

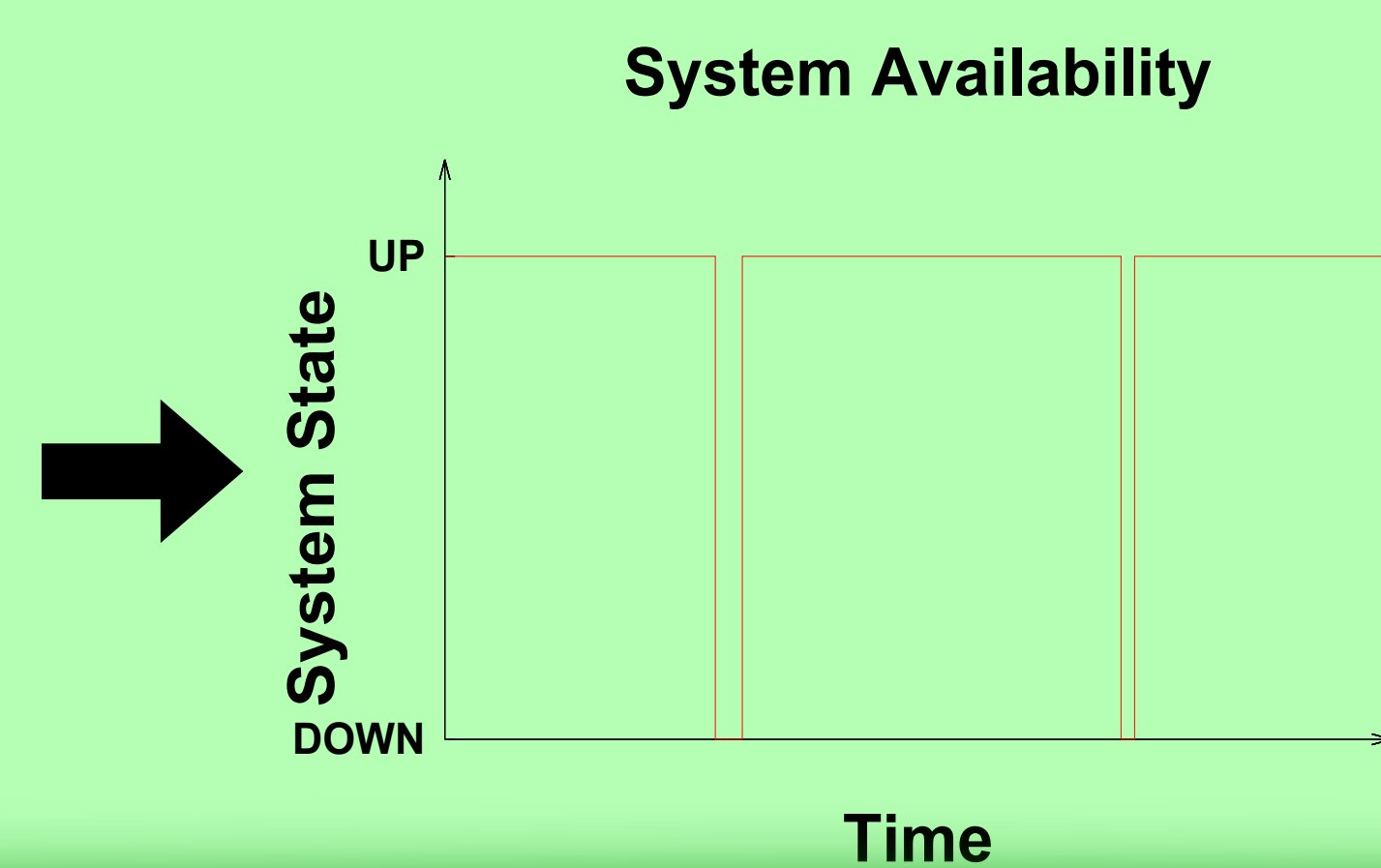
