Contribution to Envri+
Workshop on SMART Cable Systems

Secure Data Communication Protocol
For Large Number of Distributed Sensors

Brest, France, 13 November 2017

Fadi Obied, Philippe Dhaussy

Univ. Européenne de Bretagne
Lab-STICC / MOCS
UMR CNRS 6285
ENSTA-Bretagne, Brest

fadi.obeid@ensta-bretagne.org
philippe.dhaussy@ensta-bretagne.fr

Presentation Plan

- Context
- Insecure Model
  - Architecture and Functioning
- Conventional Security (AES256)
  - Scheme and Application
- Proposed Solution (RITA)
  - Scheme and Application
- Comparison
- Prototype
  - Simulation and Future Work
- Conclusion

Context

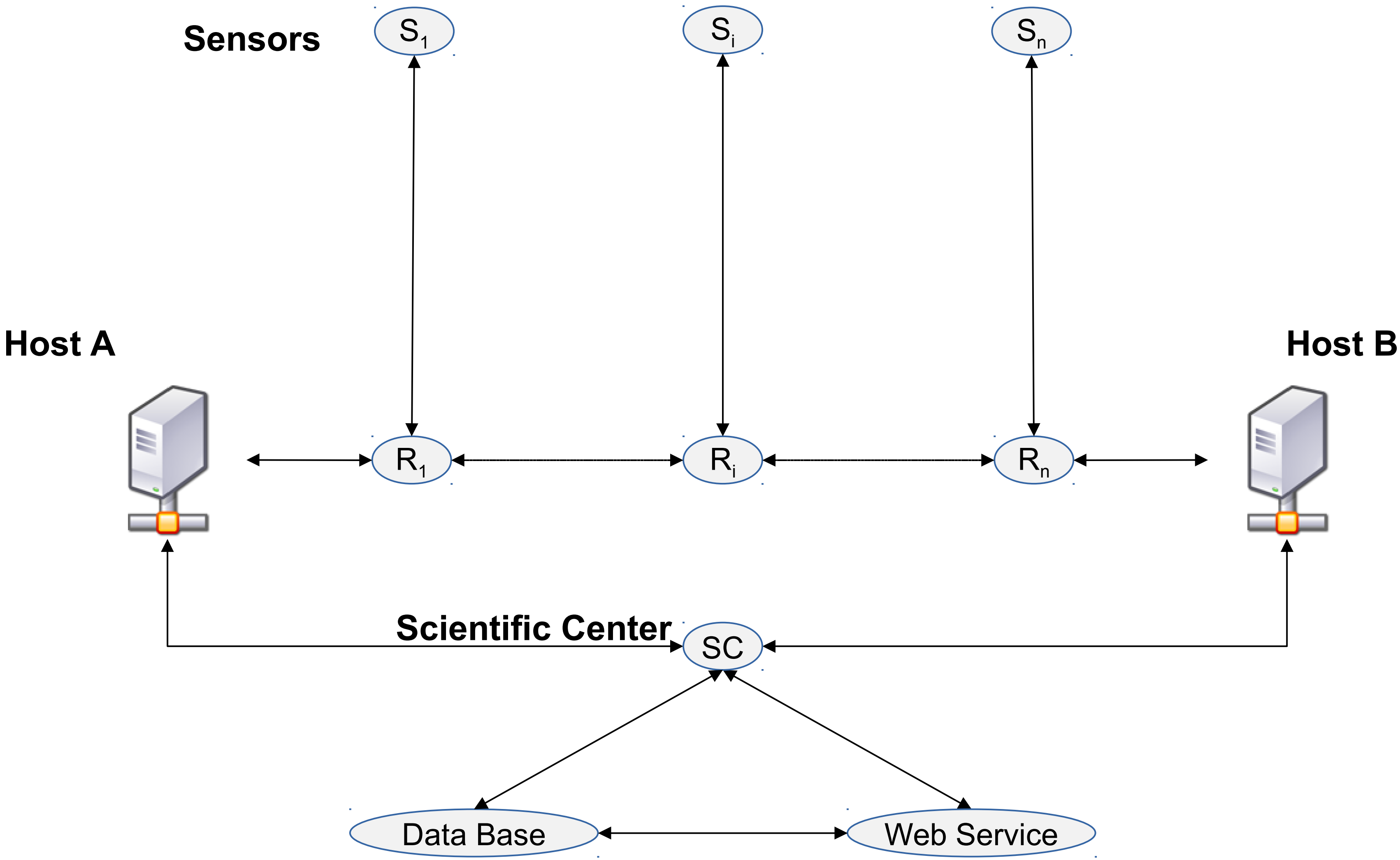
- The Joint Task Force (ITU-WMO-UNESCO IOC) investigates the potential of using submarine telecommunication cables for ocean and climate monitoring and disaster warning.

- The objectives of this contribution are to provide baseline requirements that will improve the security of data communication between sensors and data base hosts.

