MAFTIA

Yves Deswarte
LAAS-CNRS

DSN-2001 Special Track on the European Dependability Initiative
Göteborg, July 2, 2001

Motivation

- Large network infrastructures, such as the Internet, are vital for citizens to benefit from the Information Society.
- Development depends on how much the users will 'trust' the services.
- Such services must be made dependable, in particular w.r.t. malicious attacks by external hackers or by corrupt insiders.

MAFTIA:
Malicious- and Accidental-Fault Tolerance for Internet Applications

- Systematic investigation of the 'tolerance paradigm' for constructing large-scale dependable distributed applications.
- Comprehensive approach for tolerating both accidental faults and malicious intrusions in such systems, including intrusions by external hackers and by corrupt insiders.

Contract Details

- Project Start Date: 1st Jan 2000
- Duration: 3 years
- Requested Funding: 2.5 M€
- No. of person years: 55

Partners

- Newcastle University (GB) (coordinator)
  Brian Randell, Robert Stroud
- DERA, Malvern (GB)
  Sadie Crees, Tom McCutcheon
- IBM, Zurich (CH)
  Christian Cachin, Marc Dacier, Michael Waidner
- LAAS-CNRS, Toulouse (F)
  Yves Deswarte, David Powell
- Universität des Saarlandes (D)
  André Adeslbach, Birgit Pfitzmann
- Universidade de Lisboa (P)
  Nuno Neves, Paulo Veríssimo

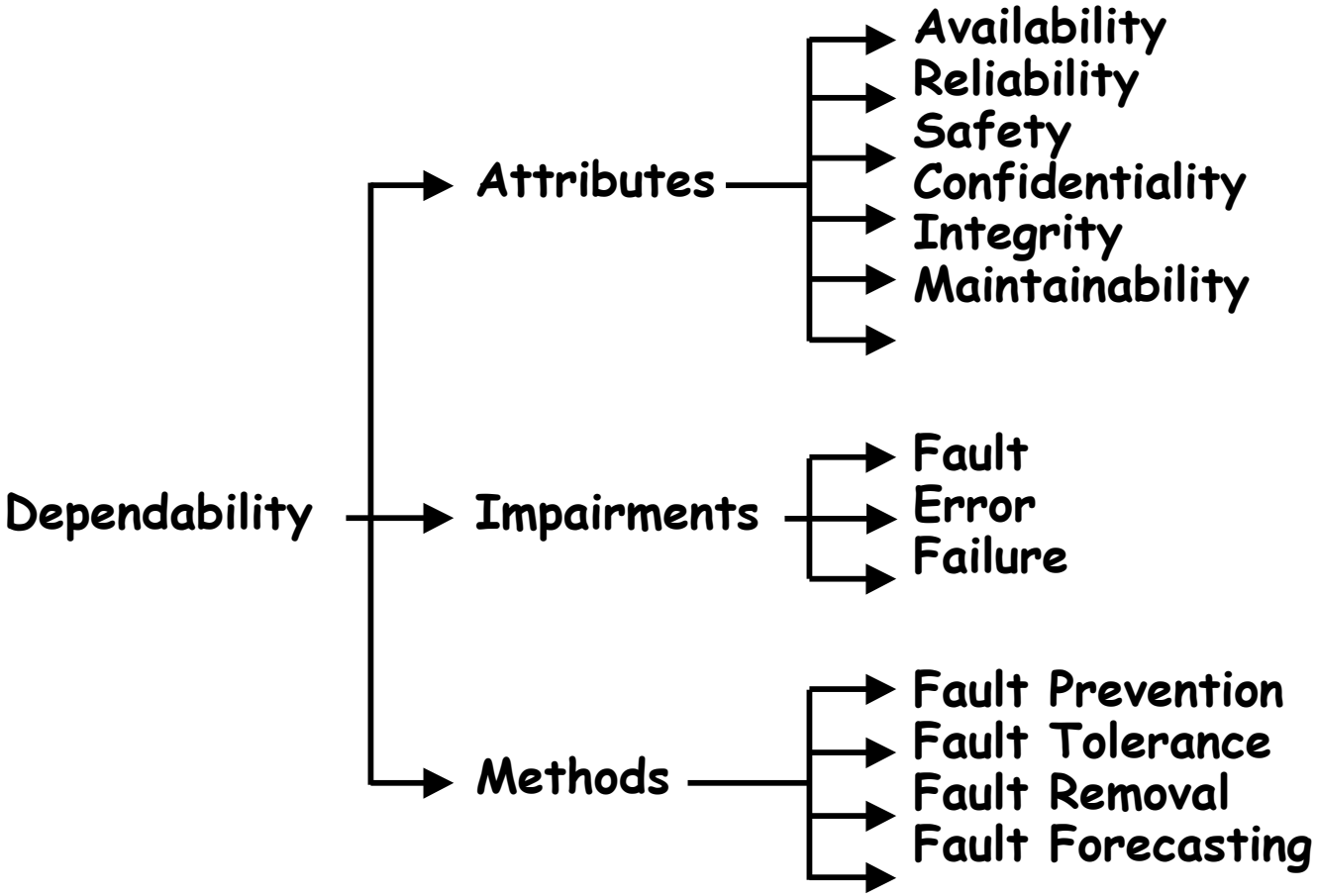
Industrial Advisory Board

- Andrew Izon (North Durham NHS Trust, GB)
- Jean-Claude Lebraud (Rockwell-Collins, F)
- Derek Long (CISA Ltd., GB)
- Joachim Posegga (SAP Systems, D)
- Carlos Quintas (Easyphone, P)
- Gilles Trouessin (Ernst & Young Audit, F)
- Gritta Wolf (Credit Suisse, CH)