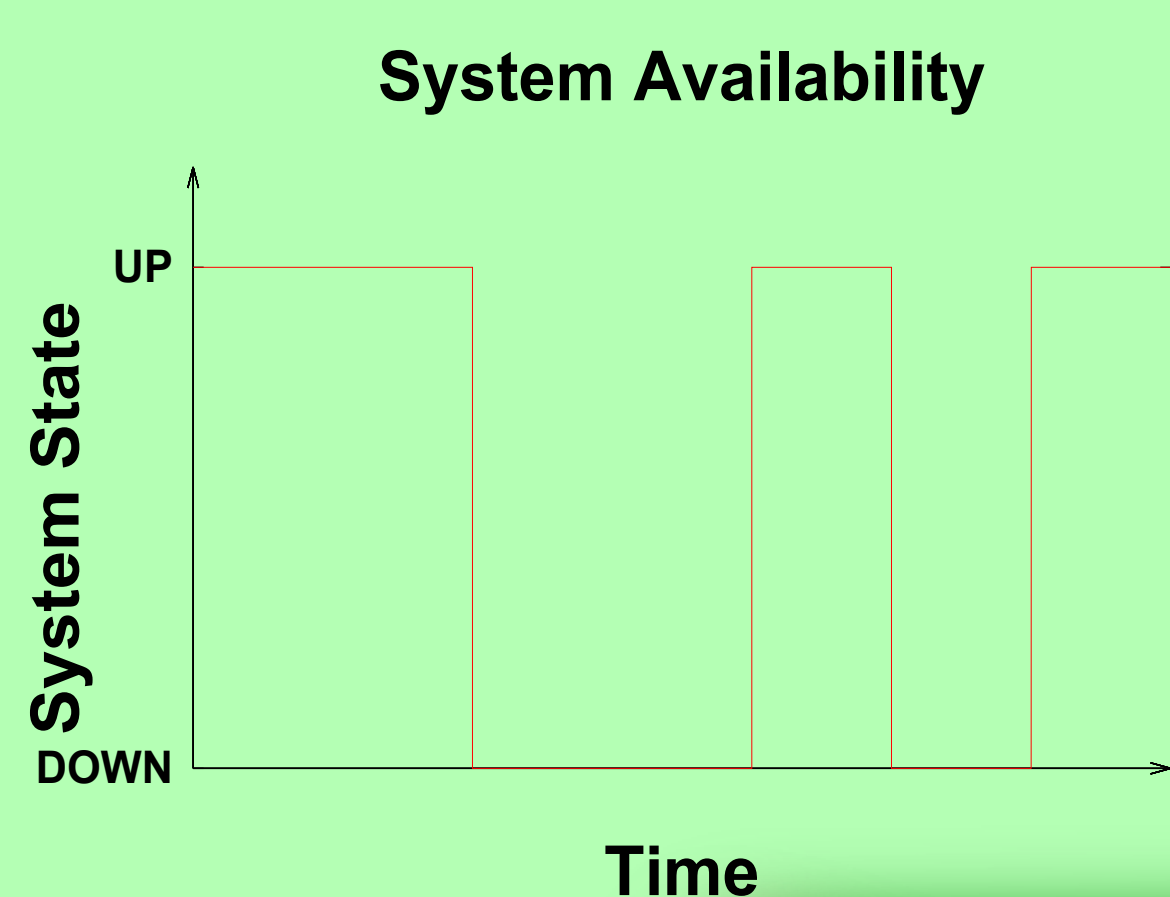
Problem and Motivation

