

LFR-FSW - Bug #801

Analyse Logiscope LFR_3.1.0.4 : Don_Initialisation_P2 Severity is High

19/10/2016 02:13 PM - William Recart

Status:	Closed	Start date:	19/10/2016
Priority:	Low	Due date:	
Assignee:	William Recart	% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:		Spent time:	0.00 hour
revision:	r0		

Description

Rappel de la règle :

Don_Initialisation_P2 :

Definition:

All variables must be initialized before they are used, without taking into account on the default value attributed by the compiler.

Global variables, parameters of a function in the function body, and data fields of a class in its methods are considered to be initialized.

Justification:

Not all compilers give the same default values. Unexpected behaviour can be avoided with better control over variable values.

Limitations:

This rule is not violated in the following cases:

If an array, a struct or a class are used, they will be considered initialized as soon as a part of them has been initialized.

For example:

```
int a2;
int b2 = {6, 7};
int h;

a[0] = b[0]; // ok
h = a[1];    // ok

struct
{
    int i;
    int j;
} e, f;

e.i = 0;
g = e;        // ok
```

This rule is violated in the following cases where initialization is uncertain:

Using a variable in a function call is considered as "being used": if it is not initialized, the rule will be violated.

This will occur whatever the use of the function, even initializing the variable.

In cases including a conditional initialization, the rule is violated even though the variable may well be initialized.

```
int i, j, k;
j = func();
if (j)
    i = 0;
k = i;        // violation
```

This applies even when there is an else branch, for example in

```
int i, j, k;  
j = func();  
if (j)  
i = 0;  
else  
i = 5;  
k = i; // violation  
where initialization is certain.
```

In the case of a loop, for example

```
int j, k;  
for (int i=0; i<glob; i++) {  
j=func(i);  
}  
k = j; // violation  
where glob is a global variable, depending on the value of glob, j will have been  
initialized or not: the rule is violated, even if the loop condition occurs or not.
```

La règle n'est pas respectée dans 352 cas d'après Logiscope:

Fichier avf0_prc0.c : lignes 70, 77, 174, 207, 210, 218, 221, 227, 230, 236, 239, 248, 253, 262, 262, 287, 289, 290, 293, 300, 302, 303, 306, 325, 327, 328, 331, 337, 339, 340, 343, 357, 360, 366

Fichier avf1_prc1.c : lignes 71, 78, 175, 208, 211, 219, 222, 228, 231, 240, 245, 254, 254, 279, 281, 282, 285, 292, 294, 295, 298, 317, 319, 320, 323, 329, 331, 332, 335, 349, 352, 358

Fichier avf2_prc2.c : lignes 59, 66, 125, 156, 159, 163, 168, 177, 177, 202, 204, 205, 205, 208, 216, 218, 219, 222, 238, 244

Fichier fsw_init.c : lignes 274, 278, 743, 752, 761, 770, 779, 805, 891, 893

Fichier fsw_misc.c : lignes 30, 195, 210, 235, 260, 262, 270, 323, 378, 379, 565, 567, 802, 802, 803, 803, 805, 806, 807, 808

Fichier fsw_processing.c : ligne 574

Fichier fsw_spacewire.c : lignes 45, 59, 60, 66, 67, 136, 142, 152, 166, 173, 173, 175, 175, 184, 186, 186, 186, 188, 193, 193, 199, 240, 250, 250, 259, 314, 329, 346, 348, 349, 352, 406, 522, 588, 611, 613, 615, 617, 619, 621, 623, 625, 627, 629, 631, 649, 674, 674, 681, 681, 688, 688, 695, 695, 702, 702, 709, 709, 716, 716, 723, 723, 730, 730, 737, 737, 744, 744, 754, 754, 757, 1122, 1124, 1125, 1208, 1209, 1211, 1296, 1298, 1299, 1360, 1362, 1363, 1440, 1442, 1443, 1520, 1522, 1523, 1586, 1586

Fichier lfr_cpu_usage_report.c : ligne 110

Fichier tc_acceptance.c : lignes 130, 130, 204, 287, 470

Fichier tc_handler.c : lignes 39, 45, 58, 58, 58, 67, 71, 71, 72, 72, 75, 76, 76, 79, 79, 80, 80, 83, 83, 84, 84, 84, 87, 87, 87, 88, 88, 91, 91, 92, 92, 95, 95, 96, 96, 99, 99, 100, 100, 103, 103, 104, 104, 107, 107, 108, 108, 111, 111, 111, 112, 112, 115, 115, 116, 116, 116, 119, 119, 120, 120, 123, 123, 124, 124, 127, 127, 128, 128, 131, 132, 132, 393

