Minor from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary DownMinor	RecoverMinorfrom SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary ReportRecover	SBCUSrecover from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary HotStandby
										SBCU.FMS	FMS.SBCU UsingPrimary
1.2.1						SBCU.PMS guarain PrimaryDown from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU PrimaryisDown				
1.2.2.1						Failure_case_Major from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary DownMajor	RecoverMajorfrom SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary ReportRecover	SBCUSrecover from SBCU.Primary_SU to SBCU.Primary_SU	SU.SBCU_Primary HotStandby
1.2.2.2										SBCUSrecover from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU UsingPrimary
1.3						SBCU.FMS guardin PrimaryDown from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU PrimaryisDown				
2.1.1	SBCU.Backup_SU	Failure	SU.SBCU_Backup ReportDown	SBCUSdown from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup Down	Failure_case_Minor from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup DownMinor	RecoverMinorfrom SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup ReportRecover	SBCUSrecover from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup HotStandby
2.1.2										SBCUSrecover from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU UsingBackup
2.2						SBCU.FMS guardin BackupDown from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU Down				
2.3						SPCU.FMS guardin BusDown from SBCU.FMS to SPCU.FMS	FMS.SPCU WaitingForBus				
2.4						SPCU.Primary_SU guardin FMSstandby from SPCU.FMS to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby				
2.5.1						Failure_case_Major from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup DownMajor	RecoverMajorfrom SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup ReportRecover	SBCUSrecover from SBCU.Backup_SU to SBCU.Backup_SU	SU.SBCU_Backup HotStandby
2.5.2										SBCUSrecover from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU UsingBackup
2.6						SBCU.FMS guardin BackupDown from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU Down				
2.7						SPCU.FMS guardin BusDown from SBCU.FMS to SPCU.FMS	FMS.SPCU WaitingForBus				
2.8						SPCU.Primary_SU guardin FMSstandby from SPCU.FMS to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby				
3.1	SBCU.Primary_PU	Failure	PU.SBCU Terminated	CPUfail from SBCU.Primary_PU to SBCU.Primary_SU	SU.SBCU_Primary Terminated						
3.2				SBCU.FMS guardin PrimaryTerminated from SBCU.Primary_SU to SBCU.FMS	FMS.SBCU PrimaryisTerminated						
4.1	SBCU.Backup_PU	Failure	PU.SBCU Terminated	CPUfail from SBCU.Backup_PU to SBCU.Backup_SU	SU.SBCU_Backup Terminated						
4.2				SBCU.FMS guardin Backup Terminated from SBCU.Backup_SU to SBCU.FMS	FMS.SBCU Down						
4.3				SPCU.FMS guardin BusDown from SBCU.FMS to SPCU.FMS	FMS.SPCU WaitingForBus						
4.4				SPCU.Primary_SU guardin FMSstandby from SPCU.FMS to SPCU.Primary_SU	SU.SPCU_PrimaryColdStandby						
5.1	SPCU.Primary_SU	Failure	SU.SPCU_Primary ReportDown	SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary Down	Recover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ReportRecover	SPCUSrecover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby		
								SPCUSrecover from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU UsingPrimary		
5.2				SPCU.FMS guardin PrimaryDown from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU Down						
6	SPCU.Backup_SU	Failure	SU.SPCU_Backup ReportDown	SPCUSdown from SPCU.Backup_SU to SPCU.Backup_SU	SU.SPCU_Backup Down	Recover from SPCU.Backup_SU to SPCU.Backup_SU	SU.SPCU_Backup ReportRecover	SPCUSrecover from SPCU.Backup_SU to SPCU.Backup_SU	SU.SPCU_Backup ColdStandby		
7.1	SPCU.Primary_SU	Failure	SU.SPCU_Primary ReportDown	SPCUSdown from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary Down	Recover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ReportRecover	SPCUSrecover from SPCU.Primary_SU to SPCU.Primary_SU	SU.SPCU_Primary ColdStandby		
7.2				SPCU.FMS guardin BackupDown from SPCU.Backup_SU to SPCU.FMS	FMS.SPCU Down						
B.1	SPCU.Primary_PU	Failure	PU.SPCU Terminated	CPUfail from SPCU.Primary_PU to SPCU.Primary_SU	SU.SPCU_Primary Terminated						
8.2				SPCU.FMS guardin PrimaryTerminated from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU PrimaryisTerminated						
8.2				CPUfail from SPCU.Primary_PU to SPCU.Primary_SU	SU.SPCU_Primary Terminated						
8.4				SPCU.FMS guardin PrimaryTerminated from SPCU.Primary_SU to SPCU.FMS	FMS.SPCU PrimaryisTerminated						
9.1	SPCU.Backup_PU	Failure	PU.SPCU Terminated	CPUfail from SPCU.Backup_PU to SPCU.Backup_SU	SU.SPCU_Backup Terminated						
9.2				SPCU.FMS guardin BackupTerminated from SPCU.Backup_SU to SPCU.FMS	FMS.SPCU Down						
9.3				CPUfail from SPCU.Backup_PU to SPCU.Backup_SU	SU.SPCU_Backup Terminated						
9.4				SPCU.FMS guardin BackupTerminated from SPCU.Backup_SU to SPCU.FMS	FMS.SPCU Down						



### Conclusions

- A new generation tool set for quantitative stochastic analysis and qualitative Failure Modes and Effects Analysis (FMEAs) for space systems is under development
  - Based on use of the Architecture Analysis and Design Language (AADL)
  - Graphically oriented
  - Modularized with reusable components
- Results will be able to support decisions from concept development through detailed design
  - Extent and type of redundancy
  - Tradeoffs of reliability vs. Weight, power, and functional capability
  - Failure rate and recovery time requirements
  - Strategies for recovering from computing disruptions
  - Handling failure propagation and common mode failures