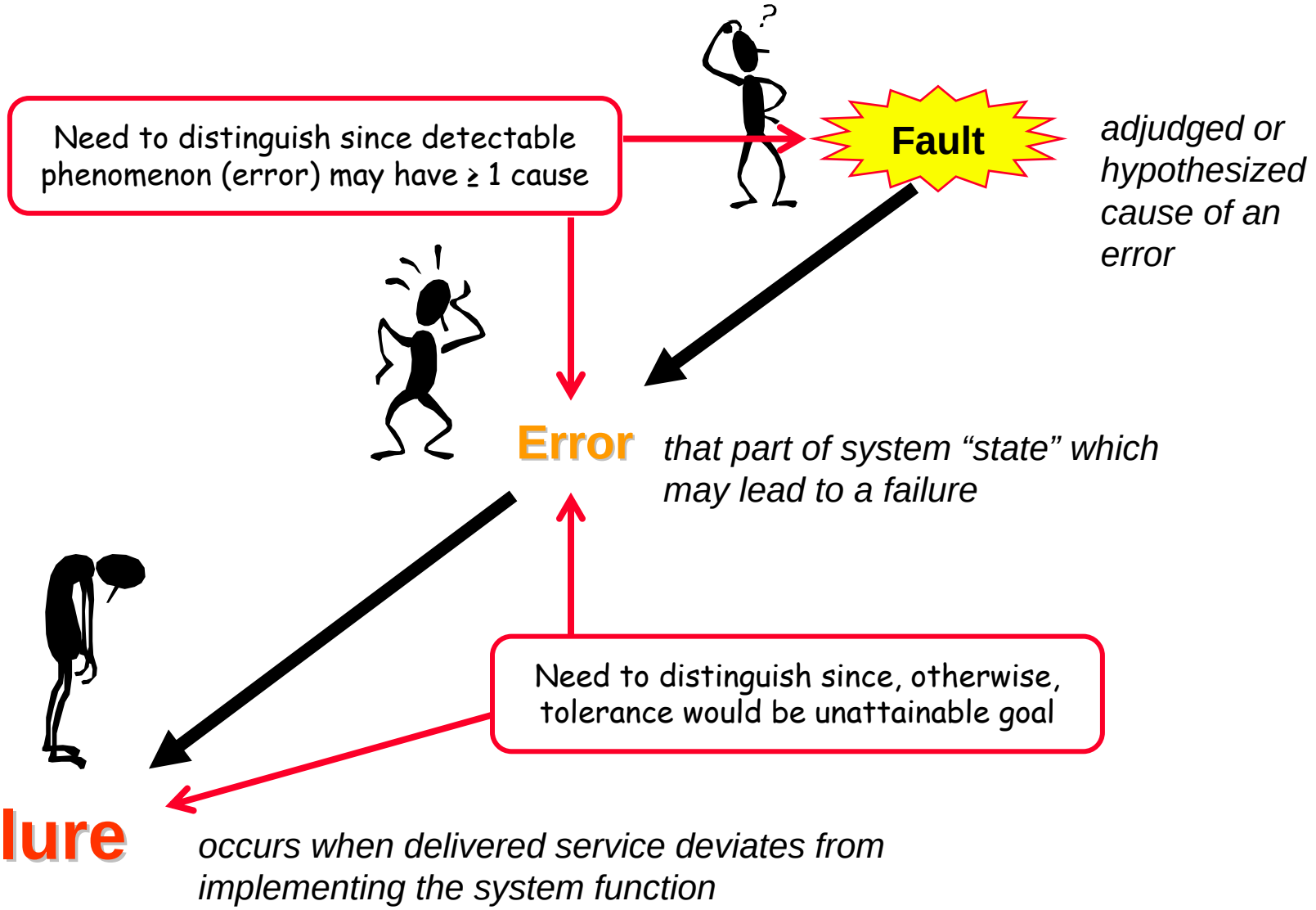

# MAFTIA
# Conceptual Model

Presented by Robert Stroud, Newcastle
MAFTIA Workshop, Newcastle, Feb 18-19, 2003

# D21 - Conceptual Model and Architecture of MAFTIA

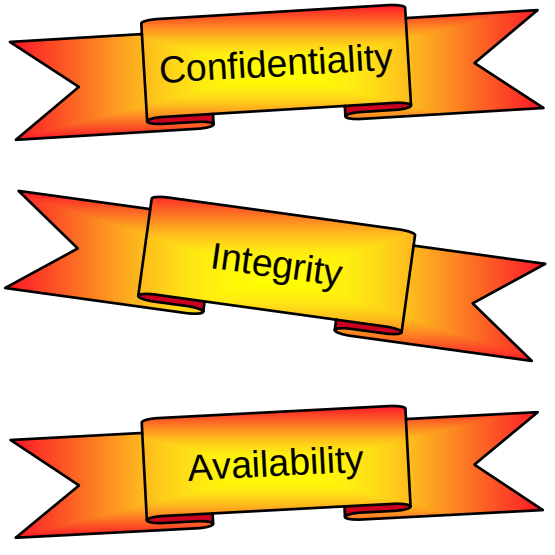
- Chapter 1 Introduction
- Chapter 2 Fundamental concepts of dependability
- Chapter 3 Refinement of core concepts with respect to malicious faults
- Chapter 4 Intrusion tolerance
- Chapter 5 Architectural overview
- Chapter 6 Verification and Assessment
- Chapter 7 Conclusion