Fichier tc_load_dump_parameters.c : lignes 878, 897, 914, 1021, 1043, 1044, 1045

Fichier tm_lfr_tc_exe.c : lignes 379, 379

Fichier wf_handler.c : lignes 145, 185, 191, 197, 197, 199, 204, 204, 212, 216, 221, 221, 223, 228, 228, 236, 241, 246, 246, 248, 253, 253, 343, 354, 356, 362, 363, 364, 366, 390, 412, 421, 426, 457, 469, 471, 473, 475, 482, 523, 534, 542, 585, 586, 838, 843, 924, 953, 1183, 1207, 1230, 1264, 1290, 1293, 1293, 1295, 1301, 1303, 1303, 1307, 1313, 1313

Fichier : lignes

History

#1 - 19/10/2016 02:19 PM - William Recart

- Subject changed from Analyse Logiscope LFR_3.1.0.4 : Don_Initialisation_P2 to Analyse Logiscope LFR_3.1.0.4 : Don_Initialisation_P2 Severity is High

#2 - 12/01/2017 09:26 AM - paul leroy

Fichier avf0_prc0.c

Fichier avf1_prc1.c

Fichier avf2_prc2.c

Fichier fsw_init.c

Fichier fsw_misc.c

Fichier fsw_processing.c

Fichier fsw_spacewire.c Faux positifs?

1122, 1124, 1125, 1208, 1209, 1211, 1296, 1298, 1299, 1360, 1362, 1363, 1440, 1442, 1443, 1520, 1522, 1523, 1586, 1586

Fichier lfr_cpu_usage_report.c

Fichier tc_acceptance.c Faux positifs?

130, 130

Fichier tc_handler.c

Fichier tc_load_dump_parameters.c

Fichier tm_lfr_tc_exe.c Faux positifs?

379, 379

Fichier wf_handler.c

145, 185, 191, 197, 197, 199, 204, 204, 212, 216, 221, 221, 223, 228, 228, 236, 241, 246, 246, 248, 253, 253
1183, 1207, 1230

#3 - 12/01/2017 12:22 PM - paul leroy

- Status changed from New to In Progress

- Priority changed from Normal to Low

#4 - 13/01/2017 03:35 PM - William Recart

Vérification effectuée sur le tag 322 (c0603702c8c8) , il reste en erreur :

avf0_prc0.c : lignes 204, 205, 206, 207, 215, 218, 226, 229, 235, 238, 244, 247, 295, 297, 298, 308, 310, 311, 333, 335, 336, 345, 347, 348, 365
=> je me demande si ce n'est pas une limitation de l'outil car d'après ce que je lit dans le code, ce sont les memset des lignes 204 à 207 qui font l'initialisation des variables en erreur sur toutes les lignes suivantes. Confirme-tu ceci ?

check.pngje confirme

avf1_prc1.c : lignes 205, 206, 207, 208, 216, 219, 227, 230, 236, 239, 287, 289, 290, 300, 302, 303, 325, 327, 328, 337, 339, 340, 357

=> même question de ma part que sur les erreurs du fichier avf0_prc0.c . Confirme-tu ?

check.pngje confirme

avf2_prc2.c : lignes 152, 153, 161, 164, 207, 209, 210, 221, 223, 224

=> même question de ma part que sur les erreurs du fichier avf0_prc0.c . Confirme-tu ?

check.pngje confirme

fsw_misc.c : lignes 241, 269, 271, 280, 411, 412, 413, 909, 909

=> même question de ma part que sur les erreurs du fichier avf0_prc0.c . Confirme-tu ?

check.pngje confirme.

Pour 411 412 413, toutes les variables sont initialisées correctement mais c'est peut-être la boucle qui ne passe pas. J'ai modifié la stratégie comme ça:

```
static unsigned int v[MOVING_AVERAGE] = {0};  
static unsigned int e1[MOVING_AVERAGE] = {0};  
static unsigned int e2[MOVING_AVERAGE] = {0};
```

