

IT Design Criteria for Damage Reduction

Dr. Volker Hammer
hammer@secorvo.de



Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-452
Fax +49 721 6105-455
E-Mail info@secorvo.de
<http://www.secorvo.de>

Content

- ◆ Reasons for addressing damage reduction
- ◆ Hints on requirement engineering methodology
- ◆ 10 IT design criteria for damage reduction

Content

- ◆ **Reasons for addressing damage reduction**
- ◆ Hints on requirement engineering methodology
- ◆ 10 IT design criteria for damage reduction

Risk and IT Security

- ◆ **Risk in engineering: 2 factors**
 - Damage probability and
 - Damage potential
- ◆ **„Classical” security approaches (e.g. CC) focus on**
 - Confidentiality
 - Integrity
 - Availability
 - Usually: preferences for damage probability
- ◆ **Sufficient security if remaining risk is acceptable**
- ◆ **Conditions of acceptable risk?**
 - Social assessment of risks

Social Risk Assessment

- ◆ **Intuitive concepts of risk: assessed as high**
 - **Dread risk: involuntarily, seem to be uncontrollable, dreadful, deadly, advantages and disadvantages distributed unfair**
 - **Unknown risk: unperceivable, new type, effects raise with a big delay**
 - **High exposure: affects a big number of human beings**
- ◆ **Human rights and constitutional norms**
 - **Avoid high damage: →social security measures required**
 - **Low damage potential: →necessity of social controls reduced**
 - **Governments must avoid catastrophic situations for supplies**
- ◆ **Keep capability to learn and survive**
- ◆ **→High weight of damage potential**

Generic Social Goals (GG)

◆ 4 Anchors for IT design

- Low Damage Potentials (GG1)
- Low Damage Probability (GG2)
- Autonomy (GG3)
- Gathering Experience (GG4)

◆ Very general clauses

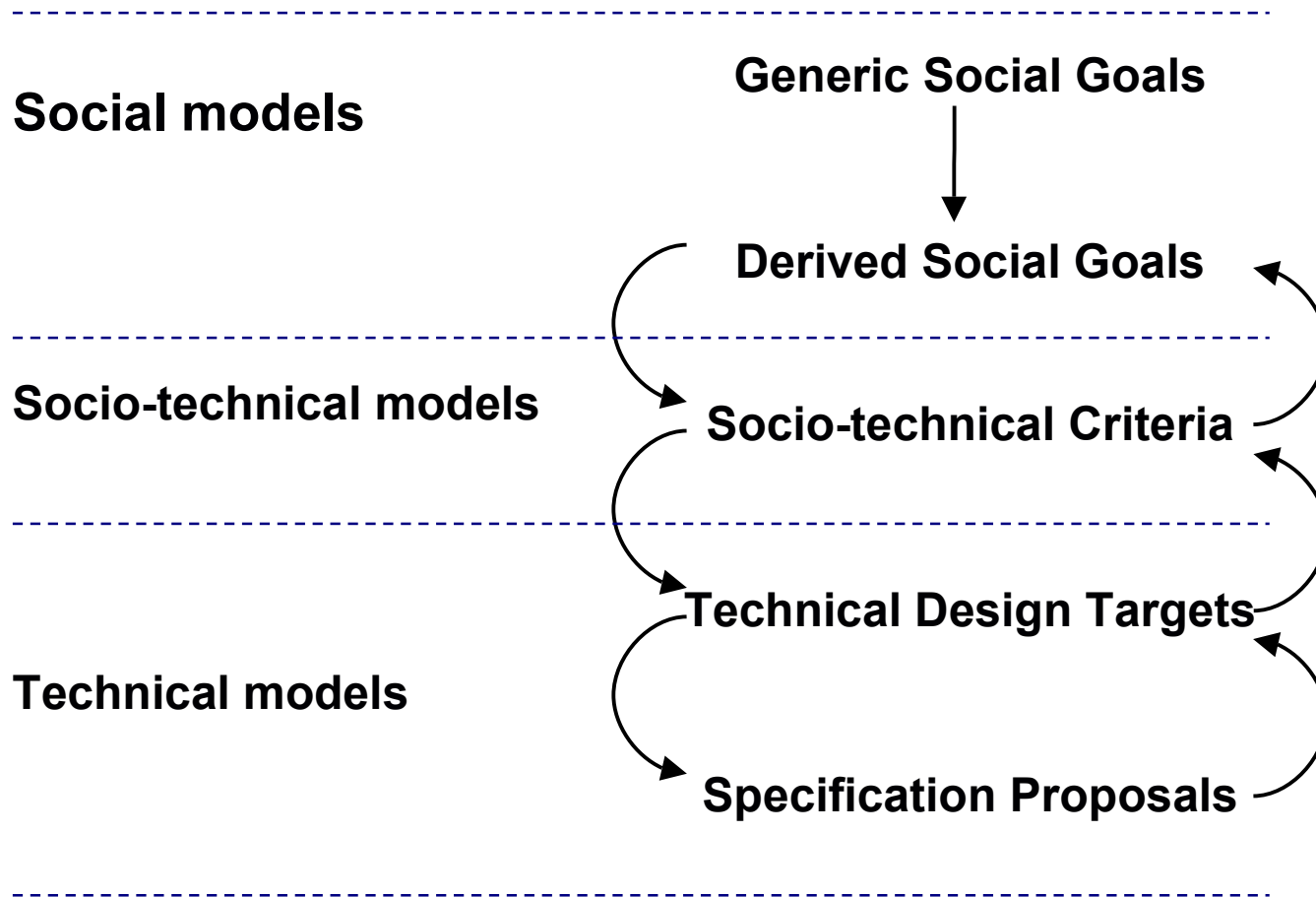
◆ How to use for IT system design?