# Causal Chain of Impairments

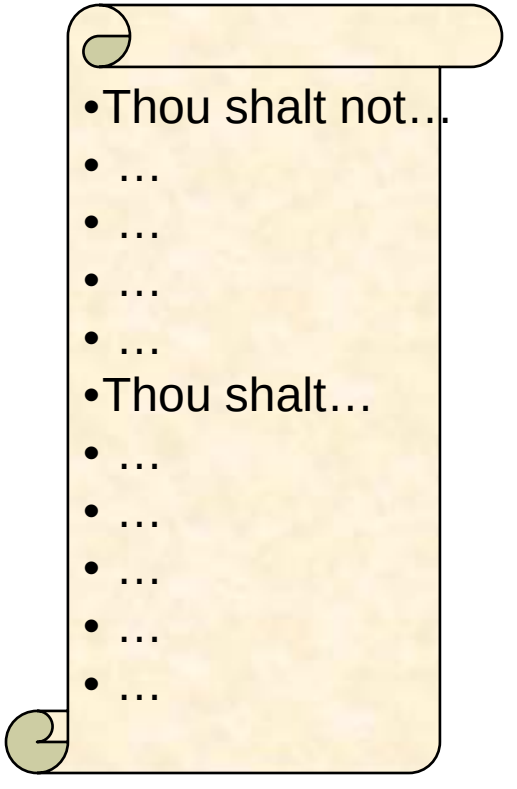


# Security Policy

- Security goals (expressed in terms of security properties) that are to be fulfilled by the system

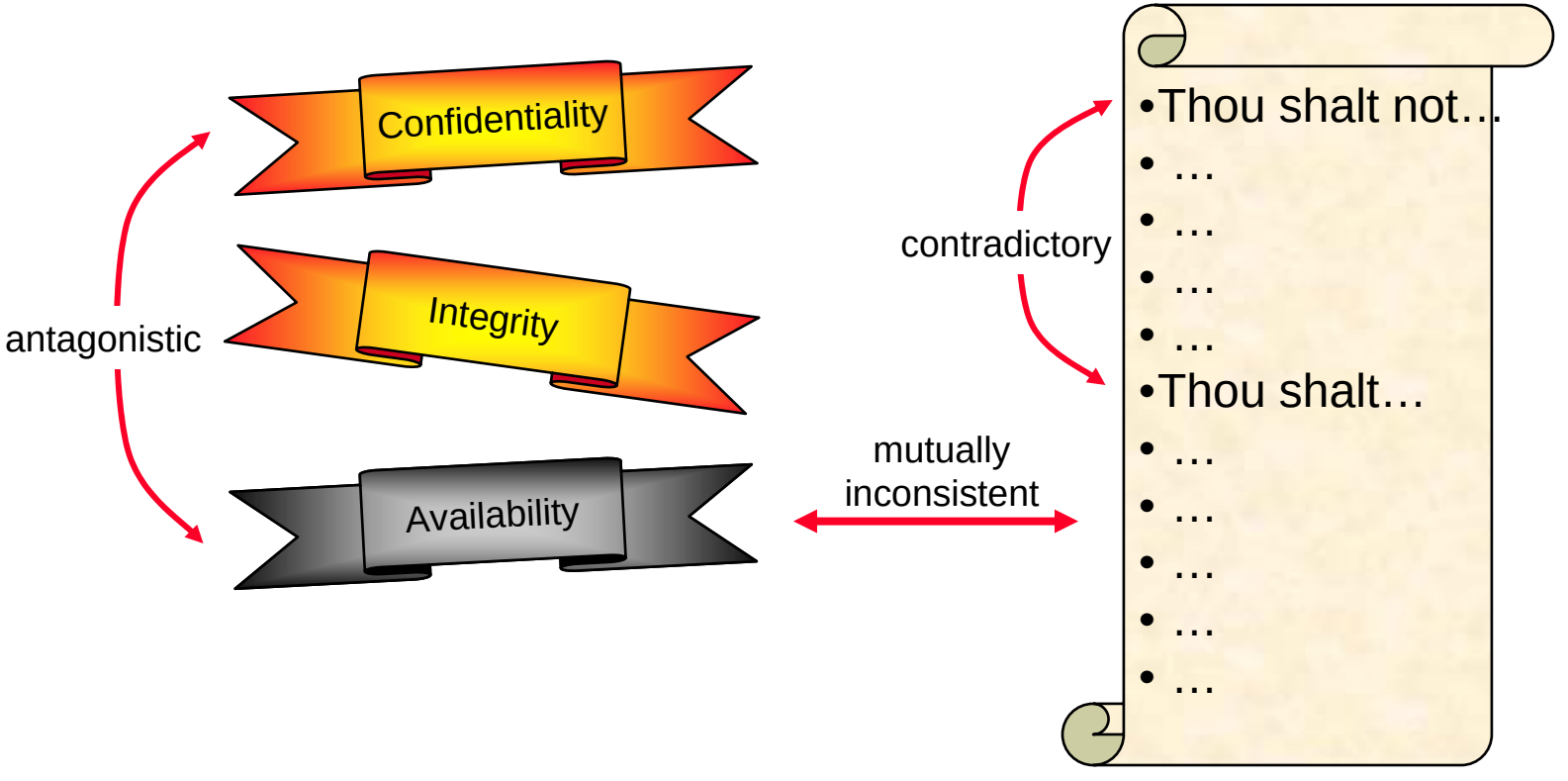



- Security rules that are intended to constrain the behaviour of the system



# Security Failure

- A security failure occurs if one of the high level goals of the security policy is violated