Pour 909 (deux fois) c'est autre chose, on initialise avec une variable globale, qui est correctement initialisée à zéro

fsw_spacewire.c : lignes 137, 160, 174, 181, 181, 183, 183, 192, 194, 201, 613, 618, 641, 643, 645, 647, 649, 651, 653, 655, 657, 659, 661, 677, 680, 705, 712, 719, 726, 733, 740, 747, 754, 761, 768, 775, 785, 785, 788, 1154, 1156, 1157, 1240, 1241, 1243, 1328, 1330, 1331, 1392, 1394, 1395, 1472, 1474, 1475, 1552, 1554, 1555, 1618, 1618

=> même question de ma part que sur les erreurs du fichier avf0_prc0.c . Confirme-tu ?

check.pngoui, sauf pour 1156 et toutes les suivantes => initialisation avec des valeurs pointées par un paramètre de la fonction

=> faux positif : manipulation des attributs d'un paramètre d'entrée, l'erreur d'initialisation n'est pas avérée (lignes 1154, 1156, 1157, 1240, 1241, 1243, 1328, 1330, 1331, 1392, 1394, 1395, 1472, 1474, 1475, 1552, 1554, 1555)

=> erreur ligne 1618 : peux-tu confirmer que lors de l'affectation de ring_node_to_send->buffer_address dans kcoefficients_dump (ligne 1616), l'attribut packetLength de kcoefficients_dump est bien renseigné et initialisé ? (car on manipule des pointeurs et on fait un cast)

check.pngje confirme

=> fonction spacewire_get_last_error : les erreurs sur current sont des faux positifs (utilisation memset) par contre, hk_lfr_last_er_rid et hk_lfr_last_er_code sont initialisés que des zéros si précédents. Du coup, il y a un risque que lors de la comparaison ligne 785, une des deux valeurs ne soient pas initialisées (même si je suppose que tu as essayé de penser à tout, mais que ce passe-t-il si une condition se rajoute et que tu oublie de la reporter ici ?)

check.pngje prends note et j'initialise les valeurs à 0

tc_acceptance.c : lignes 131, 131

=> faux positifs

tc_handler.c : lignes 39, 63, 72, 76, 77, 80, 81, 84, 85, 88, 89, 92, 93, 96, 97, 100, 101, 104, 105, 108, 109, 112, 113, 116, 117, 120, 121, 124, 125, 128, 129, 132, 133, 136, 137

=> même question de ma part que sur les erreurs du fichier avf0_prc0.c . Confirme-tu ?

check.pngje confirme

tm_lfr_tc_exe.c : lignes 379, 379

=> faux positifs

wf_handler.c : lignes 145, 184, 190, 196, 196, 198, 203, 203, 211, 215, 220, 220, 222, 227, 227, 235, 240, 245, 245, 247, 252, 252, 1208, 1232, 1255
=> je ne vois pas où est initialisé waveform_picker_regs (variable déclarée en extern dans le wf_handler.h)
check.pngla déclaration est dans fsw_globals.c mais l'initialisation n'est pas du ressort du logiciel de vol pour pas mal de champs, notamment les champs de status qui sont juste lus par le soft mais écrit par le VHDL

Tout le reste est clos sur la version tag 322 (c0603702c8c8)

#5 - 21/03/2017 04:04 PM - bruno katra

- Assignee changed from paul leroy to William Recart

#6 - 24/04/2017 12:10 PM - William Recart

- Status changed from In Progress to Closed

Status on FSW V3.2.0.15 : 191 violations due to tool limitation :

