Polyspace Code Verification

Developer Report for: Autopilot

Report Author: bpotter

Polyspace Code Verification : Developer Report for: Autopilot

Report Author: bpotter

Publication date 03-Feb-2014 08:34:17

```
Verification Author(s): bpotter
Polyspace Verions(s): 9.0 (R2013b)
Project Version(s): 1.0
```

Table of Contents

List of Tables

Chapter 1. Polyspace Code Verification Summary

Table 1.1. Code Metrics Summary

Code Metrics	
Polyspace Code Metrics	Enabled
Number of Result Sets	x 1
Pass/Fail	-

Table 1.2. Coding Rules Summary - Custom Rules Checker

Coding Rules	
Custom Rules Checker	Disabled
Pass/Fail	-

Table 1.3. Coding Rules Summary - MISRA AC AGC Checker

Coding Rules	
MISRA AC AGC Checker	Enabled
Number of Result Sets	x 1
Errors	0
Warnings	0
Pass/Fail	-

Table 1.4. Run-Time Checks Summary

Run-Time Checks	
Polyspace Code Prover	Enabled
Number of Result Sets	x 1
Number of Red Run-Time Checks	0
Number of Gray Run-Time Checks	0
Number of Orange Run-Time Checks	3

Run-Time Checks	
Number of Green Run-Time Checks	547
Proven	99.5%
Pass/Fail	-

Developer Name:

Date Reviewed:

Comments

Approved By:

Approved Date:

Chapter 2. Polyspace Proven

Table of Contents

Run-Time Checks Summary for Autopilot - Autopilot

File	Proven	Green	Red	Gray	Orange
__polyspace__stdstubs.c	NA	0	0	0	0
Altitude_Mode.c	100.0%	114	0	0	0
attitude_controller.c	100.0%	84	0	0	0
pitch_ap.c	100.0%	76	0	0	0
roll_ap.c	100.0%	64	0	0	0
__polyspace_main.c	100.0%	63	0	0	0
yaw_damper.c	100.0%	41	0	0	0
Heading_Mode.c	100.0%	36	0	0	0
Autopilot.c	100.0%	11	0	0	0
look1_binlag.c	95.1%	58	0	0	3
Total	**99.5%**	**547**	**0**	**0**	**3**

Globally Proven:99.5%

Code Coverage

Result Set	Code Coverage
Autopilot - Autopilot	100%

Chapter 3. Code Metrics

Table of Contents

Code Metrics Summary for: Autopilot - Autopilot

Table 3.1. Project Metrics

Metric	Value	Comments
Project Name	Autopilot	-
Number of Direct Recursions	0	-
Number of Files	11	-
Number of Headers	42	-
Number of Recursions	0	-
Number of Protected Shared Variables	0	-
Number of Unprotected Shared Variables	0	-

Table 3.2. File Metrics

Metric	Values (Min .. Max)	Comments
Comment Density	0 .. 100	-
Estimated Function Coupling	0 .. 8	-
Lines	18 .. 207	-
Lines Without Comment	5 .. 91	-

Table 3.3. Function Metrics

Metric	Values (Min .. Max)	Comments
Cyclomatic Complexity	1 .. 11	-

Metric	Values (Min .. Max)	Comments
Language Scope	1.3 .. 6.8	-
Number of Call Levels	1 .. 3	-
Number of Call Occurrences	0 .. 6	-
Number of Called Functions	0 .. 5	-
Number of Calling Functions	0 .. 2	-
Number of Executable Lines	1 .. 50	-
Number of Function Parameters	0 .. 17	-
Number of Goto Statements	0 .. 0	-
Number of Instructions	1 .. 39	-
Number of Lines Within Body	2 .. 153	-
Number of Paths	1 .. 576	-
Number of Return Statements	0 .. 1	-

Chapter 4. MISRA AC AGC Rules Results

Table of Contents

MISRA AC AGC Summary - Violations by File

No MISRA AC AGC Summary - Violations by File violations were found.

MISRA-AC-AGC Warnings

No MISRA AC AGC warnings were found.

MISRA-AC-AGC Errors

No MISRA AC AGC errors were found.

Chapter 5. Polyspace Run-Time Checks Results

Table of Contents

Proven Run-Time Violations

No red checks were found.

Proven Unreachable Code Branches

No unreachable branch checks were found.

Unreachable Functions

No unreachable functions were found.

Unproven Run-Time Checks

Table 5.1. look1_binlag.c

Check	ID	Function	Line	Col	Detail	Jus	Class	Status	Comment
Overflow	2	look1_binlag()	51	29	Unproven: operation [/] on float may overflow (on MIN or MAX bounds of FLOAT64)	No	-	-	-
Division by Zero	1	look1_binlag()	51	29	Warning: float division by zero may occur	No	-	-	-
Overflow	3	look1_binlag()	65	29	Unproven: operation [*] on float may overflow (on MIN or MAX bounds of FLOAT64)	No	-	-	-

Chapter 6. Appendix 1 - Configuration Settings

Table of Contents

Polyspace Settings

Option	Value
-allow-negative-operand-in-shift	true
-author	bpotter
-big-endian	true
-boolean-types	[boolean_T]
-D1	main=main_rtwec
-D10	MULTI_INSTANCE_CODE=0
-D11	INTEGER_CODE=0
-D12	MT=0
-D13	CLASSIC_INTERFACE=0
-D14	TID01EQ=0
-D15	PORTABLE_WORDSIZES
-D2	__restrict__=
-D3	MODEL=Autopilot
-D4	NUMST=1
-D5	NCSTATES=0
-D6	HAVESTDIO
-D7	ONESTEPFCN=1
-D8	TERMFCN=0