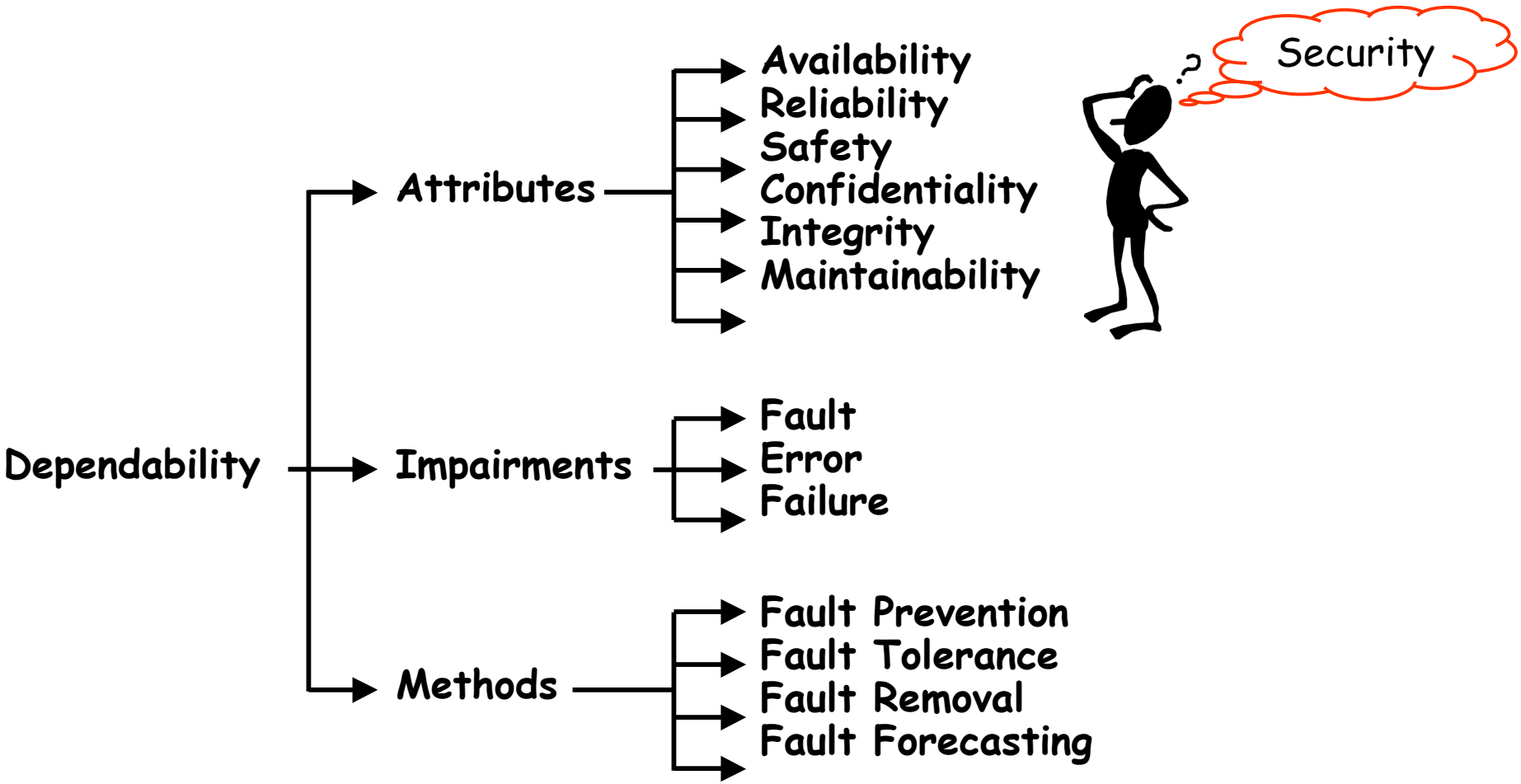
Objectives

- Architectural framework and conceptual model (WP1)
- Mechanisms and protocols:
  - dependable middleware (WP2)
  - large scale intrusion detection systems (WP3)
  - dependable trusted third parties (WP4)
  - distributed authorization mechanisms (WP5)
- Validation and assessment techniques (WP6)