- General clauses need to be operationalised
- Derive specification level requirements

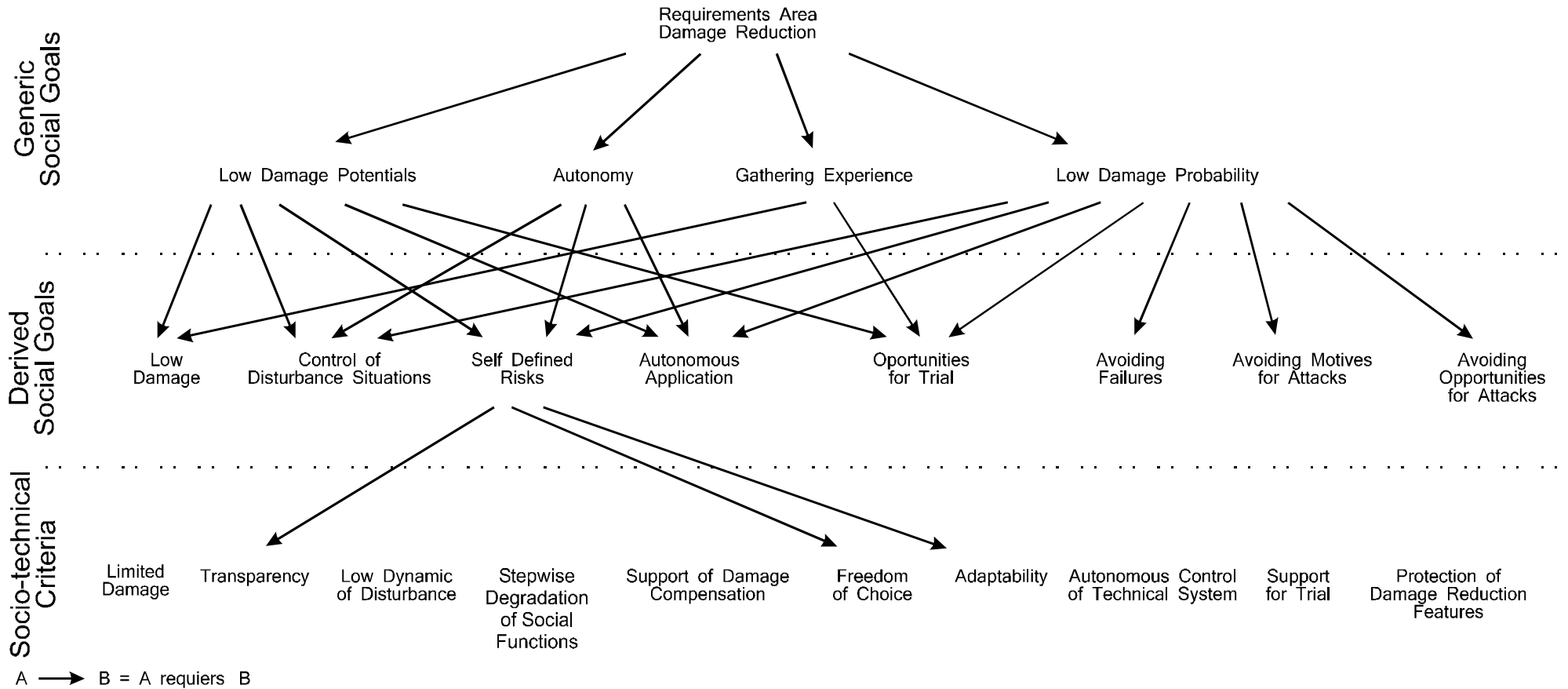
Content

- ◆ Reasons for addressing damage reduction
- ◆ **Hints on requirement engineering methodology**
- ◆ 10 IT design criteria for damage reduction