- The communication needs to have specific security properties as confidentiality, authenticity, integrity, availability, Interruptibility

- This contribution investigates an appropriate data encoding to secure data transmission.

Architecture



System Information

- **Sensors (S):**
  - They send data to hosts.
  - They do not need to be owned by the research headquarters.
- **Repeaters (R):**
  - They are owned by the same company as the communication line.
- **Hosts:**
  - Can be owned by different countries or companies.
- **Scientific Center (SC):**
  - Collects data from sensors.
- **Data Base:**
  - Provides an archive of collected data.
- **Web Services:**
  - Provides access to live and archived data.

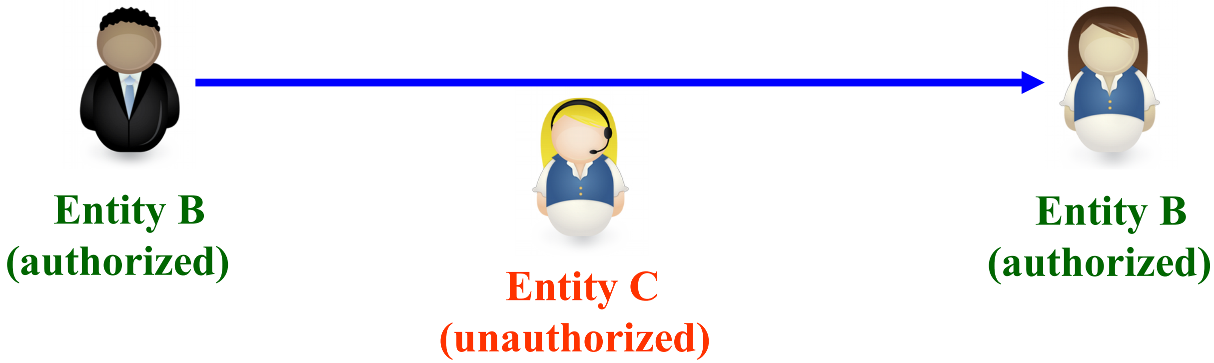
Functioning

- **Data Acquisition:**
  - Sensor S_i sends (IDS_i,data) to Host A or B, or both.
  - Hosts forward data to the scientific center.
- **Archiving:**
  - SC insures received data are stored in one or multiple data bases.
- **Public and private access:**
  - Web services provide secure access to live and stored data.
- **Control and configuration:**
  - SC should be able to control, configure, and completely manage sensors.
  - To configure S_i, SC sends (IDS_i,data) through hosts.

Security

- Concerns:
  - Communication between sensors and SC only.
- Confidentiality:
  - Messages between S_i and SC are only readable by S_i and SC.
- Authenticity:
  - Messages received by SC originate only from S_i (the correct one).
  - Messages received by S_i originate from SC.
- Integrity:
  - Messages between S_i and SC cannot be modified by other parties.
- Availability:
  - If at some point the communication is interrupted, both S_i and SC would know.
- Interruptibility:
  - Communication can be interrupted by hosts.
  - Data sent from sensors during the interruption phase are collected by hosts.
  - Unchanged, unread, collected data can be forwarded to SC after interruption.