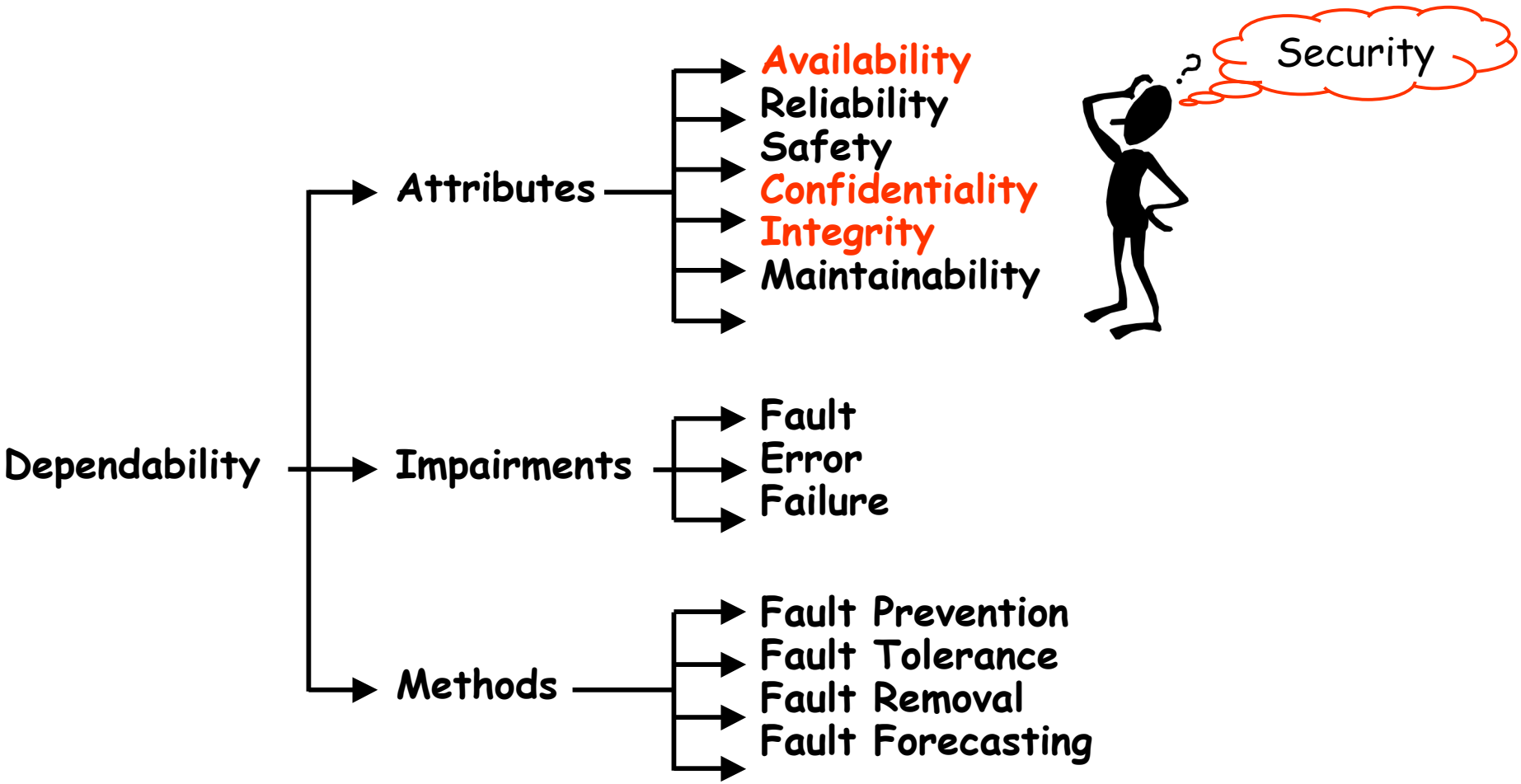
The Dependability Tree



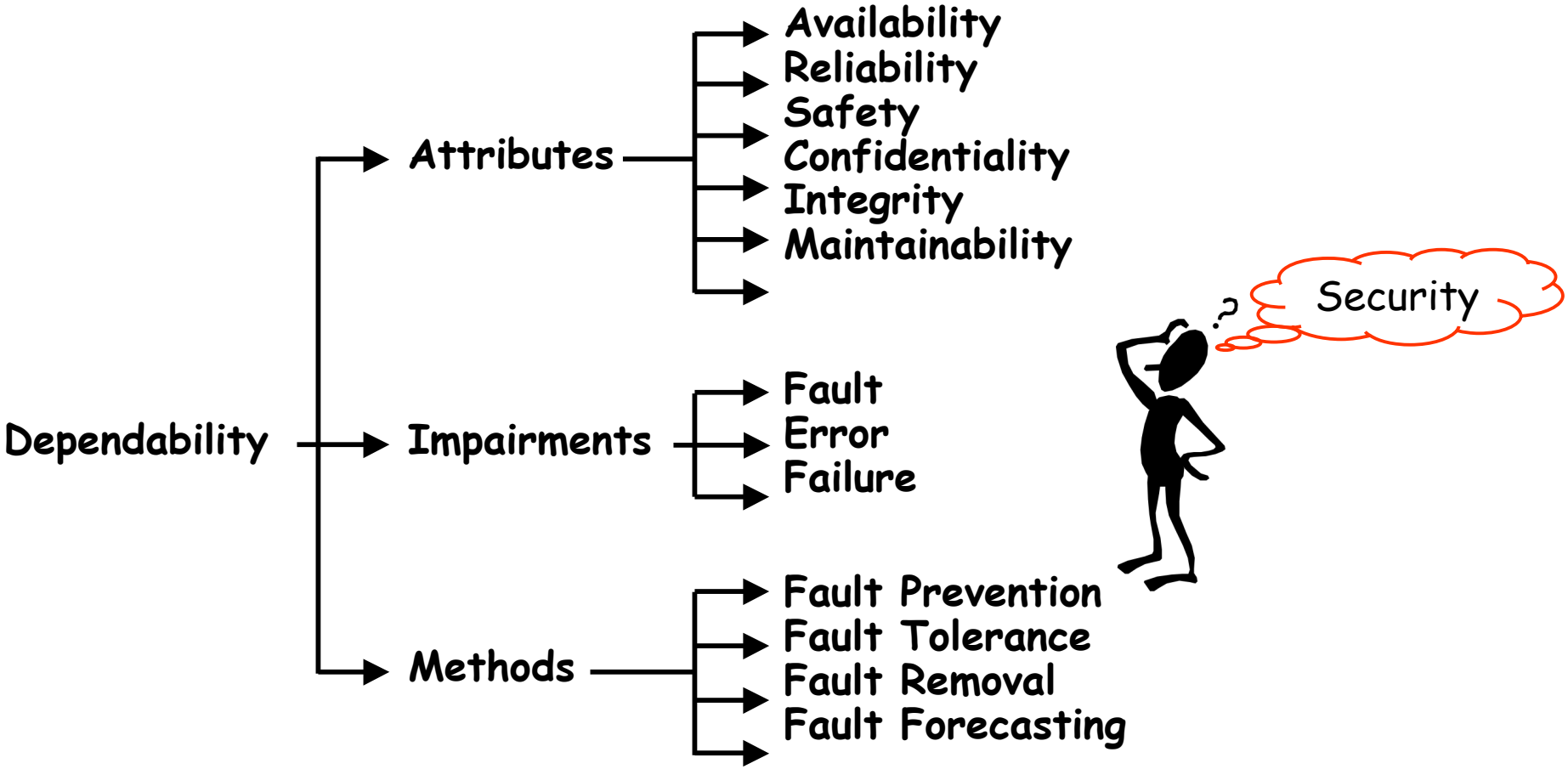
The Dependability Tree



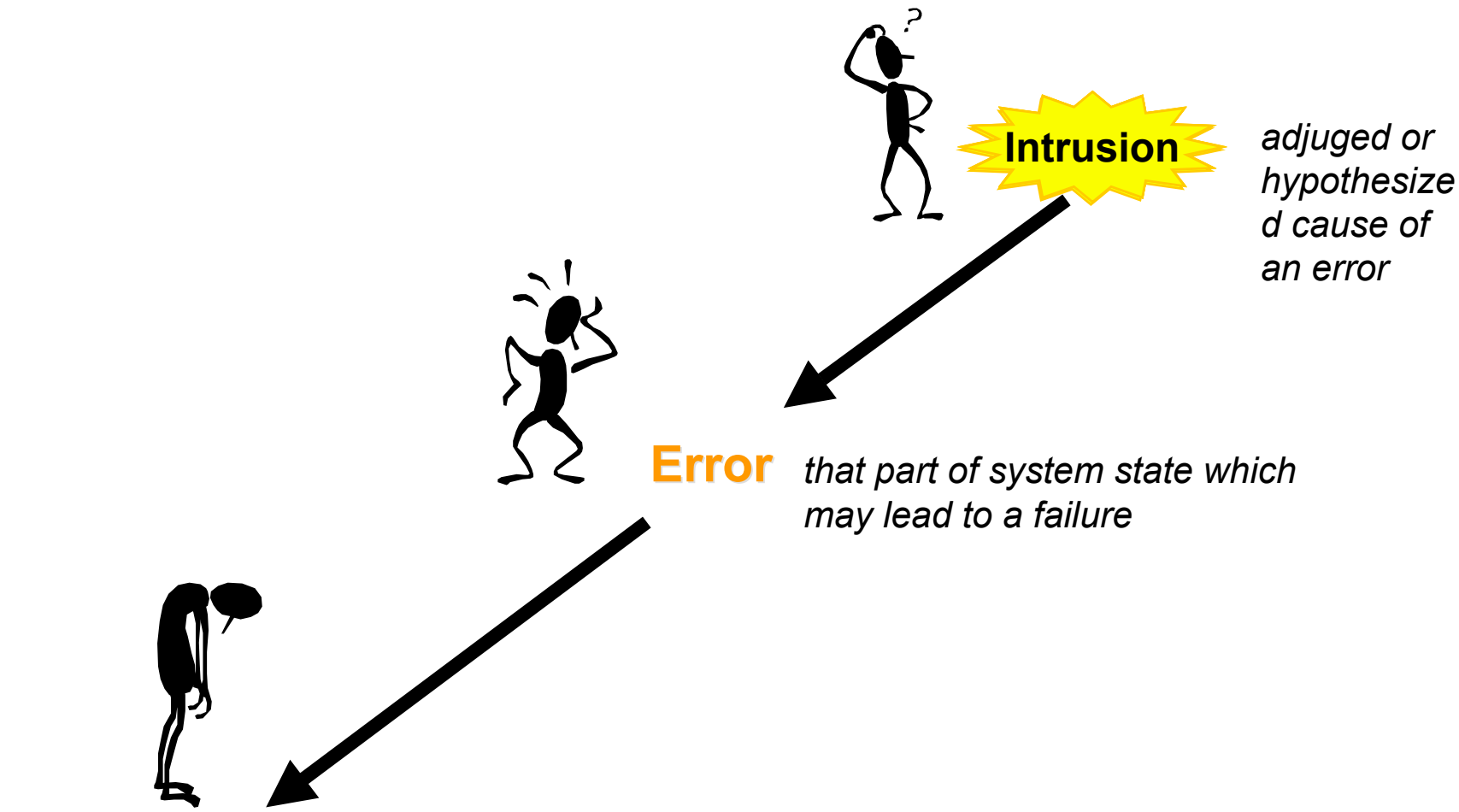