- KNX: Home- and Building Automation System used for services considered 'uncritical' like heating, ventilation, ...
- Critical applications like elevation control, access control or burglar alarms are based on dedicated systems
- Idea: unify critical and uncritical systems into one system to reduce maintenance costs
- Problem: no unified concept for providing the full CIA triad AND high availability at disposal

Design Goals

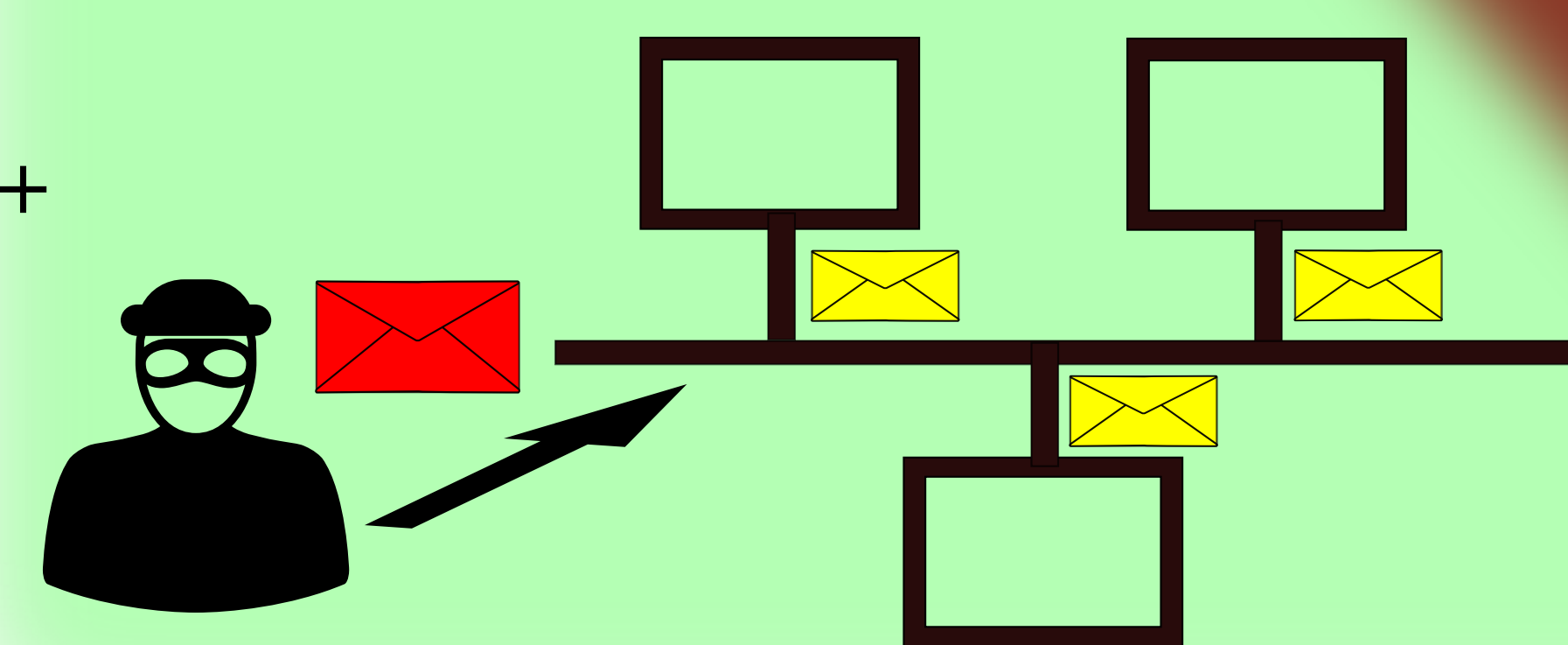
- Provide high-availability by utilizing independent communication lines and independent bus interfaces
- Also provide confidentiality and integrity by implementing strong cryptographic mechanisms
- Keep interoperability in mind by using 'plug-and-play' functionality
- Keep protocol overhead as small as possible
- Provide a prototype as proof-of-concept

Computational Security - the 'CIA Triad'



- To increase availability:
- Achieve high reliability
 - Keep 'mean-time-to-repair' low
 - Protect network from DOS attacks
 - Guard against transient hardware faults

Keep active attackers out by using message authentication codes to detect injection of arbitrary or replayed packages

