

ISRCS 2008



Practical Aspects of Applying Wireless Technology in Process Automation Environment

Alex Chernoguzov
Honeywell

September 9-10, 2008
Idaho Falls, Idaho

ISA100 Usage Classes

<i>Category</i>	<i>Class</i>	<i>Application</i>	<i>Description</i>
Safety	0	Emergency action	(always critical)
Control	1	Closed loop regulatory control	(often critical)
	2	Closed loop supervisory control	(usually non-critical)
	3	Open loop control	(human in the loop)
Monitoring	4	Alerting	Short-term operational consequence (e.g., event-based maintenance)
	5	Logging and downloading/uploading	No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)

Importance of message timeliness increases

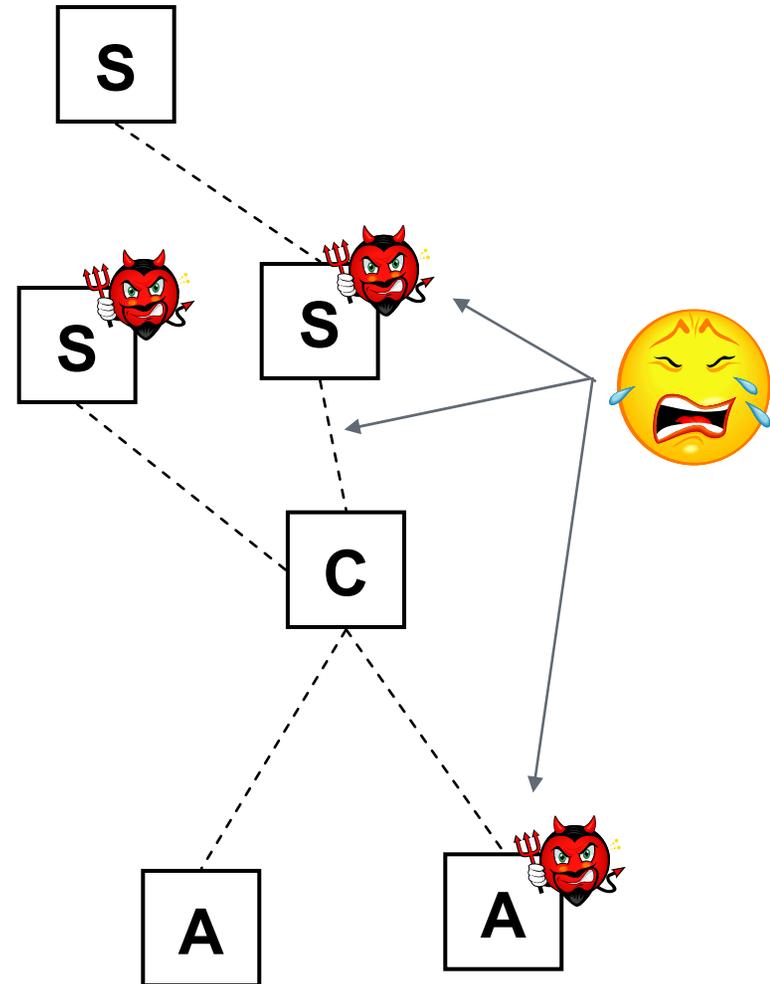
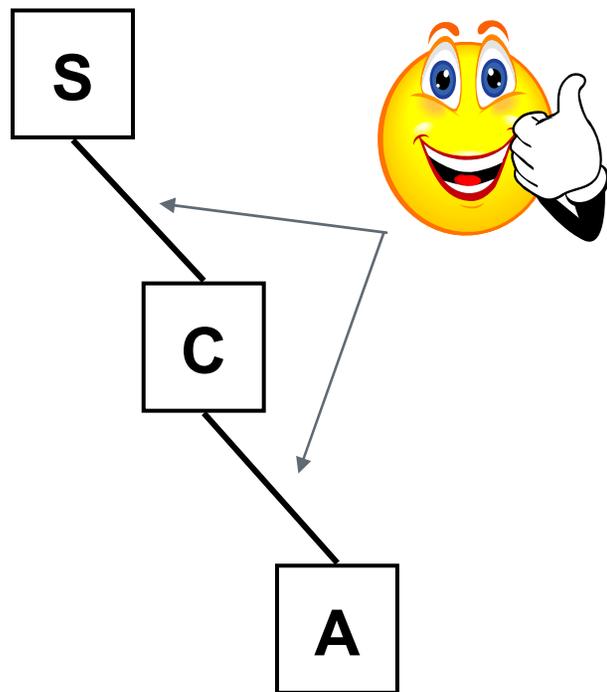


