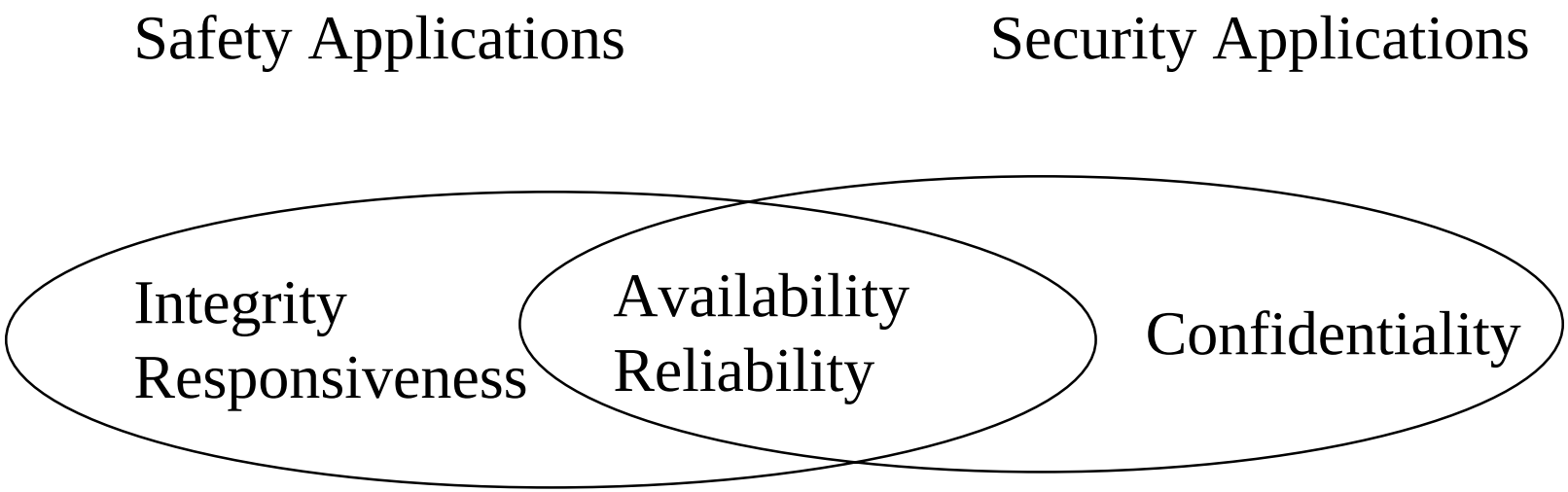
Adding Security to Operational Systems

Walt Heimerdinger
Honeywell Laboratories

IFIP WG 10.4 Meeting - 4 January 2002

Dependable Systems for Safety AND Security



“Classical” Dependability vs “Classical Security”

Assumes trustworthy operators

Assumes fault free system

Assumes closed system

Assumes open/connected system

Assumes timely response from dedicated resources

Assumes shared, generic platform

“Classical” Dependability vs “Classical Security”

Redundancy -multiple nodes and channels **Partitioning** -independent redundant channels **Design Audits** -code reviews/testing **Selection of redundant data** -voters/selectors	**Avoidance**	**Partitioning** -firewalls/router filters -VPNs **Design Audits** -open source code **Selection of actors** -authentication **Encryption**
Error detection codes **Parameter monitoring/limit checks**	**Sensing**	**Traffic monitoring** **Signature checks** **Anomaly checks**
System diagnostics/ mutual test	**Correlation**	**Intrusion state estimation**

“Classical” Dependability vs “Classical Security”

Fail silent shutdown of redundant node or channel	**Isolation**	**Rerouting** **-router filtering** **-IP shunning** **Host shutdown**
Fault masking	**Recovery**	**Rerouting** -router filtering -IP shunning **Host shutdown**
Reboot **Hardware repair**	**Repair**	**Backup site** **Scrub and Reinstall**

Conflicts -- Challenges

- Timeliness
- Severely limited resources
- Redundancy
- Closed trust model
- Continuous operation through upgrades
- Extensive use of proprietary systems
- Encryption and Authentication
- Confidentiality
- Open trust model
- Up to date security patches
- Extensive use of COTS