The Dependability Tree



The Dependability Tree

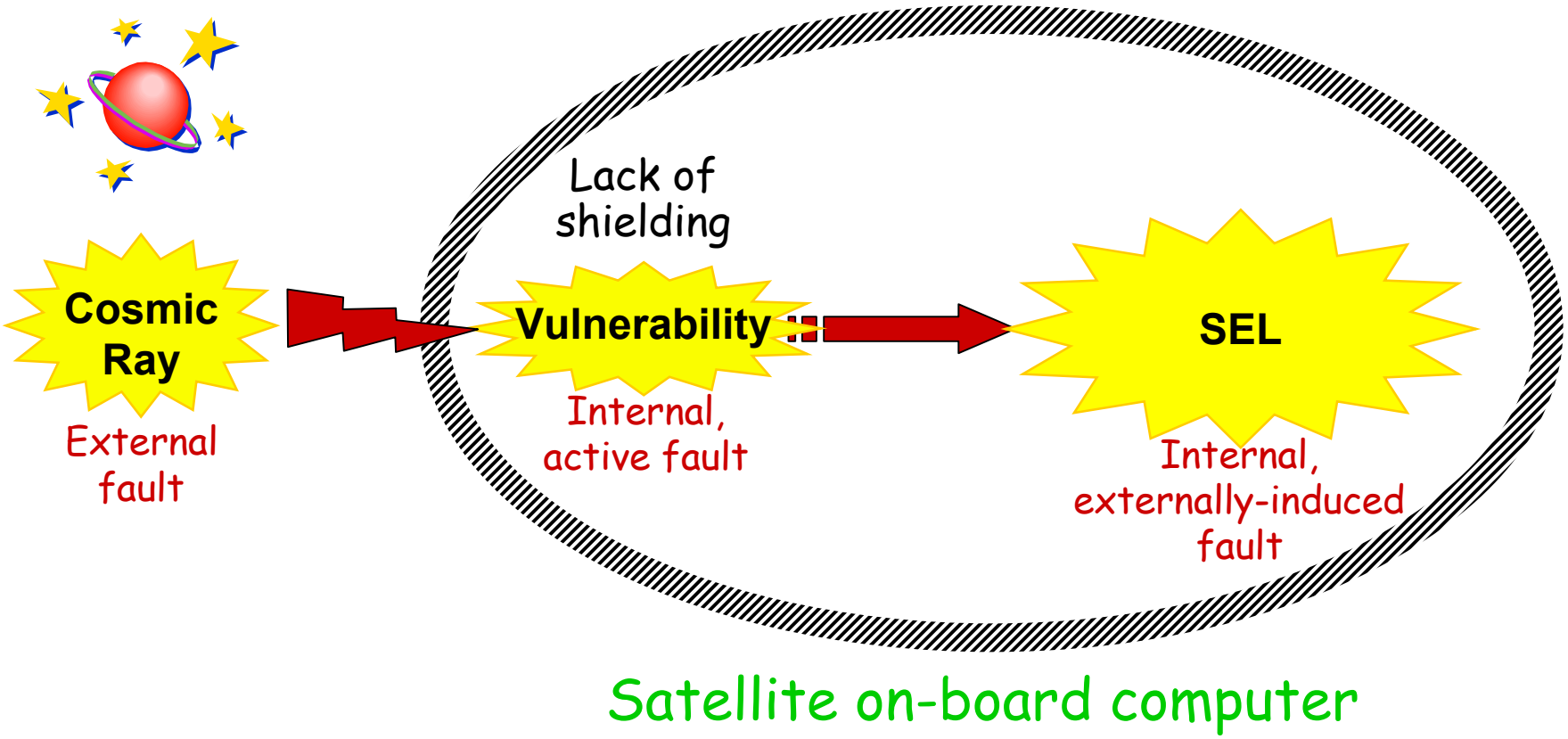


Fault, Error & Failure