Classic Cryptography



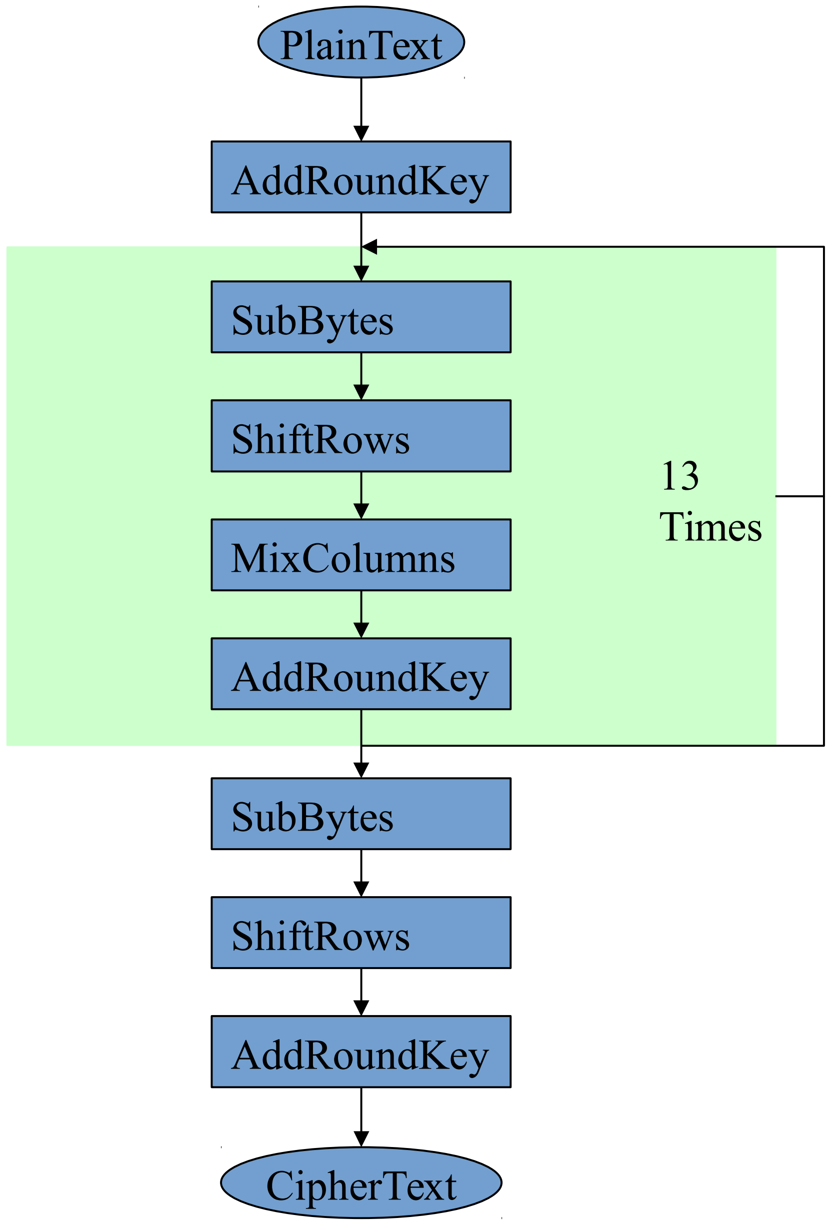
Description
- Sharing & maintaining a secret key
- No key = No encryption/decryption
- Modified ciphers = Malformed

Cost
- Encryption + Decryption time
- Expensive Materials
- Power, memory, etc. consumptions

Message Life-cycle

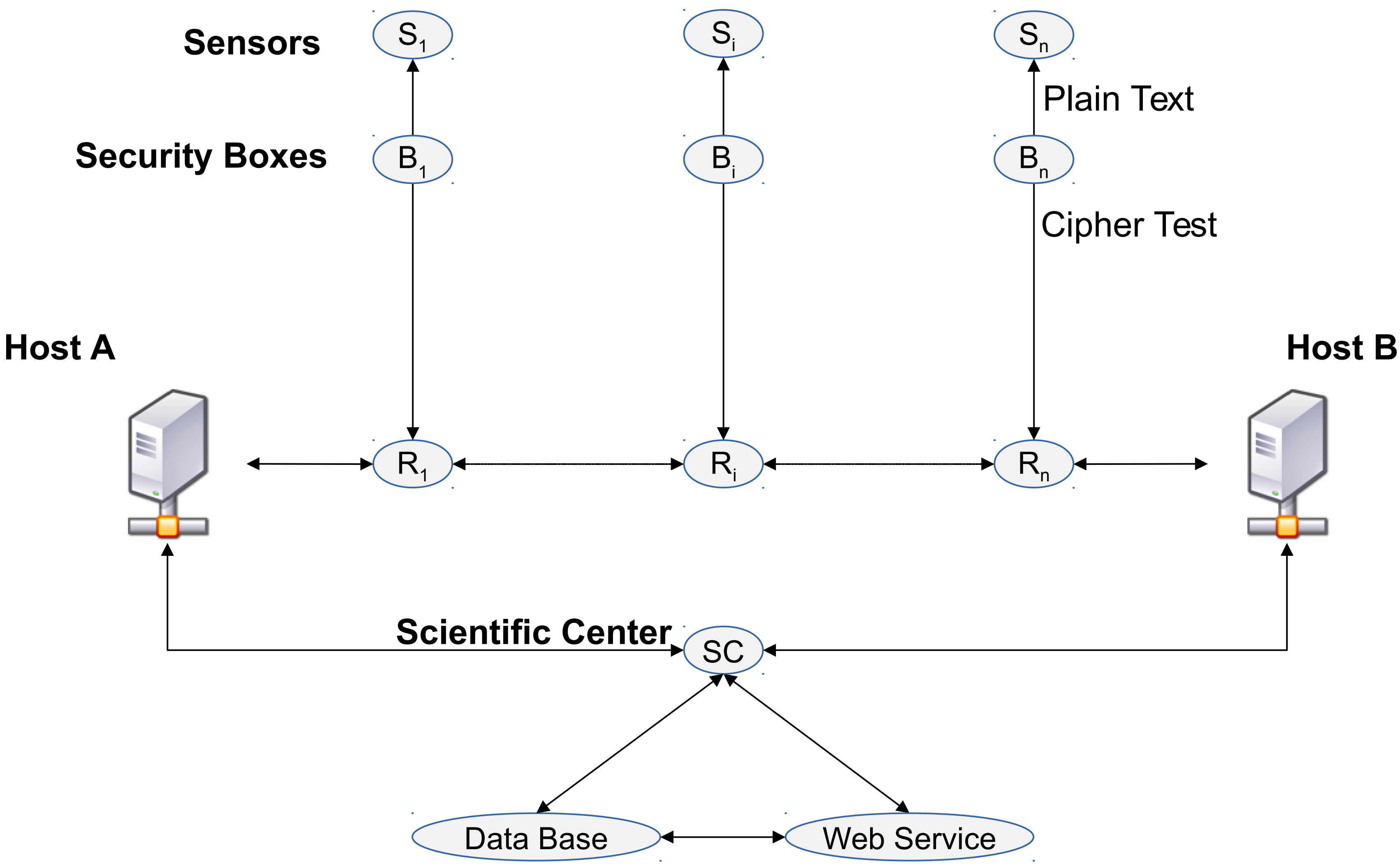
Message Created → Message Encrypted → Cipher Sent → Cipher Received → Cipher Decrypted → Message Red

