Preprint for conference proceedings for The Second World Congress on Software Quality, Yokohama, Sept 25.-29, 2000. http://www.calpoly.edu/~pmcquaid/2WCSQ

Safety critical software and development productivity

O. Benediktsson

Science Institute
University of Iceland
Dunhaga 5, IS-107 Reykjavik, Iceland
Tel: 354 525 4920, Fax: 354 552 8802, E-mail: oddur@hi.is

Abstract

The new standard IEC 61508 on safety critical systems /4/ recommends usage of a number of software practices. These recommendations become more stringent as the required safety integrity level increases. This paper relates the recommendations of the 61508 standard to two productivity related parameters - one is termed software product verifiability and the other software process capability. The COCOMO II cost estimation model is employed to give estimates of decrease/increase in development effort based on variation in the verifiability and capability parameters. Increased product verifiability will result in increase in development effort while increased process capability gives decrease in the effort.

1. Introduction

The IEC 61508 standards define four safety integrity levels (SIL) as shown in table 1. The levels are specified in terms of average probability of failures per usage for low demand systems (a) and probability of failures per hour for high demand (continuous usage) systems (b). Column (c) is derived from (b) as approximate failures per year and column (d) shows typical damages involved at system failure.

SIL level	**Low demand failures/usage (a)**	**High demand failures/hr (b)**	**High demand failures/year (c)**	**Damage (d)**
SIL1	>= 10^{-2} to 10^{-1}	>= 10^{-6} to 10^{-5}	>= 10^{-2} to 10^{-1}	injury
SIL2	>= 10^{-3} to 10^{-2}	>= 10^{-7} to 10^{-6}	>= 10^{-3} to 10^{-2}	death to one
SIL3	>= 10^{-4} to 10^{-3}	>= 10^{-8} to 10^{-7}	>= 10^{-4} to 10^{-3}	death to few
SIL4	>= 10^{-5} to 10^{-4}	>= 10^{-9} to 10^{-8}	>= 10^{-5} to 10^{-4}	catastrophe

Table 1 The SIL levels in terms of probability of failure and resulting damages

Systems that require SIL4 are of ultra high reliability and lie in general outside the considerations in this paper.

Part 3 of the 61508 standard relates to software requirements in safety critical systems. General requirements of Part 3 specify the employment of such processes as configuration management and documentation and planned and track life cycle. Part 3 enumerates also considerable number of recommended software practices. A selected set of these practices and the associated recommendations are shown in table 2.

Practice	**Category**	**61508-3**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
Use of coding standard	Coding standards	B.1	HR	HR	HR	HR
No dynamic variables		B.1	---	R	HR	HR
Test case execution from cause consequence diagrams	Dynamic analysis and testing	B.2	---	---	R	R
Structure-based testing		B.2	R	R	HR	HR
Equivalence classes and input partition testing	Black box testing	B.3	R	HR	HR	HR
Failure modes, effects and criticality analysis	Failure analysis	B.4	R	R	HR	HR
Formal methods	Modelling	B.5	---	R	R	HR
Performance modelling		B.5	R	HR	HR	HR
Time Petri nets		B.5	---	R	HR	HR
Avalanche/stress testing	Performance testing	B.6	R	R	HR	HR
Response timings and memory constraints		B.6	HR	HR	HR	HR
Performance requirements		B.6	HR	HR	HR	HR
Sequence diagrams	Semi-formal methods	B.7	R	R	HR	HR
Finite state machines/state transition diagrams		B.7	R	R	HR	HR
Decision/truth tables		B.7	R	R	HR	HR
Boundary value analysis	Static analysis	B.8	R	R	HR	HR
Control flow analysis		B.8	R	HR	HR	HR
Fagan inspections		B.8	---	R	R	HR
Symbolic execution		B.8	R	R	HR	HR
Walk-throughs/design reviews		B.8	HR	HR	HR	HR
Software module size limit	Modular approach	B.9	HR	HR	HR	HR
Information hiding/encapsulation		B.9	R	HR	HR	HR
Fully defined interface		B.9	HR	HR	HR	HR
Total recommended (R)			**12**	**12**	**3**	**1**
Total highly recommended (HR)			**6**	**10**	**20**	**22**

Legend: HR highly recommended; R recommended; --- no recommendation
Table 2 Example software practices from the 61508-3 standard

We observe considerable affinity between SIL1 and SIL2 and again between SIL3 and SIL4 but a jump going from SIL2 to SIL3. Note, however, that difference in one single practice such as the use of formal methods can have wide consequences for the project effort.

