CSC313 High Integrity Systems/ CSCM13 Critical Systems

Course Notes
Additional Material
Chapter 4: Safety Criteria

Anton Setzer
Dept. of Computer Science, Swansea University

http://www.cs.swan.ac.uk/∼csetzer/lectures/critsys/current/index.html

October 1, 2017

4 (a) Requirements

4 (b) Basic Notions

4 (c) Dimensions of Dependability

4 (d) Identification of Safety Requirements

4 (e) The Safety Case

No Additional Material

For this subsection no additional material has been added yet.

No Additional Material

For this subsection no additional material has been added yet.

Reliability

- If the reliability reduces per time interval uniformly by a certain percentage, one can show that reliability is of the form $\alpha \cdot \mathrm{e}^{-\beta t}$ for some $\beta > 0$.

Explanation of Formula for Reliability

(Only for the mathematically gifted).

- If the reliability $f(t)$ per time unit reduces by a certain percentage, we get that
$$f(t+t') = \alpha f(t)$$
for some $0 < \alpha < 1$ (say $\alpha = 80\% = 0.8$).
- If applied twice we get
$$f(t+2t') = \alpha \cdot \alpha f(t) \ ,$$
- in general
$$f(t+nt') = \alpha^n f(t) \ ,$$

Explanation of Formula for Reliability

- and for arbitrary t''

$$f(t+t'') = \alpha^{\frac{t''}{t'}} f(t) \ ,$$

- $\alpha^{\frac{1}{t'}} < 1$, let $\beta > 0$ s.t. $\mathrm{e}^{-\beta} = \alpha^{\frac{1}{t'}}$.
- Then we have

$$\alpha^{\frac{t''}{t'}} = (\mathrm{e}^{-\beta})^{t''} = \mathrm{e}^{-\beta t''}$$

therefore

$$f(t+t'') = \mathrm{e}^{-\beta t''} f(t)$$

Explanation of Formula for Reliability

- Then we get

$$\begin{aligned}\frac{f(t+t'')-f(t)}{t''} &= \frac{\mathrm{e}^{-\beta t''}-1}{t''}f(t)\\ &= \frac{\mathrm{e}^{-\beta t''}-\mathrm{e}^{-\beta 0}}{t''}f(t)\end{aligned}$$

- In the limit $t'' \longrightarrow 0$ we get

$$f'(t) = (\frac{\mathrm{d}}{\mathrm{d}t}\mathrm{e}^{-\beta t})(0)\cdot f(t) = -\beta\mathrm{e}^{-\beta 0}f(t) = -\beta f(t)$$

- This is a differential equation which has unique solution

$$f(t) = \alpha\mathrm{e}^{-\beta t}$$

No Additional Material

For this subsection no additional material has been added yet.

No Additional Material

For this subsection no additional material has been added yet.

i