AES 256



PlainText
AddRoundKey
SubBytes
ShiftRows
MixColumns
AddRoundKey
13
Times
SubBytes
ShiftRows
AddRoundKey
CipherText

Applying AES 256



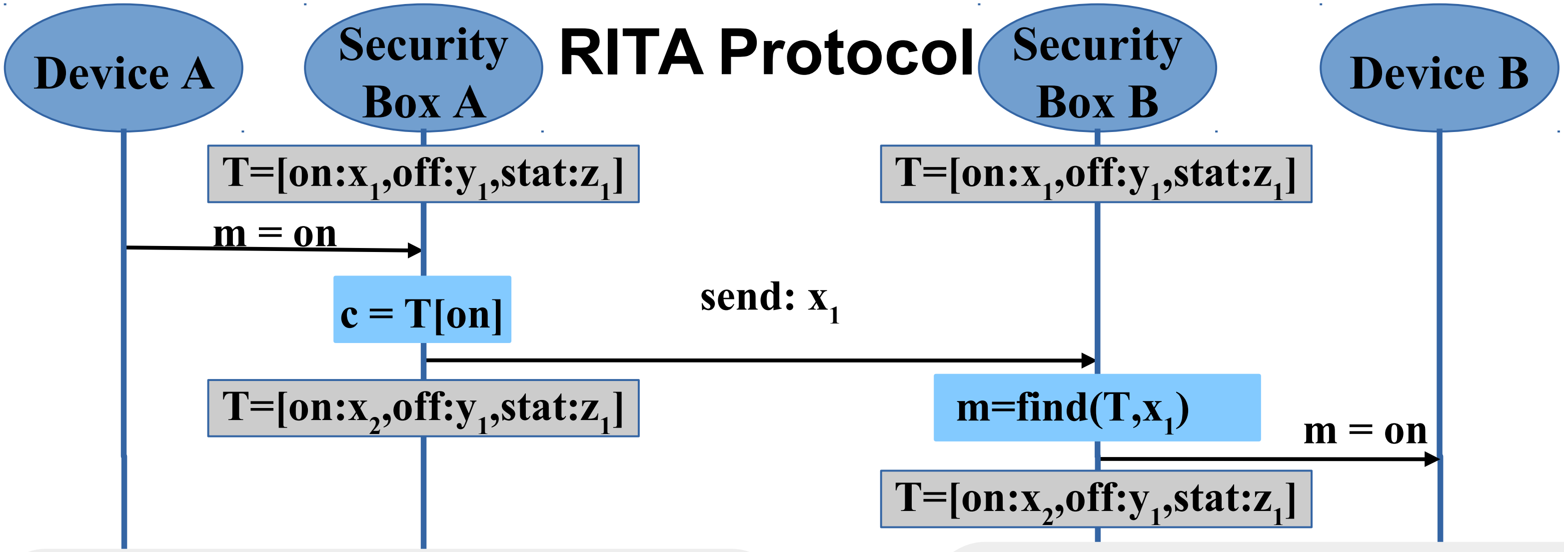
Attacks and Solutions

- **Chosen/Known plain text:**
  - **Use random padding.**
- **Replaying ciphers:**
  - **Use timestamps or session tags.**
- **Side channel analysis:**
  - **Use dynamic keys**
- **Inside job:**
  - **Use security boxes on SC.**
- **Message delay/delete:**
  - **Detect using synchronization and messages sequence.**
- **DoS:**
  - **No practical solution**

Resulting cipher:

c = (address, enc(data,pad,time-stamp))

RITA Protocol



Description

- Sharing & maintaining a secret table
- Sharing a 'secret' algorithm
- No table = No coding/decoding
- No algorithm = No table analysis
- Modified messages = Malformed