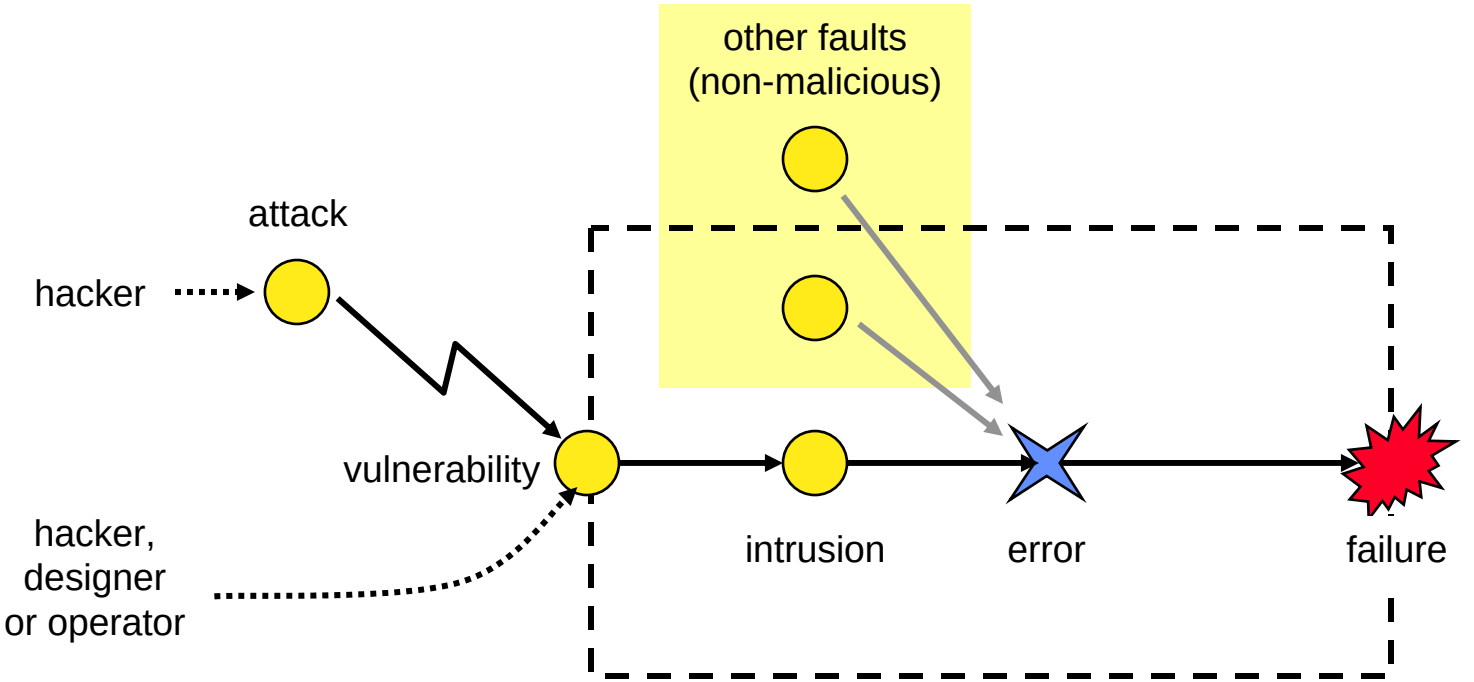
# The enforcement gap

- Security policies seek to constrain the behaviour of the full system:
  - Computer, users, security officer, adversaries
- Include duties, obligations, responsibilities
- Access control policies embody the "enforceable" aspects of the policy
- Socio-technical mechanisms seek to constrain the humans
- In practice, there is a gap between the intended security policy and the enforceable policy
- Thus, users are "trusted" not to misuse their rights

# Causes of Security Failures

- Failures of policy:
  - Faults in the specification of the security goals
  - Faults in the specification of the security rules
- Failures of mechanism:
  - Faults in the implementation of the technical rules
  - Faults in the underlying security mechanisms
- Other failures
  - Faults caused by deficiencies of formal models
  - Faults in the socio-technical mechanisms
- Abuse of privilege vs theft of privilege
  - Abuse of privilege -> failure of social mechanism
  - Theft of privilege -> failure of technical mechanism