Option	Value
-D9	MAT_FILE=0
-data-range-specifications	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\results_Autopilot\Autopilot\Autopilot_drs.txt
-date	18/11/2013
-dialect	none
-dos	true
-double-is-64bits	true
-from	scratch
-functions-called-before-loop	[Autopilot_initialize]
-functions-called-in-loop	custom=Autopilot_step
-I1	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\Autopilot_ert_rtw
-I2	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\Altitude_Mode
-I3	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\Heading_Mode
-I4	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert_sharedutils
-I5	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\attitude_controller
-I6	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\pitch_ap
-I7	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\roll_ap
-I8	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\yaw_damper
-ignore-constant-overflows	true
-includes-to-ignore1	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\Autopilot_ert_rtw
-includes-to-ignore2	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\Altitude_Mode
-includes-to-ignore3	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\Heading_Mode
-includes-to-ignore4	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert_sharedutils
-includes-to-ignore5	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\attitude_controller
-includes-to-ignore6	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\pitch_ap
-includes-to-ignore7	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\roll_ap
-includes-to-ignore8	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\slprj\ert\yaw_damper
-int-is-32bits	true
-lang	C

Option	Value
-main-generator	true
-misra-ac-agc	OBL-rules
-O	-O2
-OS-target	no-predefined-OS
-pointer-is-32bits	true
-polyspace-version	9.0 (R2013b)
-prog	Autopilot
-report-output-format	PDF
-report-template	Polyspace-Doc\Developer.rpt
-results-dir	C:\Users\bpotter\LocalWorkArea\demos\autopilot_R2013b_workarea\results_Autopilot\Autopilot
-scalar-overflows-behavior	truncate-on-error
-scalar-overflows-checks	signed
-target	mcpu
-to	Software Safety Analysis level 4
-variables-written-before-loop	none
-variables-written-in-loop	custom=Autopilot_U
-verif-version	1.0

DRS Configuration Data

DRS - Global Variables

Table 6.1. File: C:\ Users\ bpotter\ LocalWorkArea\ demos\ autopilot_R2013b_workarea\ Autopilot_ert_rtw\ Autopilot.c

Name	Type	Init Mode	Init Range	Initialize Pointer	# Allocated Objects	Init Allocated	Global Assert	Assert Range
Autopilot_U.AirData.airspeed	float64	INIT	0..1000	-	-	-	NO	-
Autopilot_U.AirData.alpha (Non Applicable)	-	INIT	-90..90	-	-	-	NO	min..max
Autopilot_U.AirData.alt	float64	INIT	0..65000	-	-	-	NO	-

Name	Type	Init Mode	Init Range	Initialize Pointer	# Allocated Objects	Init Allocated	Global Assert	Assert Range
Autopilot_U.AirData.altRate	float64	INIT	-20000..20000	-	-	-	NO	-
Autopilot_U.AirData.beta (Non Applicable)	-	INIT	-180..180	-	-	-	NO	min..max
Autopilot_U.ALTMode	uint8	INIT	0..1	-	-	-	NO	-
Autopilot_U.ALTRef	float64	INIT	0..65000	-	-	-	NO	-
Autopilot_U.APeng	uint8	INIT	0..1	-	-	-	NO	-
Autopilot_U.HDGmode	uint8	INIT	0..1	-	-	-	NO	-
Autopilot_U.HDGref	float64	INIT	-180..180	-	-	-	NO	-
Autopilot_U.Inertial.p	float64	INIT	-180..180	-	-	-	NO	-
Autopilot_U.Inertial.phi	float64	INIT	-180..180	-	-	-	NO	-
Autopilot_U.Inertial.psi	float64	INIT	-180..180	-	-	-	NO	-
Autopilot_U.Inertial.q	float64	INIT	-90..90	-	-	-	NO	-
Autopilot_U.Inertial.r	float64	INIT	-180..180	-	-	-	NO	-
Autopilot_U.Inertial.theta	float64	INIT	-90..90	-	-	-	NO	-
Autopilot_U.PitchWheel	float64	INIT	-30..30	-	-	-	NO	-
Autopilot_U.TurnKnob	float64	INIT	-45..45	-	-	-	NO	-

Chapter 7. Appendix 2 - Definitions

Table 7.1. Run-Time Checks Acronyms for C

Acronym	Definition
ABS_ADDR	Absolute address
ASRT	User assertion
COR	Correctness condition
Float OVFL	Float Overflow
IDP	Illegally dereferenced pointer
IRV	Initialized return value
K_NTC	Known non-terminating call
NIP	Non-initialized pointer
NIV	Non-initialized variable
NIVL	Non-initialized local variable
NTC	Non-terminating call
NTL	Non-terminating loop
OBAI	Out of bounds array index
OVFL	Overflow
SHF	Shift operations
STD_LIB	Invalid use of standard library routine
Scalar OVFL	Scalar Overflow
UNR	Unreachable code
VOA	Value On Assigned
ZDV	Division by Zero

Table 7.2. Abbreviations

Abbreviation	Definition
Col	Column

Abbreviation	Definition
Jus	Justified
Rvd	Reviewed
SQO	Software Quality Objectives
OBL	Obligatory
REC	Required
READ	Readability
NA	Not Available