Cost

- 2 x 'index search in table'
- Table updates: After sending/receiving
- Cheap materials
- Low power consumption
- Low to moderate memory consumption

Message Life-cycle

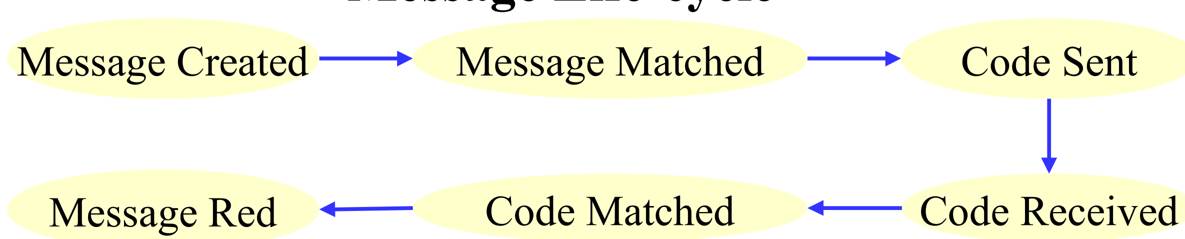
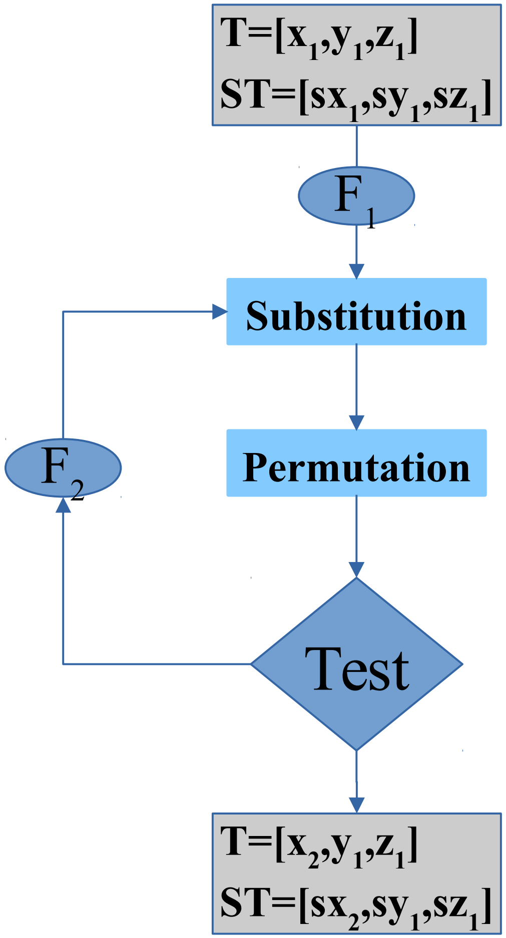


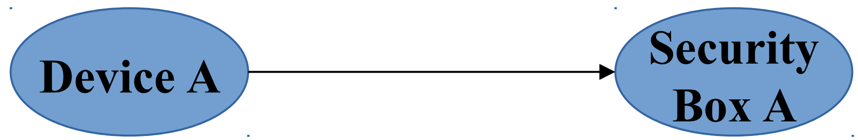
Table Update Example



Functions

F_1:	Input:	i,ST	Output:	T[i],ST[i]
F_2:	Input:	i,ST	Output:	T[i],ST[i]
Test :	Input:	i,T	Output:	ok/no