# Attack, Vulnerability, Intrusion




- **attack (*human*)** – a malicious human interaction *fault,* whereby an attacker aims to deliberately violate one or more security properties; an *intrusion* attempt
- **attack (*technical*)** – a malicious technical interaction *fault* aiming to exploit a *vulnerability* as a step towards achieving the final aim of the attacker
- **vulnerability** – a fault created during development of the system, or during operation, that could be exploited to create an *intrusion*
- **intrusion** - a malicious externally-induced fault resulting from an *attack* that has been successful in exploiting a *vulnerability*

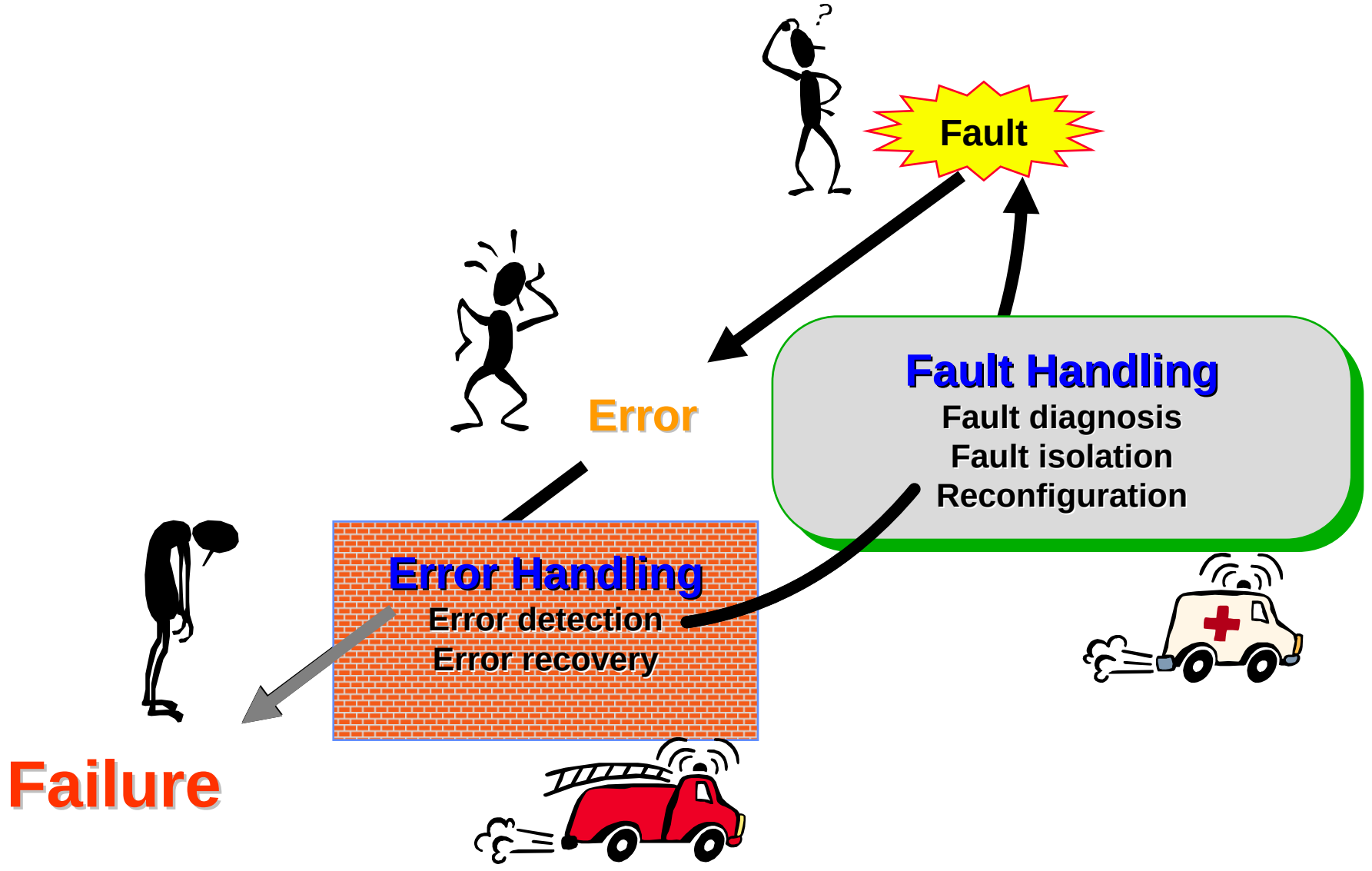
# Dependability Methods

| | |
|---|---|
| **Fault prevention** | how to prevent the occurrence or introduction of faults |
| **Fault tolerance** | how to provide a service capable of or implementing the system function despite faults |
| **Fault removal** | how to reduce the presence (number, severity) of faults |
| **Fault forecasting** | how to estimate the presence, creation and consequences of faults |