Level of comfort



- ❖ Why low levels of comfort?
 - Wireless is less secure
 - Wireless is less reliable
 - Wireless is less deterministic

Wireless Security Fears



Wireless Security

Security Basics

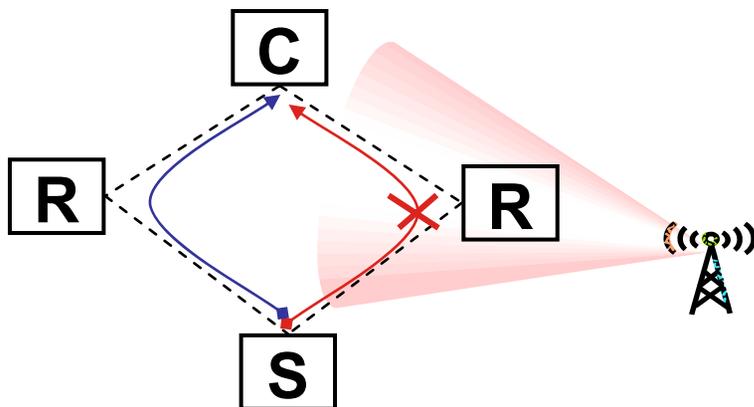
- ❖ Source authentication
 - Only accept data from known sources. Data source authenticity is cryptographically verified.
- ❖ Data integrity
 - Protect application data with cryptographic integrity code. Prevent data tampering by intermediate nodes.
- ❖ Confidentiality
 - Encrypt application data. Only source and destination understand the context.
- ❖ Auditing
 - Log unauthorized access attempts, decryption failures.

Resilience Aspects

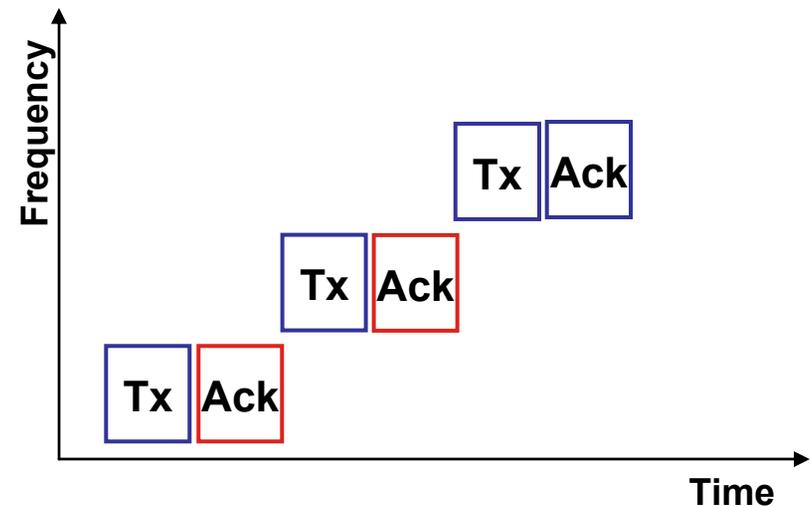
- ❖ Limit scope of trust
 - Different communication sessions do not share any state or cryptographic material.
 - Compromised device can only affect limited set of communication partners
- ❖ Unverified trust decays with time
 - Periodically refresh key material
- ❖ Assume humans are the weakest link
 - Keep humans away from security key material
 - Keep humans away from trust maintenance activities

Wireless Reliability – Interference

- ❖ Wireless signal can be jammed
 - **Accidentally by plant interference sources**
 - **Intentionally by an attacker**
- ❖ Traditional defense techniques
 - **Spatial diversity**
 - **Temporal diversity**
 - **Frequency diversity (FH/DS etc.)**