Special Cases



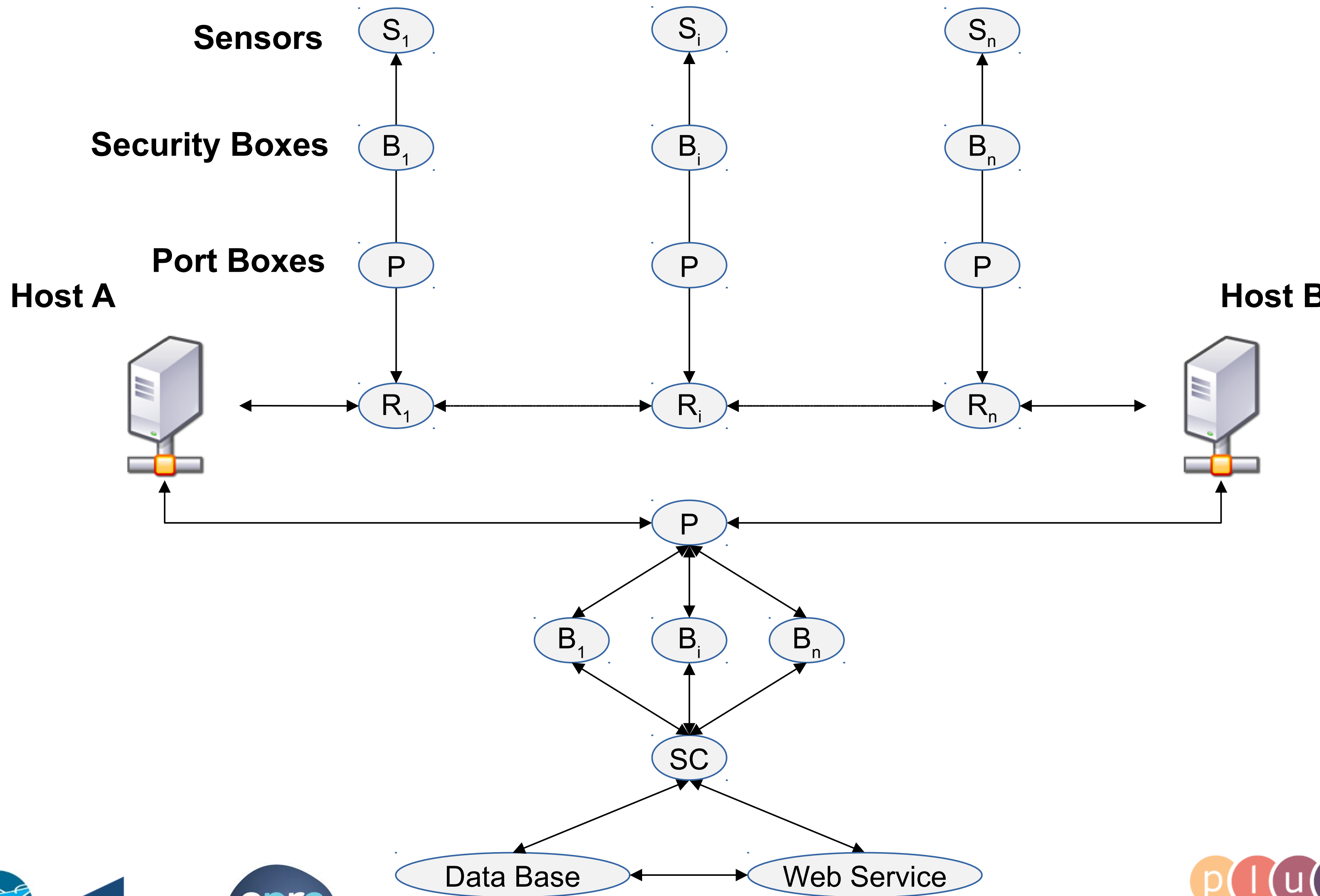
- Device A: Production frequency: 5x
- SBox A: Update frequency: 1x

Solution : Multiple SBoxes.

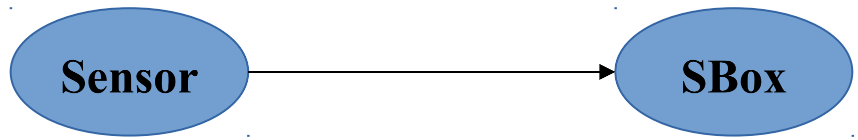
- Device A: unlimited/many possibilities
- SBox A: very limited possibilities.

Solution : Binary, base ten, etc..
+ multiple SBoxes if needed.