NORA - Normative Requirements Analysis



NORA Criteria System



Terms

◆ Disturbance situation

- Event chain
 - Often caused by an initial multi factor event
- “Disturbance” contains attacks and failures

◆ Social systems

- Individuals
- Organisations
- Society
- Damage potential level is relative per social system

◆ Damage potential

- Sum of all kinds of damage
 - e.g. monetary, reputational, health-related, ...
- Occuring from an event chain
- Identified per social system

Content

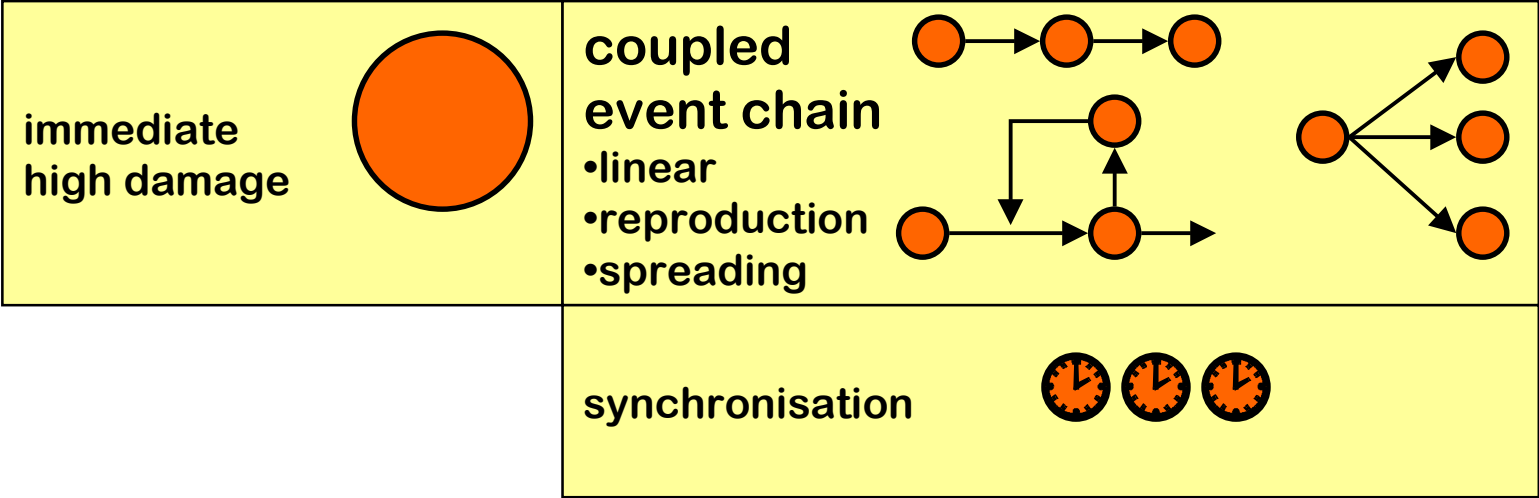
- ◆ Reasons for addressing damage reduction
- ◆ Hints on requirement engineering methodology
- ◆ **10 IT design criteria for damage reduction**

Socio-Technical Criteria (1)

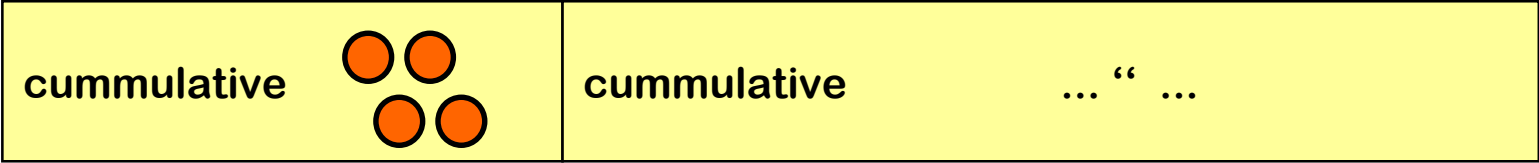
- ◆ **STC1) Limited Damage**

Contribution of IT to High Damage Potential

◆ Single primary event



◆ Multiple primary events



Socio-Technical Criteria (2)