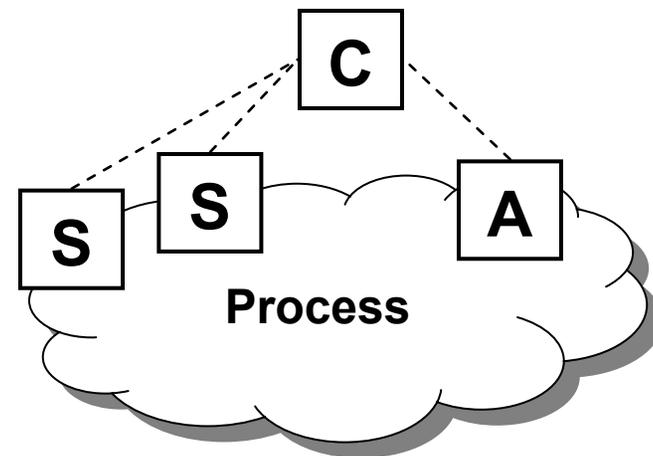
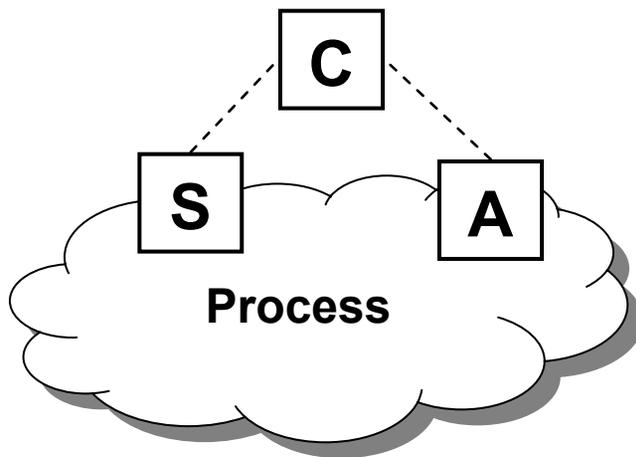
- ❖ Mesh networking
 - Multiple data paths
 - No single point of failure
 - Load balancing
 - Failure avoidance routing
- ❖ Advanced anti-jamming techniques



Wireless Reliability – Control Aspects

❖ Dealing with missing data

- Sensor redundancy
 - MVC instead of SVC algorithms
- MPC techniques
 - Variations of Kalman filter to reconstruct missing data



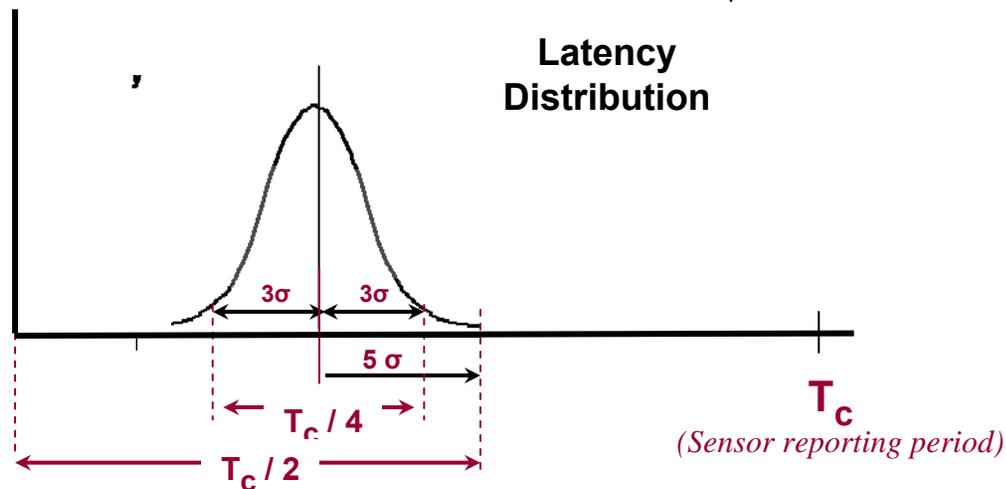
Wireless Determinism

❖ Manage wireless network access and bandwidth

- TDMA rather than CSMA media access
- Latency and jitter constraints
 - Controlled number of retries
 - Controller number of mesh hops
 - Time-synchronous routing

❖ Mesh network fault isolation/localization

- Prevent fault of one node to disrupt wide areas of the mesh network
- Keep latency/jitter constraints when re-routing around faults



ISRCS 2008



Practical Aspects of Applying Wireless Technology in Process Automation Environment

Alex Chernoguzov	alexander.chernoguzov@honeywell.com	(215) 641-3279
------------------	----------------------------------------------------------------------------------------------	----------------