# Security Methods

| Fault | Attack (human sense) | Attack (technical sense) | Vulnerability | Intrusion |
|---|---|---|---|---|
| **Prevention** (how to prevent occurrence or introduction of…) | deterrence, laws, social pressure, secret service… | firewalls, authentication, authorisation… | semi-formal and formal specification, rigorous design and management… | = attack & vulnerability prevention & removal |
| **Tolerance** (how to deliver correct service in the presence of…) | = vulnerability prevention & removal, intrusion tolerance | | = attack prevention & removal, intrusion tolerance | error detection & recovery, fault masking, intrusion detection, fault handling |
| **Removal** (how to reduce number or severity of…) | physical countermeasures, capture of attacker | preventive & corrective maintenance aimed at removal of attack agents (i.e., some forms of malicious logic) | 1. formal proof, model-checking, inspection, test… 2. preventive & corrective maintenance, including security patches | ⊆ attack & vulnerability removal |
| **Forecasting** (how to estimate present number, future incidence, likely consequences of…) | intelligence gathering, threat assessment… | assessment of presence of latent attack agents, potential consequences of their activation | assessment of: presence of vulnerabilities, exploitation difficulty, potential consequences… | = vulnerability & attack forecasting |

# Fault Tolerance



# Intrusion Detection: Definition

[NSA 1998]

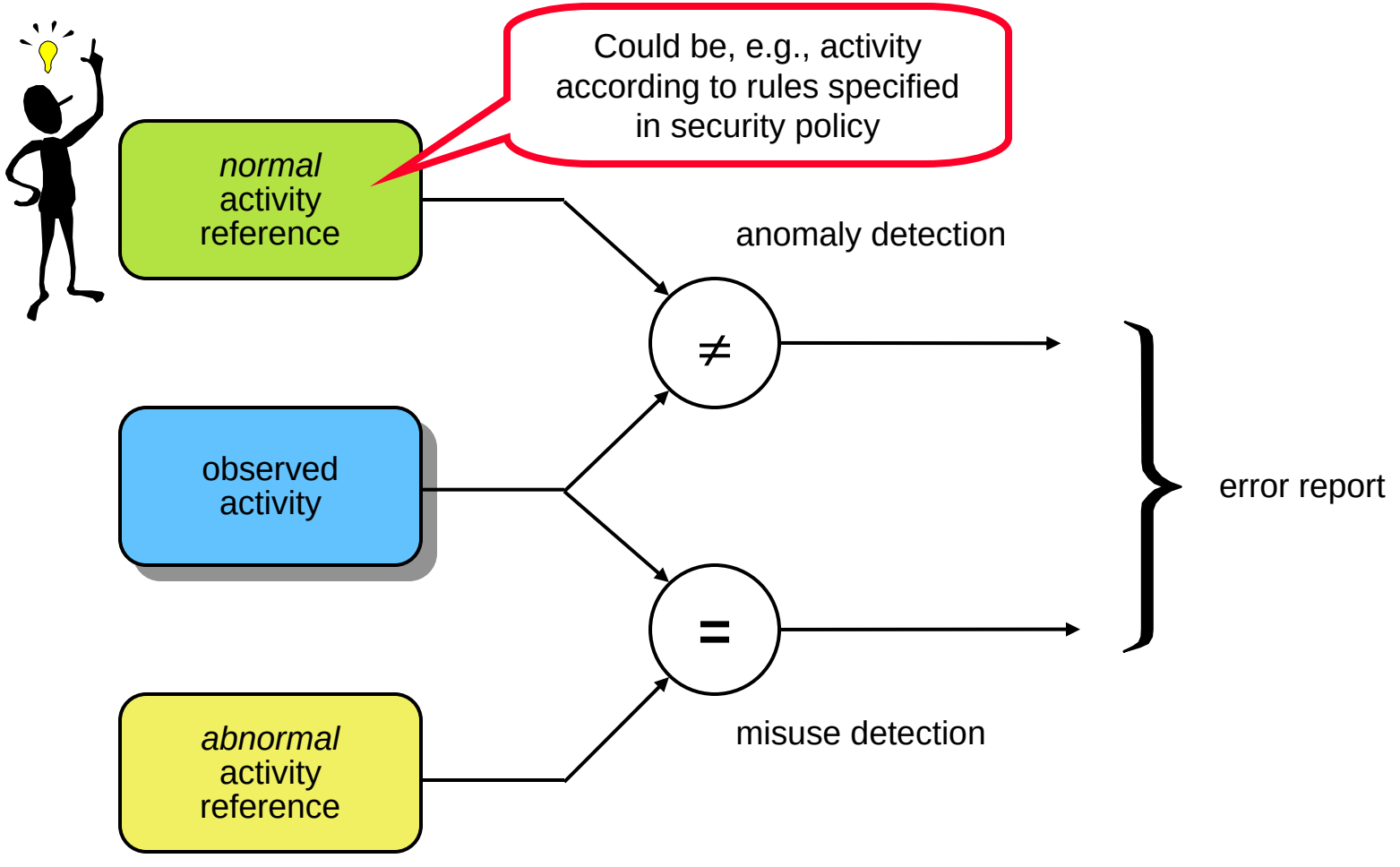
> " *Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network* "