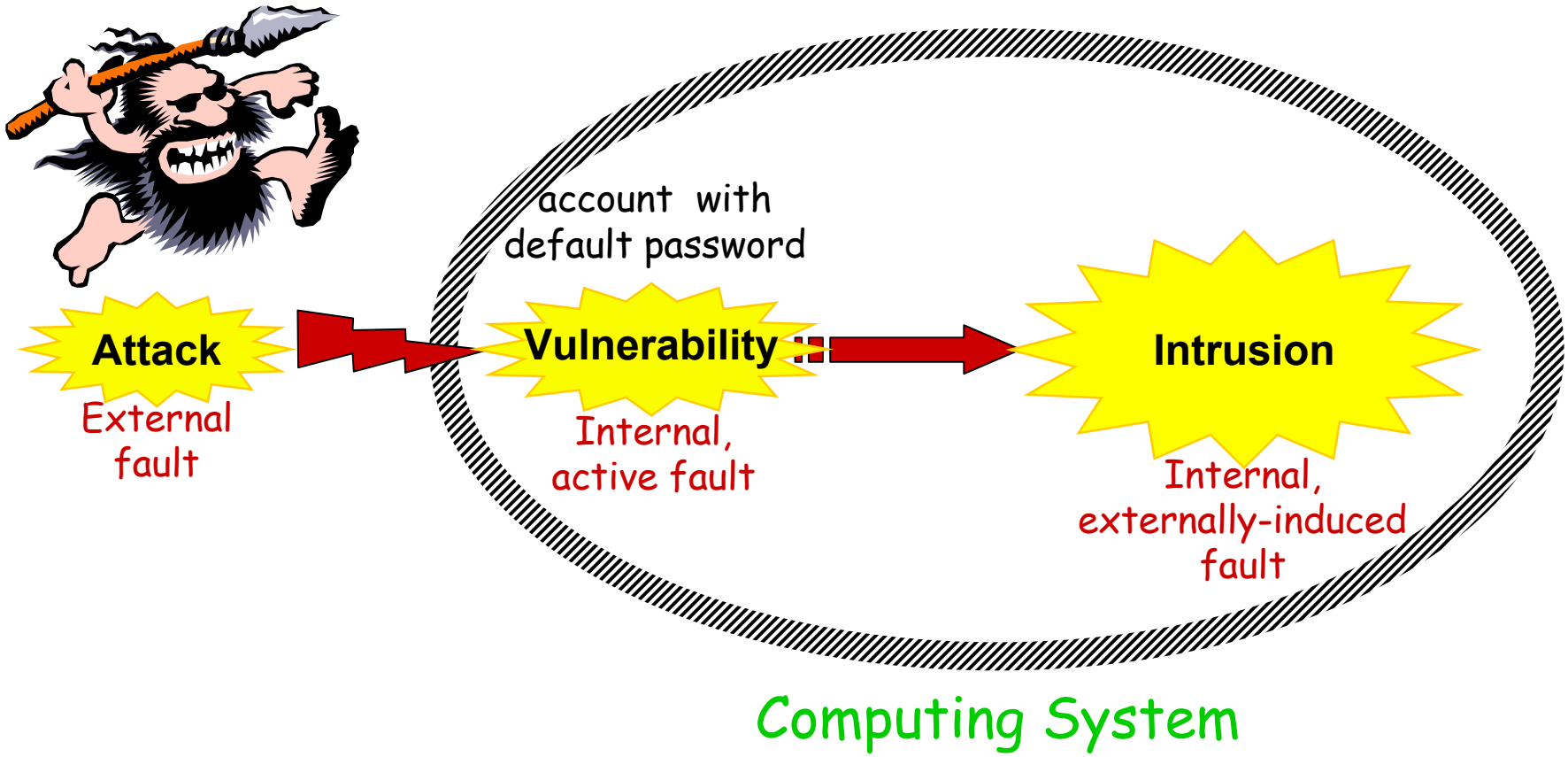
Example: Single Event Latchup

SELs (reversible stuck-at faults)
may occur because of radiation
(e.g., cosmic ray, high energy ions)