The main task in this paper is to relate the requirements of the 61508-3 standard to software development productivity. To this end the COCOMO II model will be brought to bear.

The COCOMO II model /2, 3, 5/ estimates effort in person months (PM) required to complete a software development project. The model has twenty-two parameters, seventeen of which are termed "effort multipliers" (EM) and five are termed "scale factors" (SF). These parameters are calibrated with real world data that has been collected during the passed three decades by Barry W. Boehm and his co-workers.

The effort is related to estimated size of a project stated thousand source lines of code (KSLOC) and the parameters through the equation

$$PM = A\ (Size)^{B} \quad \text{(Eq. 1)}$$

where A = product (of EM factors) and B = 1.01 + sum(of SF factors).

For simplification the project size is fixed to 100 KSLOC in this paper.

COCOMO II is available as a tool from the University of Southern California /3/. The effort figures shown in this paper are computed with the tool with unaltered values of parameters.

3. The product verifiability index

This paper relates the recommendations of the 61508 standard to parameters termed *product verifiability index* on one hand and software *process capability index* on the other hand.

The product verifiability index (VI) has three values i.e. VI1, VI2 and VI3. See the definition in the table 3. In constructing the verifiability indices an attempt was made to reflect the verification requirements of SIL levels directly so that VI1 corresponds to SIL1, VI2 to SIL2 and CL3 to SIL3.

The VI index is taken to consist of three following COCOMO II parameters: *Software reliability* (RELY), *documentation needs* (DOCU) and *development flexibility* (FLEX). RELY and DOCU are effort multipliers while FLEX is a scale factor. The postulated relation of these COCOMO II parameters to the VI levels is arrived at by relating the recommendation of the standard to the COCOMO II parameters. This is done by using intuition mainly. The values of the parameters show in the table are those supplied in the COCOMO II tool. The NOM column is included for reference. The "Resulting effort - PM_{100} " row shows the resulting project months for 100 KSLOC size project. When all of the parameters in the model are set to NOM the development effort is 465.3 PM. The effort is seen to increase as the product verifiability requirements become more stringent. The bottom row shows the effort as related to the nominal effort. From it we see that the effort increases by 70% as we move from product with nominal verifiability requirements to that of VI3.

	NOM	**VI1**	**VI2**	**VI3**
Required Reliability (RELY)	Moderate, easily recoverable losses (NOM = 1)	High financial loss (HI = 1.10)	High financial loss (HI = 1.10)	Risk to human life (VHI = 1.26)
Documentation Match to Lifecycle Needs (DOCU)	Right-sized to life-cycle needs (NOM = 1)	Right-sized to life-cycle needs (NOM = 1)	Excessive for life-cycle needs (HI = 1.11)	Very excessive for life- cycle needs (VHI = 1.23)
Development Flexibility (FLEX)	Some relaxation (NOM = 3.04)	Occasional relaxation (LO = 4.05)	Occasional relaxation (LO = 4.05)	Rigorous (VLO = 5.07)
Resulting effort PM_{100}	465.3	536.2	595.2	791.8
Product verifiability effort factor	**1**	**1.15**	**1.28**	**1.70**

Table 3 Product verifiability productivity

4. Process capability index

It has been reasoned that minimum capability level must be set at CMM Level 2 for the development of SIL1 software in accordance to the 61508 standard /1/. (SW-CMM is the Software Capability Maturity Model of Software Engineering Institute /6/). We will therefore focus our attention on software development at capability levels 2, 3, and 4. (Level 5 is rarely attained and is left out.) The *process maturity* (PMAT) scale factor of the COCOMO II model ties in with the levels of CMM. PMAT relates CMM level 1 (lower half) to VLO, level 1 (upper half) to LO, level 2 to NORM, level 3 to HI and level 4 to VHI.