**intrusion detection**: concerns the set of practices and mechanisms used towards:

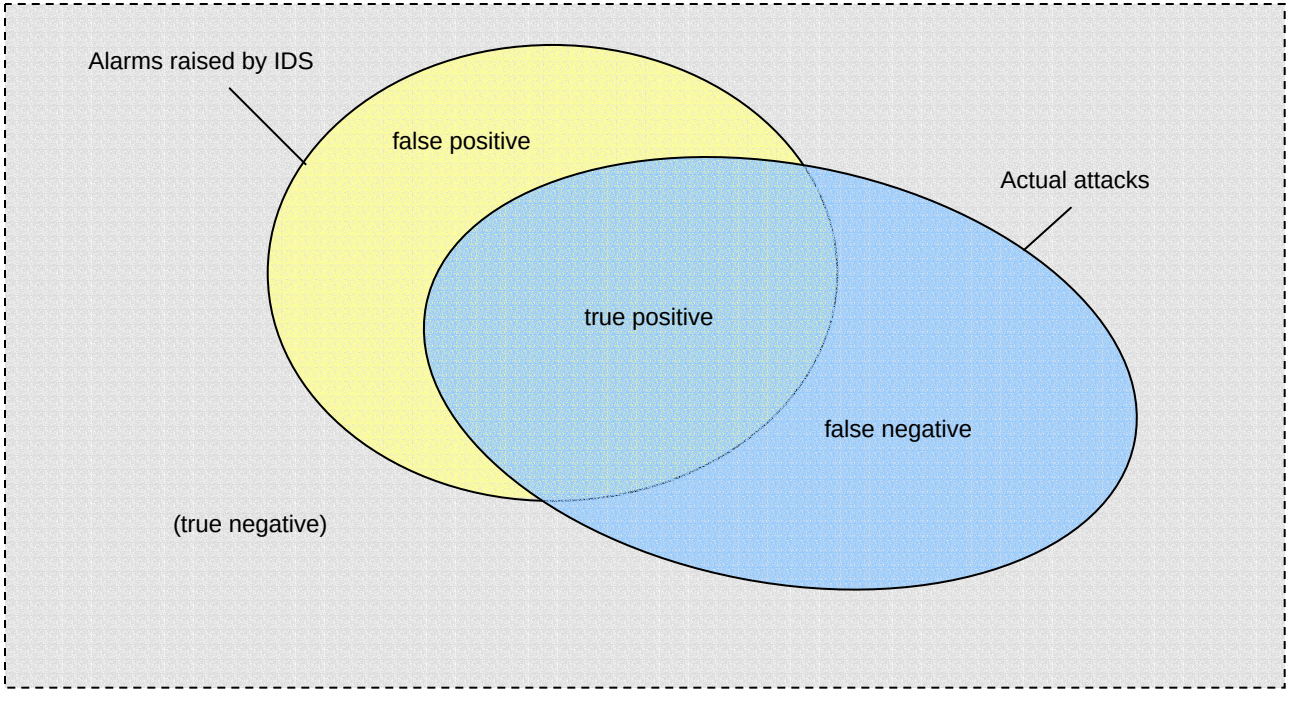
- detection of errors that may lead to security failure
- diagnosing intrusions, vulnerabilities and attacks