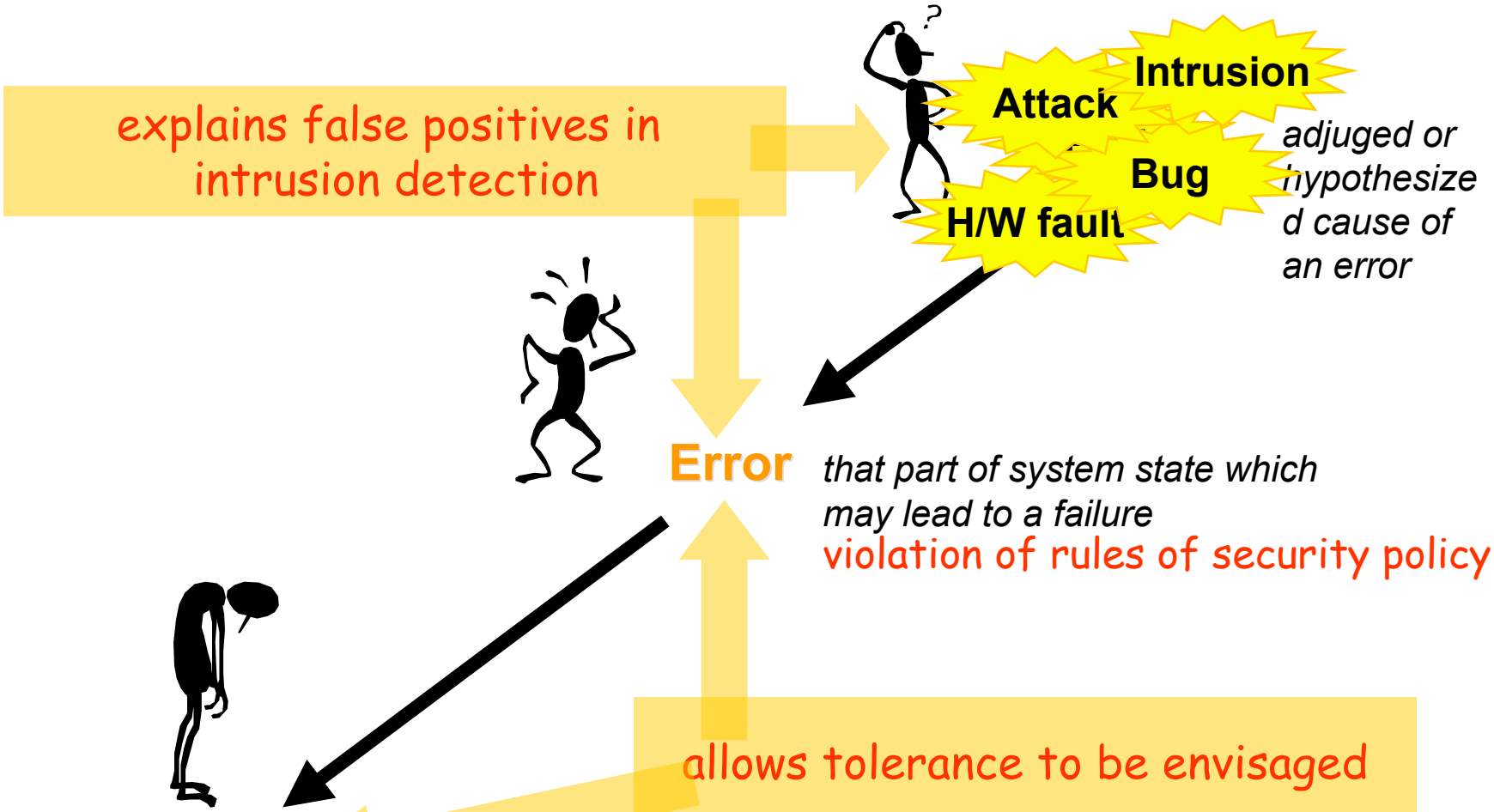


Intrusions

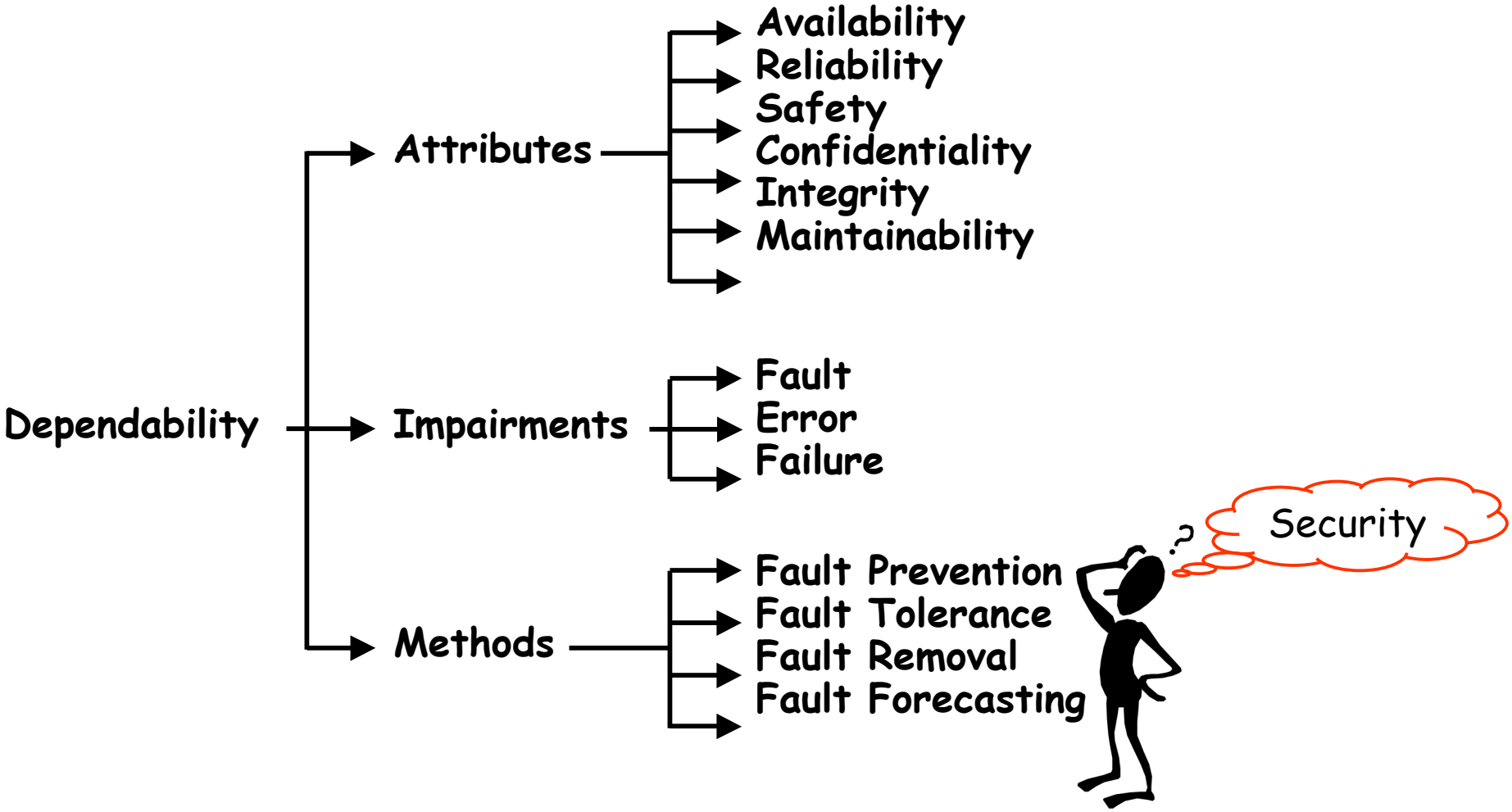
Intrusions result from
(at least partially) successful attacks:



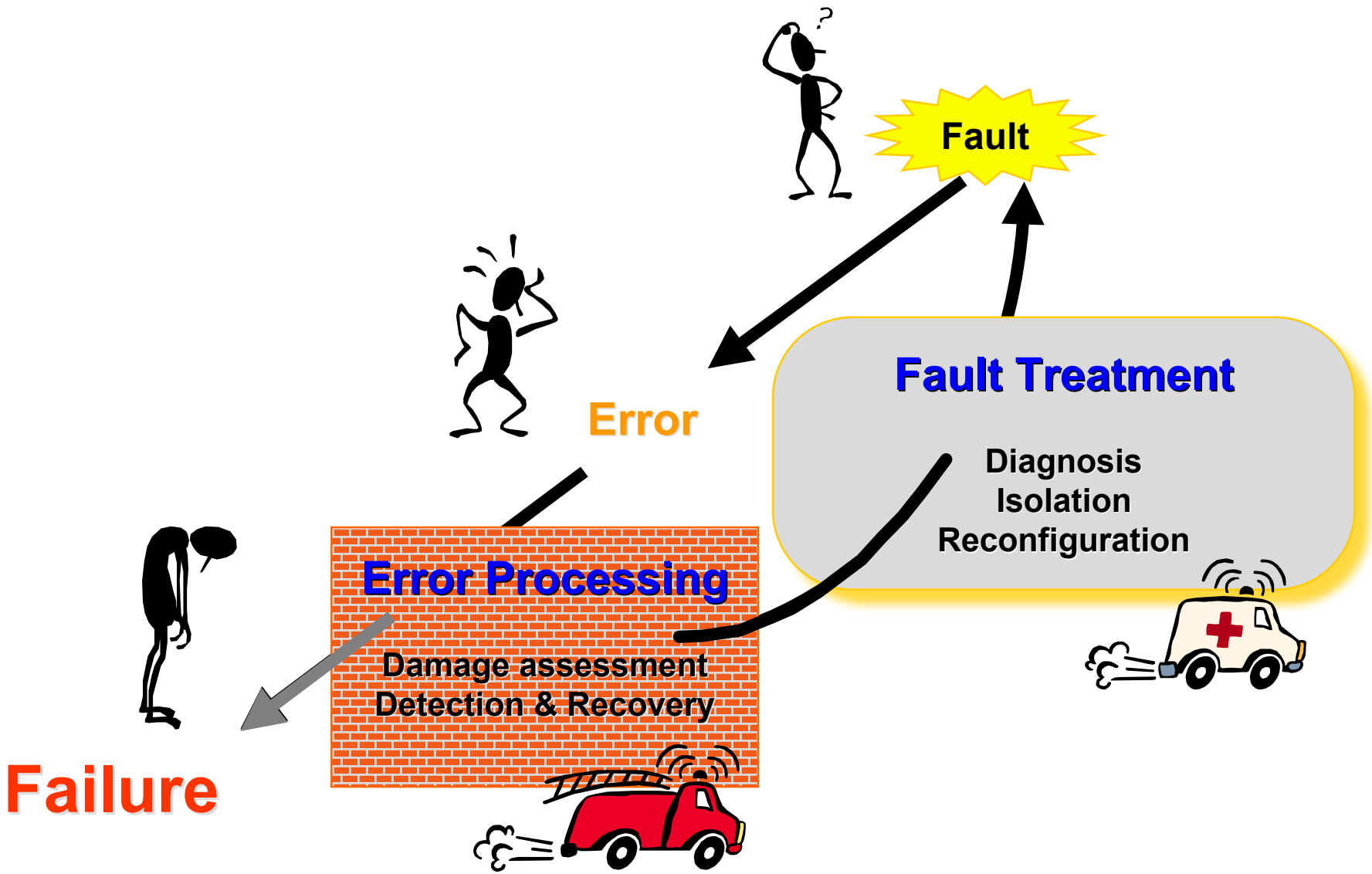
Fault, Error & Failure



The Dependability Tree

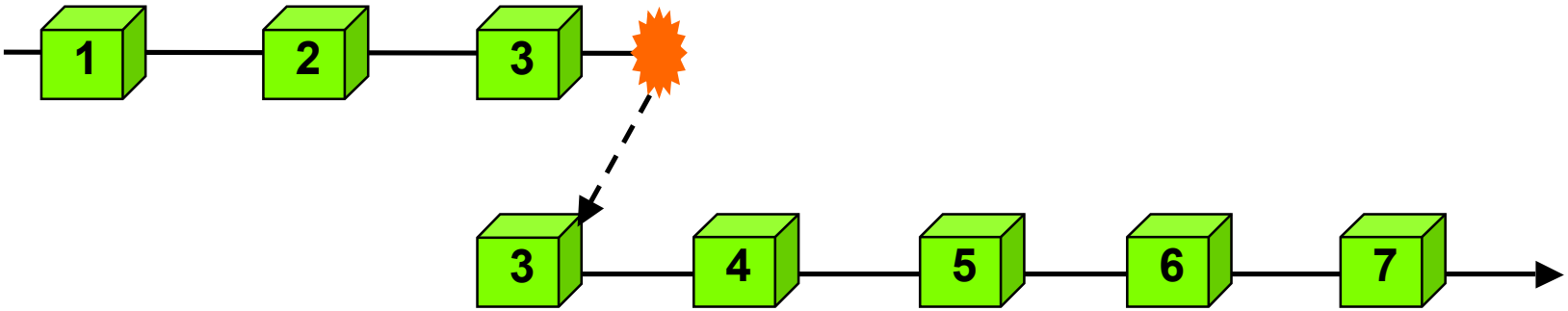


Fault Tolerance



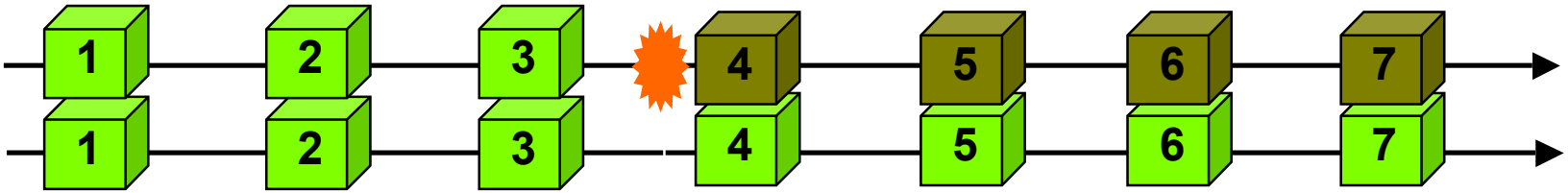
Error Processing

Backward recovery



Forward recovery

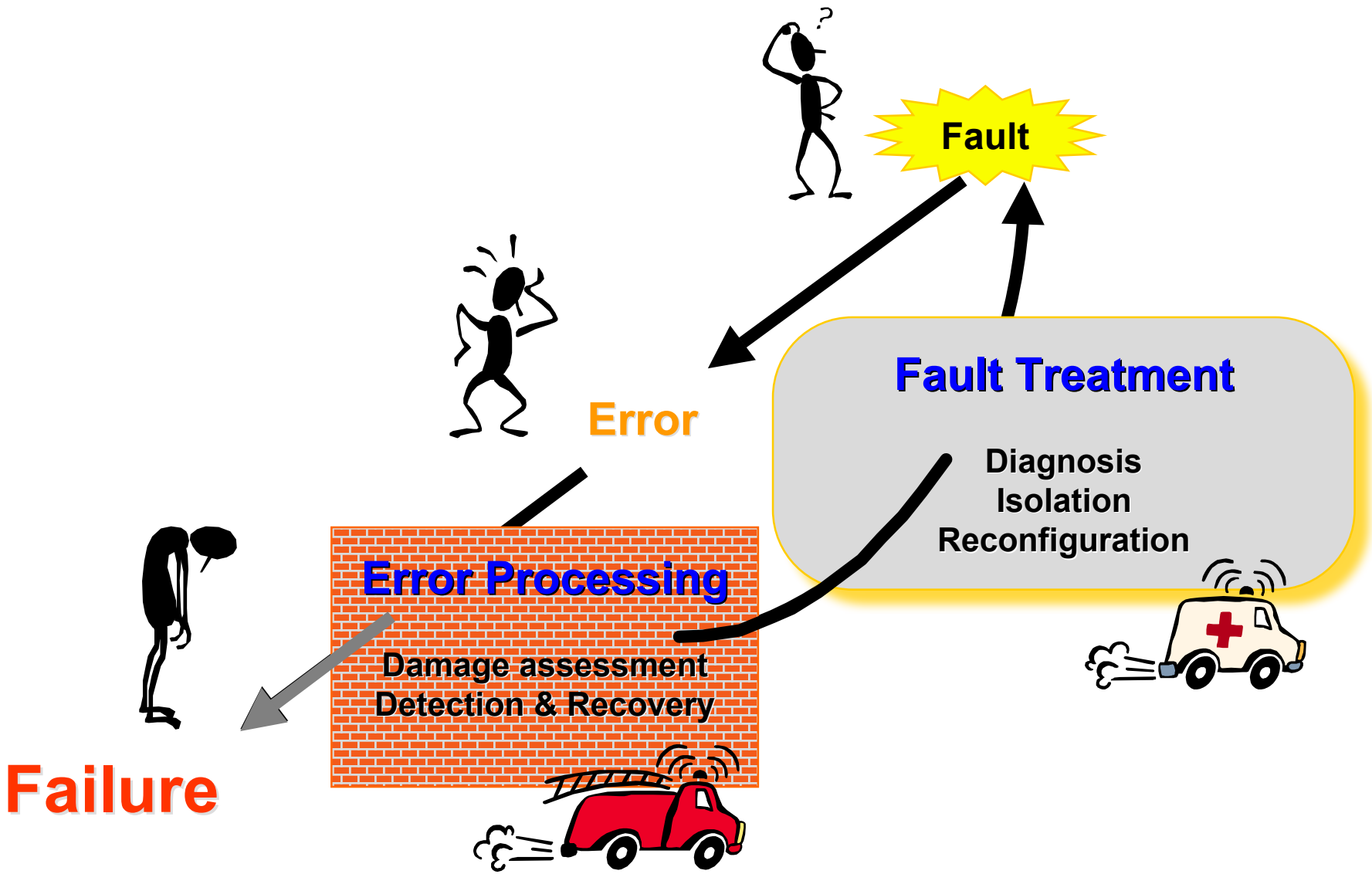
Compensation-based recovery (fault masking)