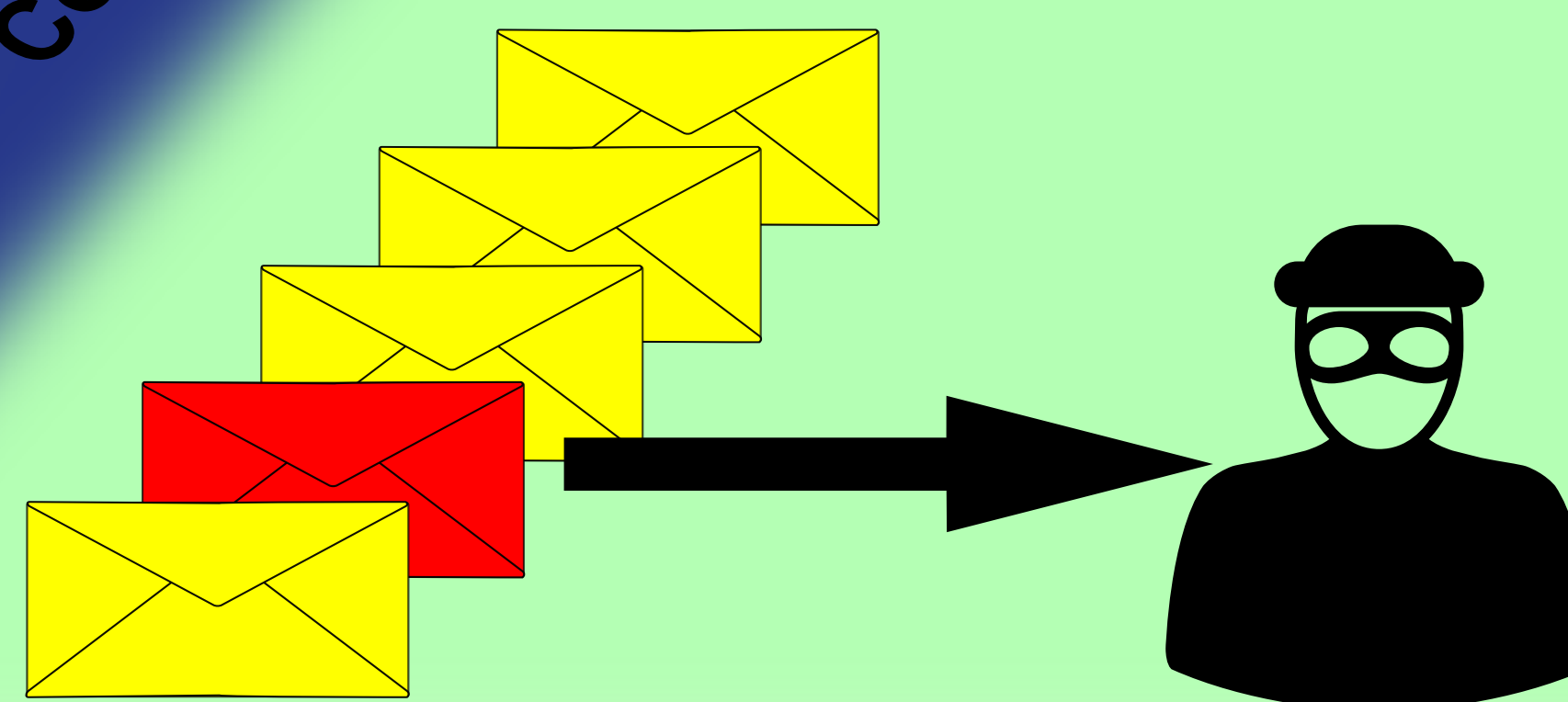


Availability

Integrity

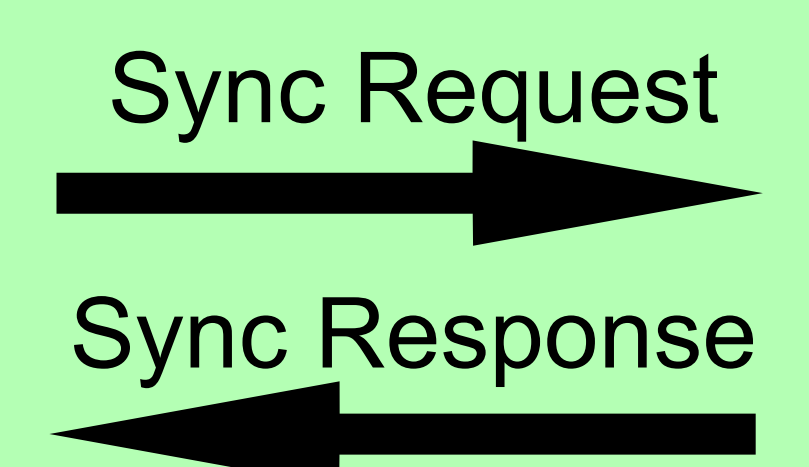
Confidentiality

Keep passive attackers out by utilizing strong encryption to hide exact topology from attacker and make traffic analysis difficult

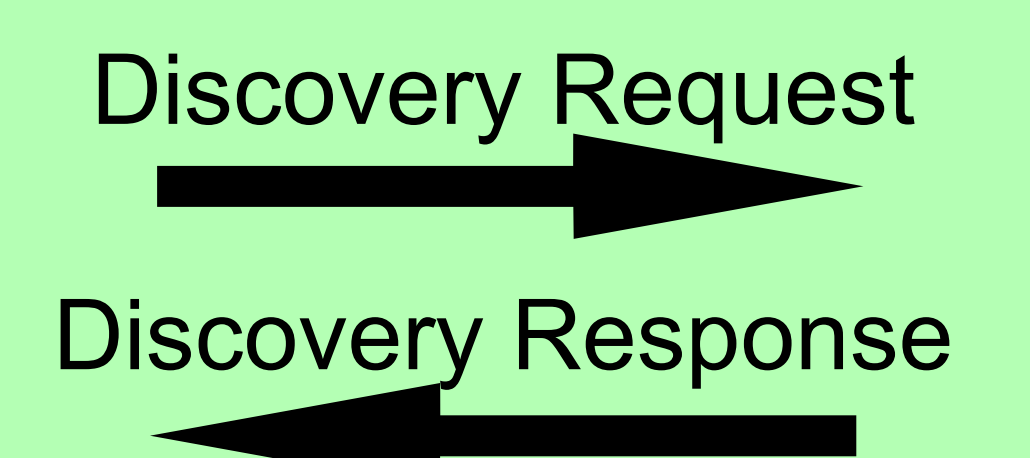


Protocol Overview

Synchronization Service for distributing global counter to assure data freshness



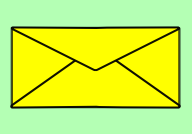
Discovery Service to achieve end-to-end encryption with perfect forward secrecy



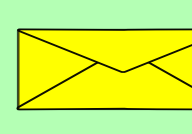
Data Service for secure communication



Operational Overview

1. Standard KNX device sends package 

2. Gateway determines responsible remote gateways and establishes independent asymmetric point-to-point session keys for both communication lines

3. Gateway encrypts and wraps original package  into two independent KNX packages, destined for the responsible remote gateway

4. The two packages are sent independently from each other

5. Based on a counter, the receiving gateway discards the duplicate, and forwards the decrypted original message to the intended final destination