**intrusion detection system**: is an implementation of the practices and mechanisms of intrusion detection

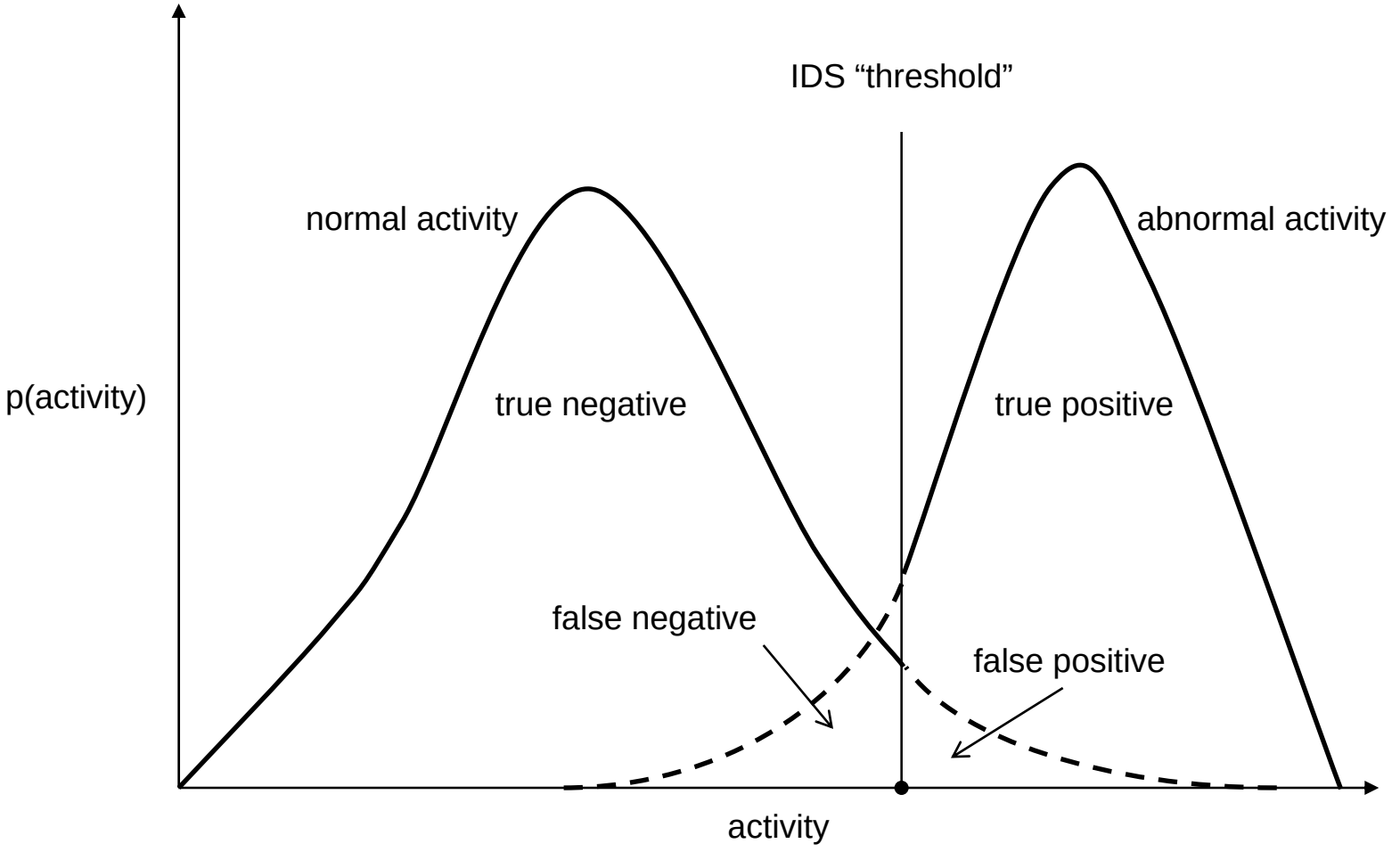
# Error Detection



# IDS events


Alarms raised by IDS
false positive
Actual attacks
true positive
false negative
(true negative)

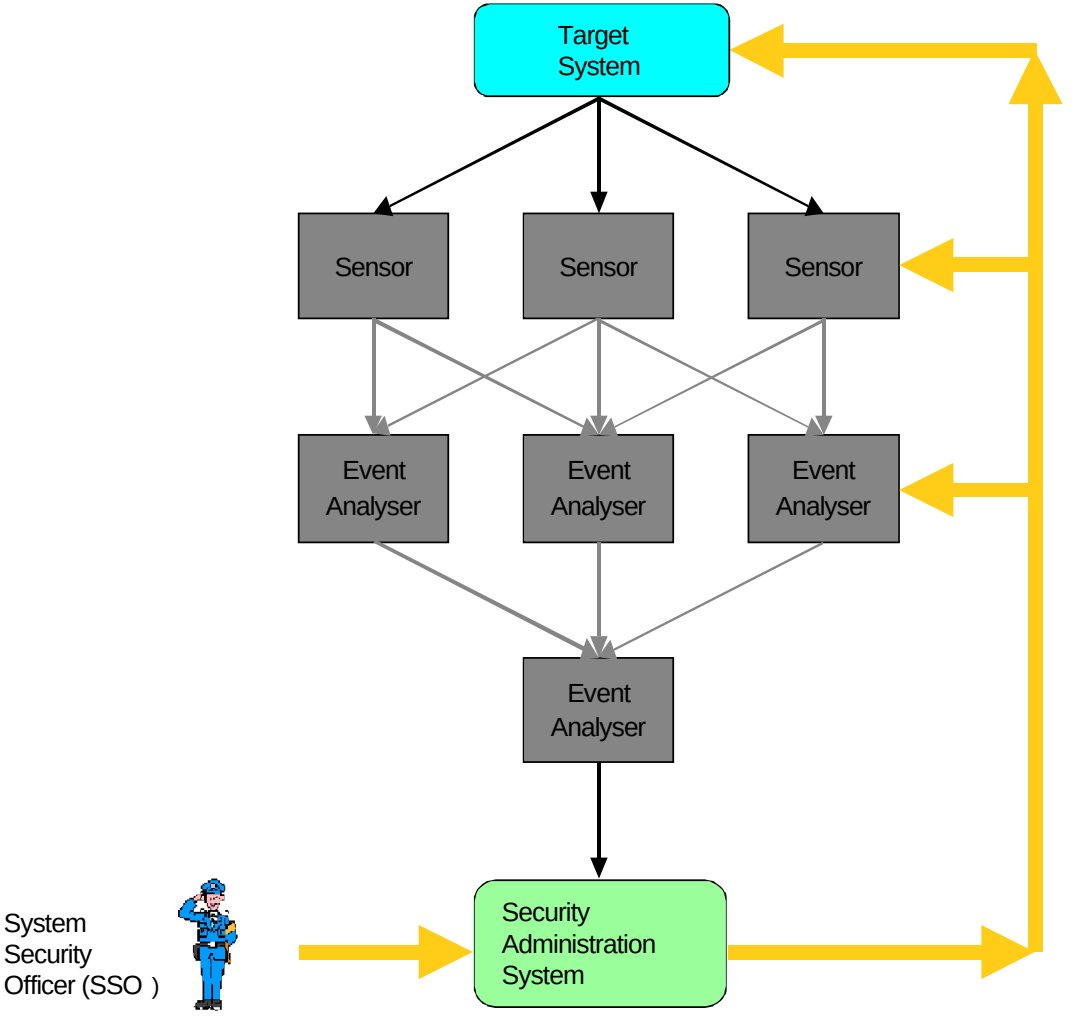
# Compromise between false negatives and false positives