Error Processing (wrt intrusions)

- Error (security policy violation) detection
  - + Backward recovery (availability, integrity)
  - + Forward recovery (availability, confidentiality)
- Intrusion masking
  - Fragmentation (confidentiality)
  - Redundancy (availability, integrity)
  - Scattering

Fault Tolerance

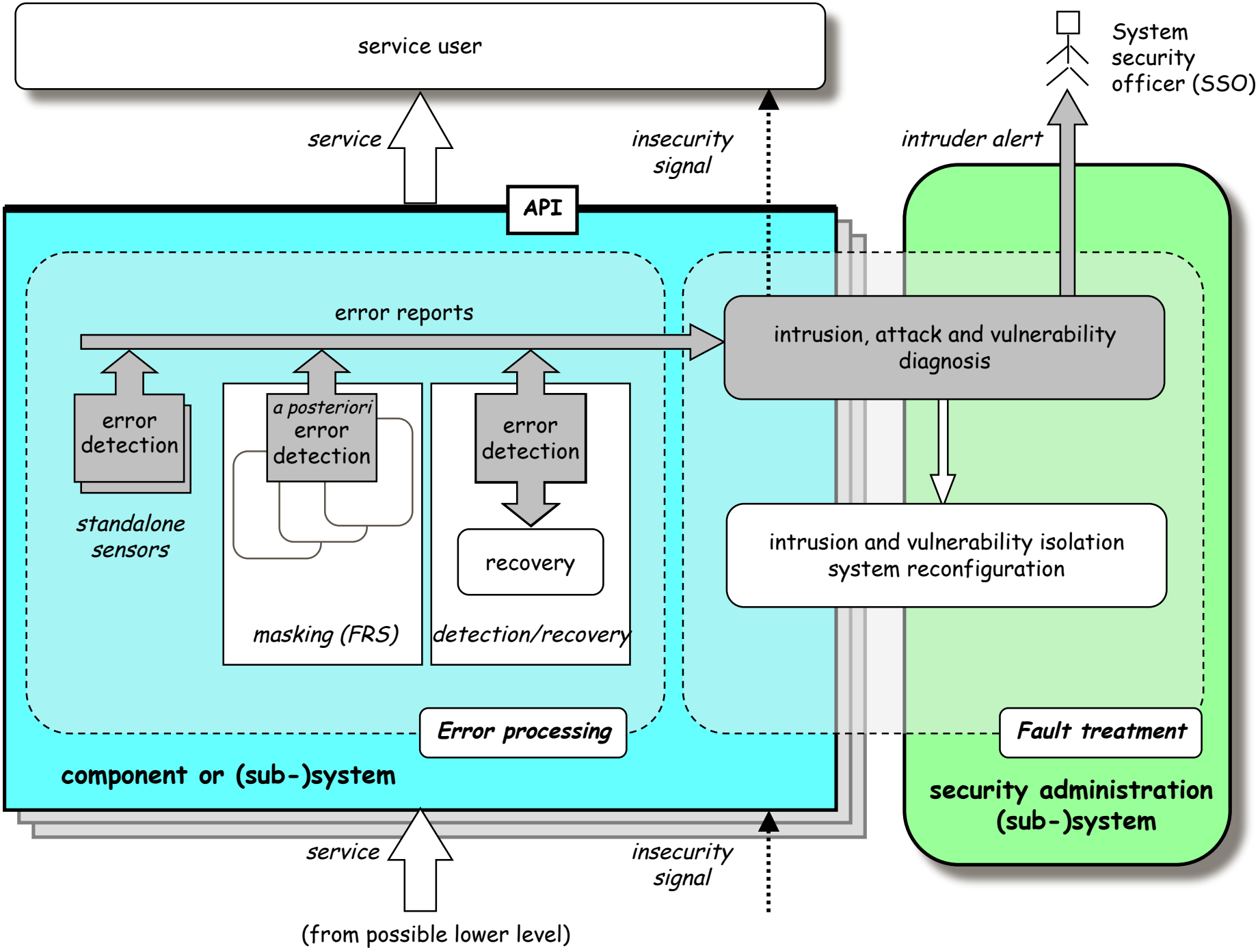


Fault Treatment

- Diagnosis
  - determine cause of error, i.e., the fault(s)
    - localization
    - nature
- Isolation
  - prevent new activation
- Reconfiguration
  - so that fault-free components can provide an adequate, although degraded, service

Fault Treatment (wrt intrusions)

- Diagnosis
  - Non-malicious or malicious (intrusion)
  - Attack (to allow retaliation)
  - Vulnerability (to allow removal)
- Isolation
  - Intrusion (to prevent further penetration)
  - Vulnerability (to prevent further intrusion)
- Reconfiguration
  - Contingency plan to degrade/restore service
    - inc. attack retaliation, vulnerability removal


service user
System security officer (SSO)
service
insecurity signal
intruder alert
API
error reports
intrusion, attack and vulnerability diagnosis
error detection
a posteriori error detection
error detection
recovery
intrusion and vulnerability isolation system reconfiguration
standalone sensors
masking (FRS)
detection/recovery
Error processing
Fault treatment
component or (sub-)system
security administration (sub-)system
service
insecurity signal
(from possible lower level)

http://www.research.ec.org/maftia/