We define the *process capability index* as consisting of CI1, CI2, and CI3 categories as shown in table 4. The capability index is taken to depend on PMAT as well as *risk resolution* (RESL) and *use of software tools* (TOOL). PMAT and RESL are scale factors while TOOL is an effort multiplier. As in the case for the VI index then CL1 is designed to reflect the SIL1 requirements, CI2 those of SIL2 and CL3 those of SIL3.

The bottom row of table 4 shows that the development effort at CI3 is 56% of that of the nominal case.

	NOM	**CI1**	**CI2**	**CI3**
Process Maturity (PMAT)	CMM Level 2 (NOM = 4.68)	CMM Level 2 (NOM = 4.68)	CMM Level 3 (HI = 3.12)	CMM Level 4 (VHI = 1.56)
Tool Usage (TOOL)	Basic lifecycle tools, moderately integrated (NOM = 1)	Basic lifecycle tools, moderately integrated (NOM = 1)	Strong, mature lifecycle tools, moderately integrated (HI = 0.90)	Tools well integrated with processes, methods, reuse (VHI = 0.78)
Architecture and Risk Resolution (RESL)	Often (60%) (NOM = 4.24)	Generally (75%) (HI= 2.83)	Mostly (90%) (VHI = 1.41)	Full (100%) (XHI = 0.00)
Resulting effort $\mathbf{PM_{100}}$	465.3	436.1	342.1	258.6
Capability effort factor	**1**	**0.94**	**0.74**	**0.56**

Table 4 Process capability levels and productivity

5. Process capability and product verifiability combined

Let $\underline{PM}_{100}$ denote effort estimate of 100 KSLOC project where the parameters that enter into VI and CI are set at NOM (i.e. the parameters RELY, DOCU, FLEX, PMAT, TOOL and RESL). The remaining COCOMO II parameters are set as the needs of a project may be. The development effort in a safety critical project may then expressed as

$$PM_{100} = VI\ CI\ \underline{PM}_{100} \quad \text{(Eq. 2)}$$

We see from eq. 2 that the effort factors of product verifiability and process capability can be combined by multiplication to give the combined effect of the VI and CI factors. The result is shown in table 5.

	NOM	VI1	VI2	VI3
NOM	1.00	1.15	1.28	1.70
CI1	0.94	1.08	1.20	1.60
CI2	0.74	0.85	0.95	1.26
CI3	0.56	0.65	0.72	0.95

Table 5 Combined effort factor of capability and verifiability

The ratio between the highest and lowest productivity in table 5 is 2.7 (i.e. 1.70/0.56).

Summary

The data in the diagonal in table 5 show approximately constant nominal productivity as the VI and CI change in unison. Above a diagonal the productivity goes up (with higher capability or lower verifiability requirements) while below the diagonal productivity goes down.

The CI and VI categories are designed to reflect the SIL levels of the 61508 standard. This is represented in table 6 where the "combined factor" row is the diagonal of table 5.

		SIL1	SIL2	SIL3
Verifiability	NOM	VI1	VI2	VI3
Capability	NOM	CI1	CSI2	CI3
SIL effort factor	**1.00**	**1.08**	**0.95**	**0.95**

Table 6 SIL effort factor

Again, the SIL effort factor remains approximately constant as the SIL level increases from SIL1 to SIL3. The decrease in productivity with increased verifiability requirements is counteracted by the increased productivity with increased process capability. Please note that this holds specifically for project size of 100 KSLOC and for the postulated mapping of the recommendations of 61508 into the COCOMO II parameters.

References

1. Benediktsson O, Hunter R B, McGettrick A D 1999; *Processes for Software in Safety Critical Systems*. To be published.
2. Boehm B W1981; *Software Engineering Economics*, Prentice-Hall.
3. COCOMO II, http://sunset.usc.edu/COCOMOII/cocomo.html
4. IEC; DIS 61508 1998; *Functional safety of electrical/electronic/programmable electronic safety related systems*, International Electrotechnical Commission, Geneva.

5. Clark B K1999; *Effects of Process Maturity on Development Effort*, URL: http://sunset.usc.edu/COCOMOII/cocomo.html, The University of Southern California.

6. Paulk M C, , Weber C V, Curtis B, Chrisis M B 1995, *The Capability Maturity Model: Guidelines for Improving the Software Process*, Addison Wesley,.

7. ISO/IEC, TR 15504-9 1998, *Information technology – Software process assessment – Parts 1-9*.