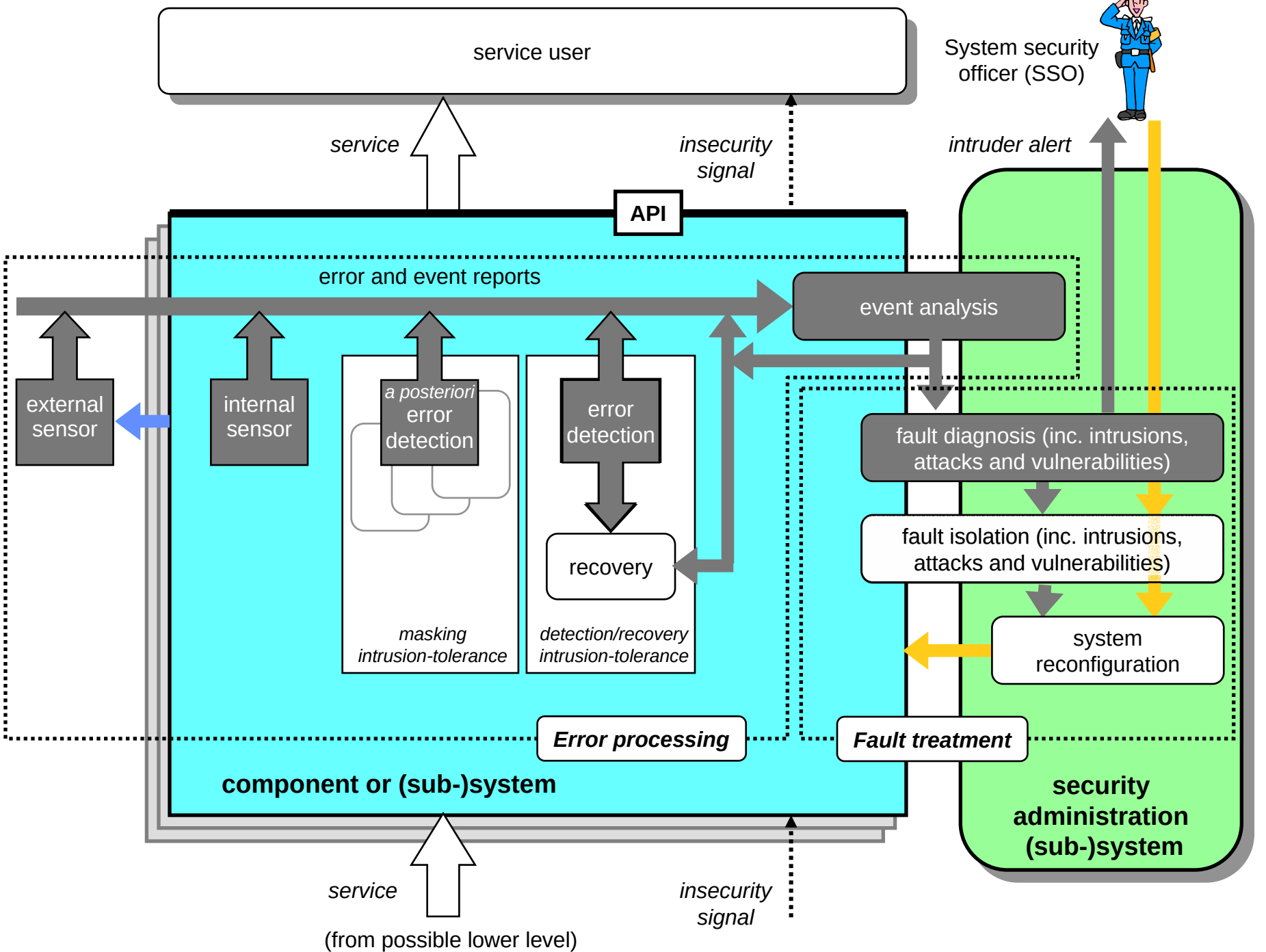


# Error Recovery

- Backward recovery
  - Operating system re-installation
  - TCP/IP connection resets
  - System reboots and process re-initialisation
  - Software downgrades
- Forward recovery
  - Automated re-keying procedures
  - Put system into diminished "safe" mode.
  - Software upgrades
- Masking
  - Voting mechanisms
  - Fragmentation-Redundancy-Scattering
  - Sensor correlation

# Error detection, fault diagnosis, and corrective maintenance




service user
System security officer (SSO)
service
insecurity signal
intruder alert
API
error and event reports
event analysis
external sensor
internal sensor
a posteriori error detection
error detection
recovery
fault diagnosis (inc. intrusions, attacks and vulnerabilities)
fault isolation (inc. intrusions, attacks and vulnerabilities)
system reconfiguration
masking intrusion-tolerance
detection/recovery intrusion-tolerance
Error processing
Fault treatment
component or (sub-)system
security administration (sub-)system
service
insecurity signal
(from possible lower level)

# A (very) Simple Example