

Development Methodology for the Software Life Cycle Process of the Safety Software

*,
BNF ()
150

, , ,
150

-

, ESF-CCS ESF-CCS

IEEE Std.

1074-1997

. 가 OPA SLC

, SLCP

Abstract

A methodology for developing software life cycle processes (SLCP) is proposed to develop the digital safety-critical Engineered Safety Features - Component Control System (ESF-CCS) successfully. A software life cycle model is selected as the hybrid model mixed with waterfall, prototyping, and spiral models and is composed of two stages, development stages of prototype of ESF-CCS and ESF-CCS. To produce the software life cycle (SLC) for the Development of the Digital Reactor Safety System, the Activities referenced in IEEE Std. 1074-1997 are mapped onto the hybrid model. The SLCP is established after the available OPAs (Organizational Process Asset) are applied to the SLC Activities, and the known constraints are reconciled. The established SLCP describes well the software life cycle activities with which the Regulatory Authority provides.

1.

()
가

가 .

,
,
.

(Common

Mode Failure)

가 . [1]

3,4

3,4

. ,

,

가

.

.

,

.

2001

7

.

가

,

.

가

가

,

[2]

.

SLCP

, IEEE Std. 1074-1997 [3]

SLCP

. 2

IEEE Std. 1074-1997 [3]

, 3

SLCP

. 4

.

2.

가

,

,

가

. [4] IEEE Std. 1074-1997 [3]

SLCP

.

, , [3]
 SLCP [3] 1 SLCP
 ,
 ,
 , , ,
 .

3.

3.1

(SLCM: Software Life Cycle Model)

(Waterfall) ,

가 (Prototyping)

가

(Spiral)

-

7

가

[3] [5]

SLCP

1 (2001.7 ~ 2004.6)

, 2 (2004.7 ~ 2008.6)

1

, 가 . 1 2

, 1 가 2 가 .

1

2

가

-

13

35

I

VI

1

VII

XIII

2

, , , , , , 1 , ,

, , , , , , 2 , ,

, , , , , , .

, 가 가 가 . -

1

.

3.2

-

[6] 5

,

,

,

,

,

2 ESF-CCS

18 71

.

3.3

-

3 ESF-CCS

[3] 가

,

,

가

,

가

.

ESF-CCS 4

,

,

가

.

4.

-

,

가

.

가

,

.

5.

[1] , “ ”, '94

[2] NUREG-0800, "Standard Review Plan : Chapter 7. Instrumentation and Controls", 1997

[3] IEEE Std. 1074-1997, "Standard for Developing Software Life Cycle Processes"

[4] IEEE Std. 610.12-1990, "Standard Glossary of Software Engineering Terminology"

[5] USNRC Reg. Guide 1.173, "Development of Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", 1997

[6] NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems", 1993

1 ESF-CCS

1		2	
I.	I.A I.B I.C I.D I.E	VII.	VII.A VII.B VII.C VII.D
II.	II.A	VIII.	VIII.A
III.	III.A III.B III.C	IX.	IX.A IX.B IX.C
IV.	IV.A IV.B	X.	X.A X.B
V.	V.A V.B V.C	XI.	XI.A XI.B XI.C XI.D
VI.	VI.A VI.B	XII.	XII.A XII.B XII.C XII.D
		XIII. 가	XIII.A 가

2 ESF-CCS

A1 (Projection Management Activity Groups)	A11 (Project Initiation Activities)	A111 SLCP A112 A113 A114
	A12 (Project Planning Activities)	A121 가 A122 A123 A124 A125 A126 A127 A128 A129 A1210 A1211
	A13 (Project Monitoring and Control Activities)	A131 A132 A133 SLCP A134 A135
A2 (Pre-Development Activity Groups)	A21 (Concept Exploration Activities)	A211 A212 가 A213 가 A214
	A22 (System Allocation Activities)	A221 A222 A223
	A23 (Software Importation Activities)	A231 A232 가 A233 A234
A3 (Development Activity Groups)	A31 (Requirements Activities)	A311 A312 A313
	A32 (Design Activities)	A321 A322 A323 A324
	A33 (Implementation Activities)	A331 A332 A333

A4 (Post-Development Activity Groups)	A41 (Installation Activities)	A411 A412 A413
	A42 (Operation and Support Activities)	A421 A422 A423
	A43 (Maintenance Activities)	A431 A432 A433 SLC
	A44 (Retirement Activities)	A441 A442 A443
A5 (Integral Activity Groups)	A51 가 (Evaluation Activities)	A511 A512 A513 A514 A515 A516 A517 가
	A52 (Software Configuration Management Activities)	A521 A522 A523
	A53 (Documentation Development Activities)	A531 A532 A533 가
	A54 (Training Activities)	A541 A542 A543
	A55 (Safety Activities)	A551 A552