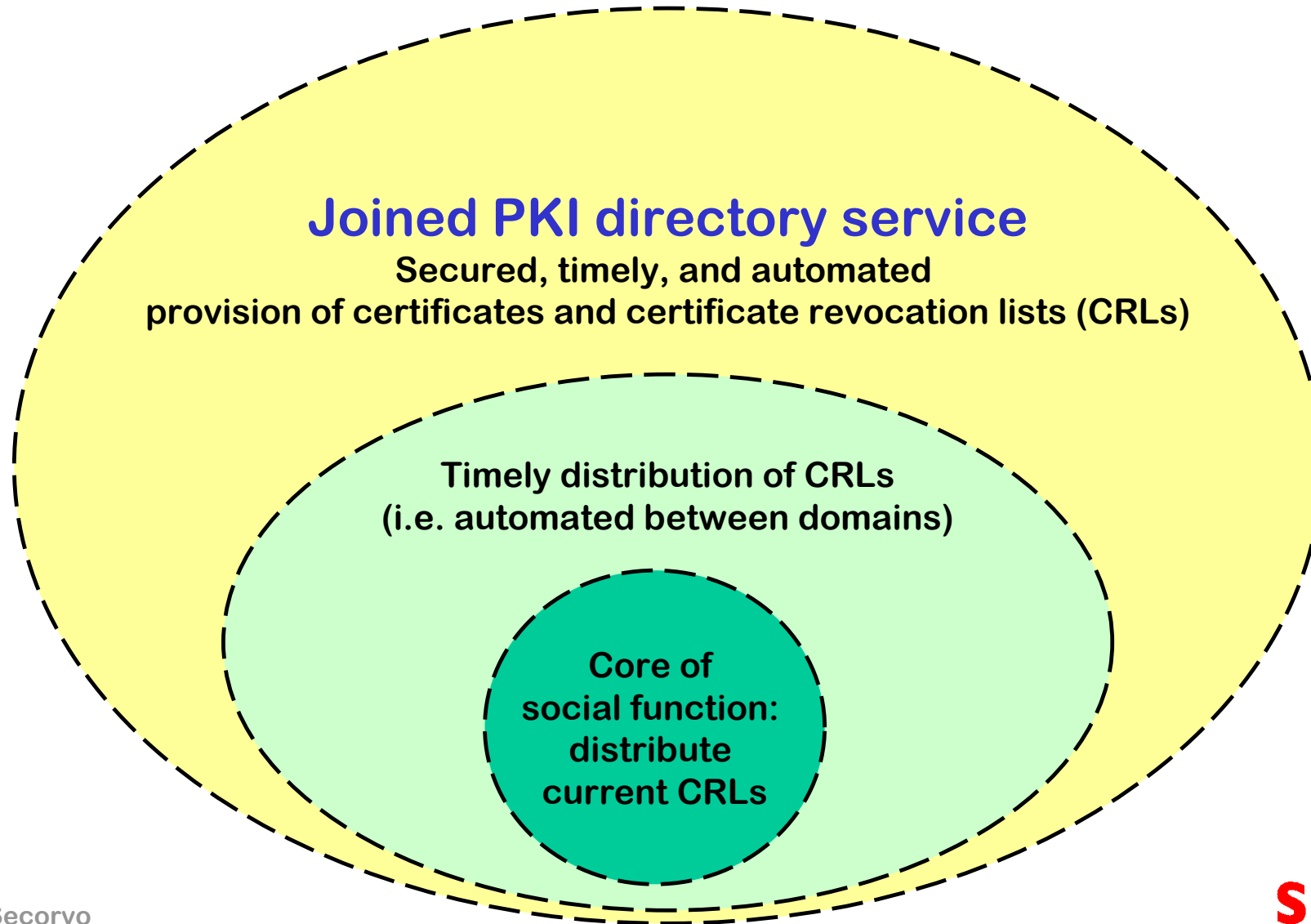
◆ **STC1) Limited Damage**

◆ **STC2) Transparency**

◆ **STC3) Low Dynamic of Disturbance**

◆ **STC4) Stepwise Degradation of Social Functions**

Stepwise Degradation



Socio-Technical Criteria (3)

◆ **STC1) Limited Damage**

◆ **STC2) Transparency**

◆ **STC3) Low Dynamic of Disturbance**

◆ **STC4) Stepwise Degradation of Social Functions**

◆ **STC5) Support of Damage Compensation**

Socio-Technical Criteria (4)

- ◆ **STC6) Freedom of Choice**
- ◆ **STC7) Adaptability**
- ◆ **STC8) Autonomous Control of Technical Systems**
- ◆ **STC9) Support for Testing**
- ◆ **STC10) Protection of Damage Reduction Features**

Conclusions

- ◆ **Main objectives of the approach:**
 - **Considers social assessment of risk**
 - **Damage reduction must have high priority**
 - **Low dynamic of disturbance**
- ◆ **10 criteria open the second dimension of security oriented system design**
- ◆ **Use competence of social systems for reactions**
- ◆ **Good applicability in early design stages for new applications**
- ◆ **Good chances for reuse of design results per area of technology**



Secorvo Security Consulting GmbH

Albert-Nestler-Straße 9

D-76131 Karlsruhe

Tel. +49 721 6105-452

Fax +49 721 6105-455

E-Mail info@secorvo.de

<http://www.secorvo.de>