Applying RITA



Specifications

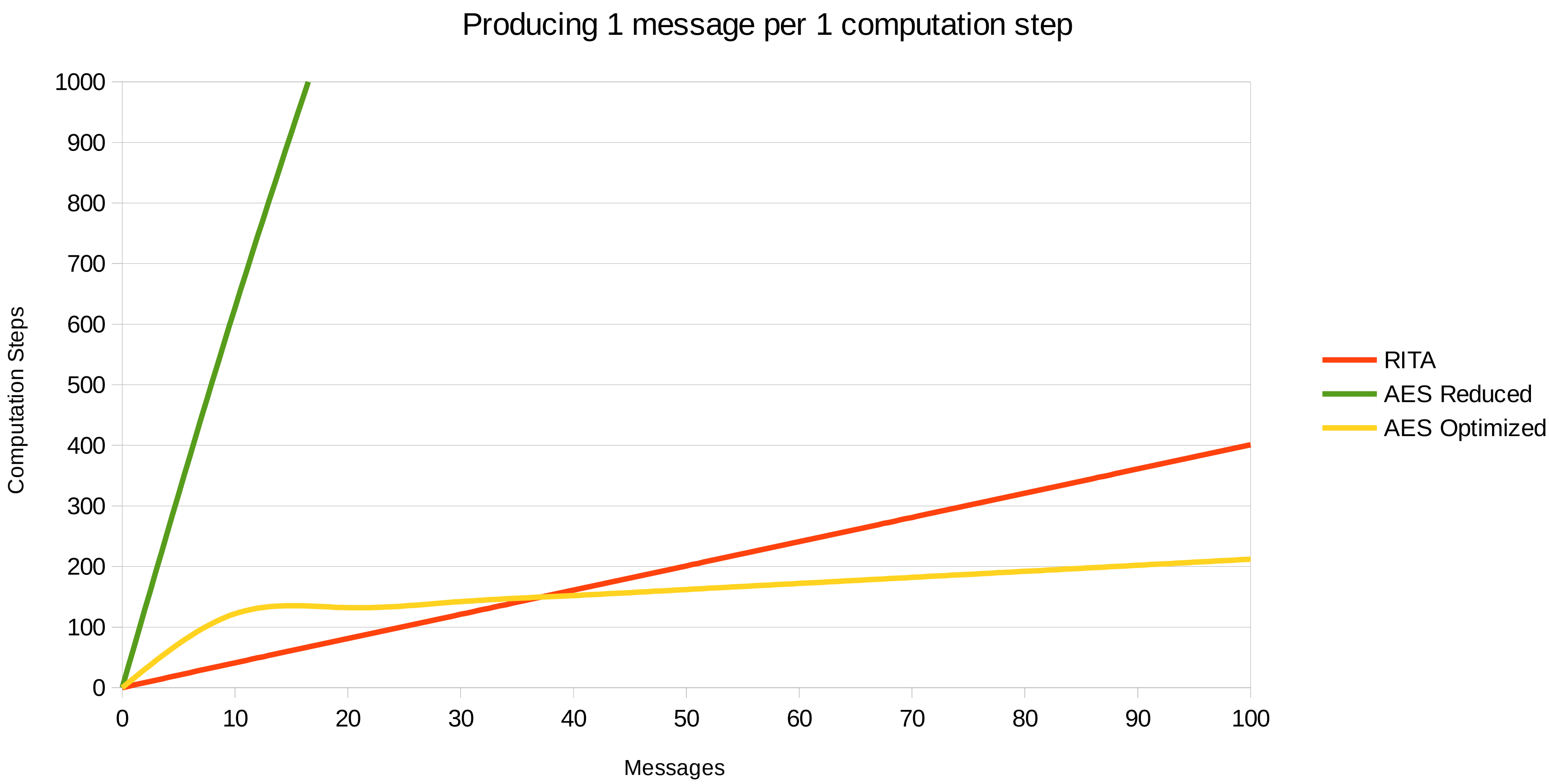


- Temperature/Pressures/Location/..
  - C = x/s, F = 1/s.
  - SBox big/numerous enough for x/s.
  - First value is divided.
- Images/Videos/.. (large data)
  - Binary.
  - Multiple SBoxes.
  - Or : Simulating multiple SBoxes.