3 ESF-CCS

I.A	A111; A132; A134; A211; A212
I.B	A112; A113; A114; A121; A122; A124; A125; A126; A127; A128; A129; A1210; A1211; A131; A132; A133; A134; A432; A511; A521; A522; A523; A531; A551; A552
I.C	A131; A132; A133; A134; A135; A211; A212; A213; A214; A432; A511; A522; A523; A531; A551; A552
I.D	A131; A132; A133; A134; A135; A211; A212; A213; A214; A221; A222; A231; A432; A511; A522; A523; A531; A551; A552
I.E	A131; A132; A133; A134; A135; A211; A212; A213; A214; A221; A222; A223; A232; A233; A234; A432; A511; A512; A513; A517; A521; A522; A523; A531; A551; A552
II.A	A131; A132; A133; A134; A135; A231; A311; A312; A313; A432; A511; A512; A522; A523; A531; A551; A552
III.A	A131; A132; A133; A134; A135; A232; A233; A234; A321; A323; A324; A432; A511; A512; A522; A523; A531; A551; A552
III.B	A131; A132; A133; A134; A135; A323; A432; A512; A522; A523; A531; A551; A552
III.C	A131; A132; A133; A134; A135; A432; A512; A514; A515; A517; A522; A523; A531; A551; A552
IV.A	A131; A132; A133; A134; A135; A331; A432; A512; A521; A522; A523; A551; A552
IV.B	A131; A132; A133; A134; A135; A432; A512; A514; A515; A517; A521; A522; A523; A551; A552
V.A	A131; A132; A133; A134; A135; A333; A432; A522; A523; A551; A552
V.B	A131; A132; A133; A134; A135; A333; A432; A522; A523; A551; A552
V.C	A131; A132; A133; A134; A135; A332; A432; A511; A522; A523; A531; A532; A541; A542; A543; A551; A552
VI.A	A131; A132; A134; A432; A516; A517; A522; A523; A551; A552
VI.B	A131; A132; A134; A411; A412; A413; A432; A513; A522; A523; A551; A552

VII.A	A112; A113; A114; A121; A122; A123; A124; A125; A126; A127; A128; A129; A1210; A1211; A131; A132; A133; A134; A432; A443; A511; A522; A523; A531; A533; A551; A552
VII.B	A131; A132; A133; A134; A135; A211; A212; A213; A214; A432; A511; A522; A523; A531; A551; A552
VII.C	A131; A132; A133; A134; A135; A211; A212; A213; A214; A221; A222; A231; A432; A511; A522; A523; A531; A551; A552
VII.D	A131; A132; A133; A134; A135; A211; A212; A213; A214; A221; A222; A223; A232; A233; A234; A432; A511; A512; A513; A522; A523; A531; A551; A552
VIII.A	A131; A132; A133; A134; A135; A231; A311; A312; A313; A432; A511; A512; A522; A523; A531; A551; A552
IX.A	A131; A132; A133; A134; A135; A232; A233; A234; A321; A323; A324; A432; A511; A512; A522; A523; A531; A551; A552
IX.B	A131; A132; A133; A134; A135; A323; A432; A512; A522; A523; A531; A551; A552
IX.C	A131; A132; A133; A134; A135; A432; A512; A514; A515; A517; A522; A523; A531; A551; A552
X.A	A131; A132; A133; A134; A135; A331; A432; A512; A522; A523; A551; A552
X.B	A131; A132; A133; A134; A135; A432; A512; A514; A515; A517; A521; A522; A523; A551; A552
XI.A	A131; A132; A133; A134; A135; A333; A432; A522; A523; A551; A552
XI.B	A131; A132; A133; A134; A135; A333; A432; A522; A523; A551; A552
XI.C	A131; A132; A133; A134; A135; A332; A432; A522; A523; A551; A552
XI.D	A131; A132; A134; A432; A516; A517; A522; A523; A551; A552
XII.A	A131; A132; A133; A134; A135; A412; A432; A522; A523; A551; A552
XII.B	A131; A132; A133; A134; A135; A421; A431; A432; A441; A442; A522; A523; A551; A552
XII.C	A131; A132; A133; A134; A135; A422; A431; A432; A433; A522; A523; A551; A552
XII.D	A131; A132; A134; A422; A423; A431; A432; A441; A442; A513; A517; A522; A523; A551; A552
XIII.A 가	A533

4 ESF-CCS

1 : ESF-CCS			
1		2	
I.A; I.B; I.C; I.D; I.E	II.A	III.A; III.B; III.C	IV.A; IV.B
ESF-CCS	ESF-CCS S/W Group Controller	ESF-CCS S/W Group Controller	ESF-CCS Group Controller
ESF-CCS	Loop Controller	Loop Controller	Loop Controller
ESF-CCS S/W			
S/W		ESF-CCS S/W	/
S/W		Group Controller	/
S/W		Loop Controller	
S/W			
S/W		ESF-CCS S/W	
S/W			
S/W			
S/W			
ESF-CCS	ESF-CCS	ESF-CCS	ESF-CCS
V&V	V&V	V&V	V&V
2 : ESF-CCS 가			
1		2	
VII.A; VII.B; VII.C; VII.D	VIII.A	IX.A; IX.B; IX.C	X.A; X.B
ESF-CCS	ESF-CCS S/W	ESF-CCS S/W	ESF-CCS
ESF-CCS	Group Controller	Group Controller	Group Controller
ESF-CCS S/W	Loop Controller	Loop Controller	Loop Controller
S/W			
S/W		ESF-CCS S/W	/
S/W		Group Controller	/
S/W		Loop Controller	
S/W			
S/W		ESF-CCS S/W	
S/W			
S/W			
ESF-CCS	ESF-CCS	ESF-CCS	ESF-CCS
V&V	V&V	V&V	V&V

4 ESF-CCS

()

1 : ESF-CCS		
3		
V.A; V.B; V.C		VI.A; VI.B
ESF-CCS S/W H/W		
ESF-CCS		
ESF-CCS		
ESF-CCS	ESF-CCS	
V&V	V&V	
2 : ESF-CCS 가		
3		4
		가
XI.A; XI.B; XI.C; XI.D	XII.A; XII.B; XII.C; XII.D	XIII.A
ESF-CCS S/W H/W	ESF-CCS	ESF-CCS Topical
ESF-CCS	ESF-CCS	가 가
ESF-CCS	ESF-CCS Topical	
ESF-CCS		
ESF-CCS		
ESF-CCS	ESF-CCS	
V&V	V&V	