- avf0_prc0.c : lines 204, 205, 206, 207, 215, 218, 226, 229, 235, 238, 244, 247, 295, 297, 298, 308, 310, 311, 333, 335, 336, 345, 347, 348, 365 : wrong positives due to use of memset function to initialize variables;
- avf1_prc1.c : lines 205, 206, 207, 208, 216, 219, 227, 230, 236, 239, 287, 289, 290, 300, 302, 303, 325, 327, 328, 337, 339, 340, 357 : wrong positives due to use of memset function to initialize variables;
- avf2_prc2.c : lines 152, 153, 161, 164, 207, 209, 210, 221, 223, 224 : wrong positives due to use of memset function to initialize variables;
- fsw_misc.c : lines 245, 273, 275, 284, 950, 950 : wrong positives due to use of memset function to initialize variables for lines 245 to 284 and line 950 : housekeeping_packet is global variable initialized to 0;
- fsw_spacewire.c : lines 137, 160, 174, 181, 181, 183, 183, 192, 194, 201, 613, 618, 641, 643, 645, 647, 649, 651, 653, 655, 657, 659, 661, 677, 682, 707, 714, 721, 728, 735, 742, 749, 756, 763, 770, 777, 790, 1156, 1158, 1159, 1242, 1243, 1245, 1330, 1332, 1333, 1394, 1396, 1397, 1474, 1476, 1477, 1554, 1556, 1557, 1620, 1620 : lines 137 to 790 wrong positives due to use of memset function to initialize variables and lines 1156 to end : variable are initialized by values pointed by function parameters;
- tc_acceptance.c : lines 131, 131 : wrong positives, TCPacket is initialized;
- tc_handler.c lines : 39, 63, 72, 76, 77, 80, 81, 84, 85, 88, 89, 92, 93, 96, 97, 100, 101, 104, 105, 108, 109, 112, 113, 116, 117, 120, 121, 124, 125, 128, 129, 132, 133, 136, 137, 182, 183 : lines 39 to 137 wrong positives due to use of memset function to initialize variables, lines 182, 183 : wrong positives due to initialization of transitionCoarseTime by using function copyInt32ByChar;
- tc_load_dump_parameters.c : lines 1001, 1007, 1013, 1019 : wrong positives : flag is initialized by using an if then else instruction (lines 987 to 994);
- tm_lfr_tc_exe.c : lines 379, 379 : wrong positives, TC is initialized;
- wf_handler.c : lines 145, 184, 190, 196, 196, 198, 203, 203, 211, 215, 220, 220, 222, 227, 227, 235, 240, 245, 245, 247, 252, 252, 1208, 1232, 1255 : wrong positives, declaration done in fsw_globals.c but it consists in registers, not initialized by SW.

#7 - 03/10/2018 06:35 PM - William Recart

Status on FSW V3.2.0.21: 259 violations due to tool limitation :

- avf0_prc0.c : lines 228, 229, 230, 231, 239, 242, 250, 253, 259, 262, 268, 271, 319, 321, 322, 332, 334, 335, 357, 359, 360, 369, 371, 372, 389 : wrong positives due to use of memset function to initialize variables;
- avf1_prc1.c : lines 229, 230, 231, 232, 240, 243, 251, 254, 260, 263, 311, 313, 314, 324, 326, 327, 349, 351, 352, 361, 363, 364, 381 : wrong positives due to use of memset function to initialize variables;
- avf2_prc2.c : lines 176, 177, 185, 188, 231, 233, 234, 245, 247, 248 : wrong positives due to use of memset function to initialize variables;
- fsw_misc.c : lines 277, 305, 307, 316, 612, 816, 1023, 1023 : wrong positives due to use of memset function to initialize variables for lines 245 to 284 and line 950 : housekeeping_packet is global variable initialized to 0;
- fsw_spacewire.c : lines 161, 184, 198, 205, 205, 207, 207, 216, 218, 225, 637, 642, 648, 650, 652, 654, 656, 658, 660, 662, 664, 666, 668, 684, 689, 697, 704, 711, 718, 725, 732, 739, 746, 753, 760, 767, 780, 1146, 1148, 1149, 1232, 1233, 1235, 1320, 1322, 1323, 1384, 1386, 1387, 1464, 1466, 1467, 1549, 1551, 1552, 1619, 1619 : lines 137 to 790 wrong positives due to use of memset function to initialize variables and lines 1156 to end : variable are initialized by values pointed by function parameters;
- lfr_cpu_usage_report.c : lines 59,60 : fval is initialized passing by reference at line 59 and use at line 60;
- tc_acceptance.c : lines 154, 154: wrong positives, TCPacket is initialized;
- tc_handler.c lines : 62, 86, 95, 99, 100, 103, 104, 107, 108, 111, 112, 115, 116, 119, 120, 123, 124, 127, 128, 131, 132, 135, 136, 139, 140, 143, 144, 147, 148, 151, 152, 155, 156, 159, 160, 205, 206 : lines 62 to 160 wrong positives due to use of memset function to initialize variables, lines 205, 206: wrong positives due to initialization of transitionCoarseTime by using function copyInt32ByChar;
- tc_load_dump_parameters.c : lines 1021, 1027, 1033, 1039 : wrong positives : flag is initialized by using an if then else instruction (lines 987 to 994);
- tm_lfr_tc_exe.c : lines 403, 403 : wrong positives, TC is initialized;
- wf_handler.c : lines 169, 208, 214, 220, 220, 222, 227, 227, 236, 240, 245, 245, 247, 252, 252, 260, 265, 270, 270, 272, 277, 1230, 1254, 1277 : wrong positives, declaration done in fsw_globals.c but it consists in registers, not initialized by SW.