

# 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

4 (a) Requirements

4 (b) Basic Notions

4 (c) Dimensions of Dependability

4 (d) Identification of Safety Requirements

4 (e) The Safety Case

For this subsection no additional material has been added yet.

4 (a) Requirements

4 (b) Basic Notions

4 (c) Dimensions of Dependability

4 (d) Identification of Safety Requirements

4 (e) The Safety Case

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.

## Reliability

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

- ▶ Then we get

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

- ▶ In the limit  $t'' \rightarrow 0$  we get

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

- ▶ This is a differential equation which has unique solution

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

## 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.  $e^{-\beta} = \alpha^{\frac{1}{t'}}$ .

- ▶ Then we have

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

therefore

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

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.

4 (a) Requirements

4 (b) Basic Notions

4 (c) Dimensions of Dependability

4 (d) Identification of Safety Requirements

4 (e) The Safety Case

i