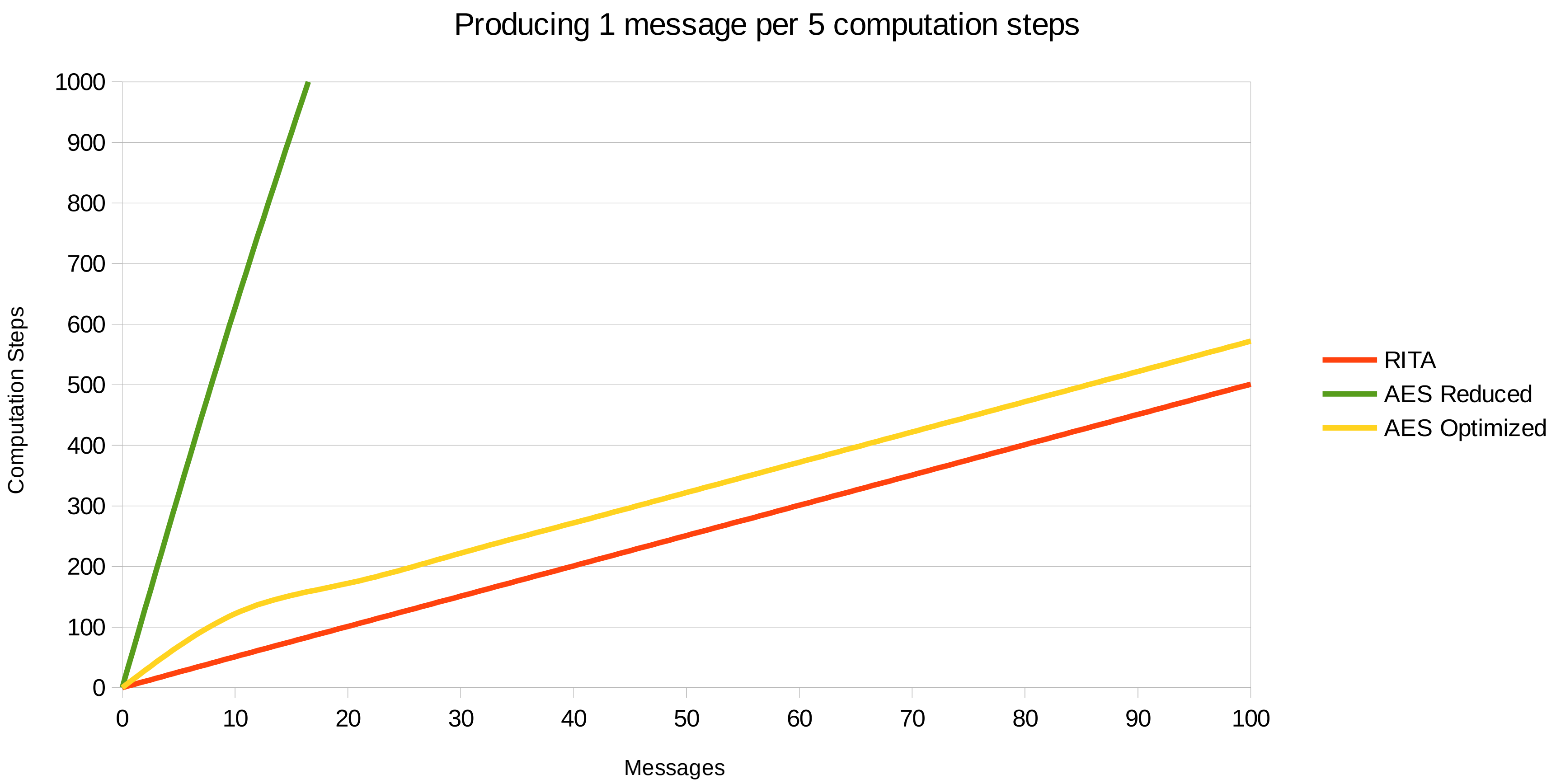
Robustness

- **Confidentiality:**
  - Messages between $SBox_i$ and his twin are meaningless to others.
- **Authenticity:**
  - Only the twin of an SBox can send readable messages.
- **Integrity:**
  - Modified messages = unreadable messages.
- **Availability:**
  - Synchronous communication guarantees detection of unavailability.
- **Interruptibility:**
  - Communication can be interrupted by hosts.
  - The order is conserved, which means that messages can be processed later.

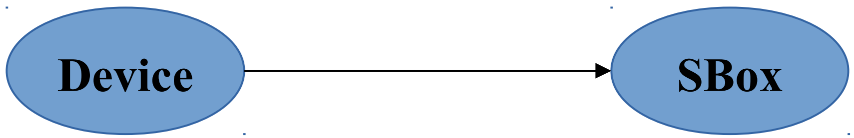
AES256 vs RITA



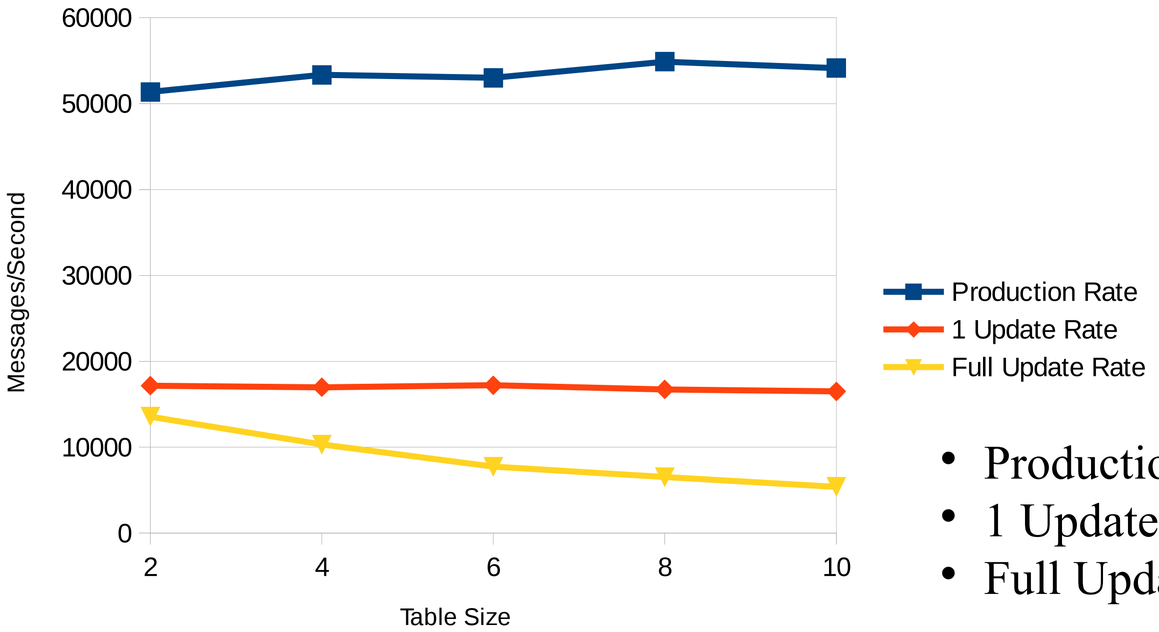
AES256 vs RITA



Simulation

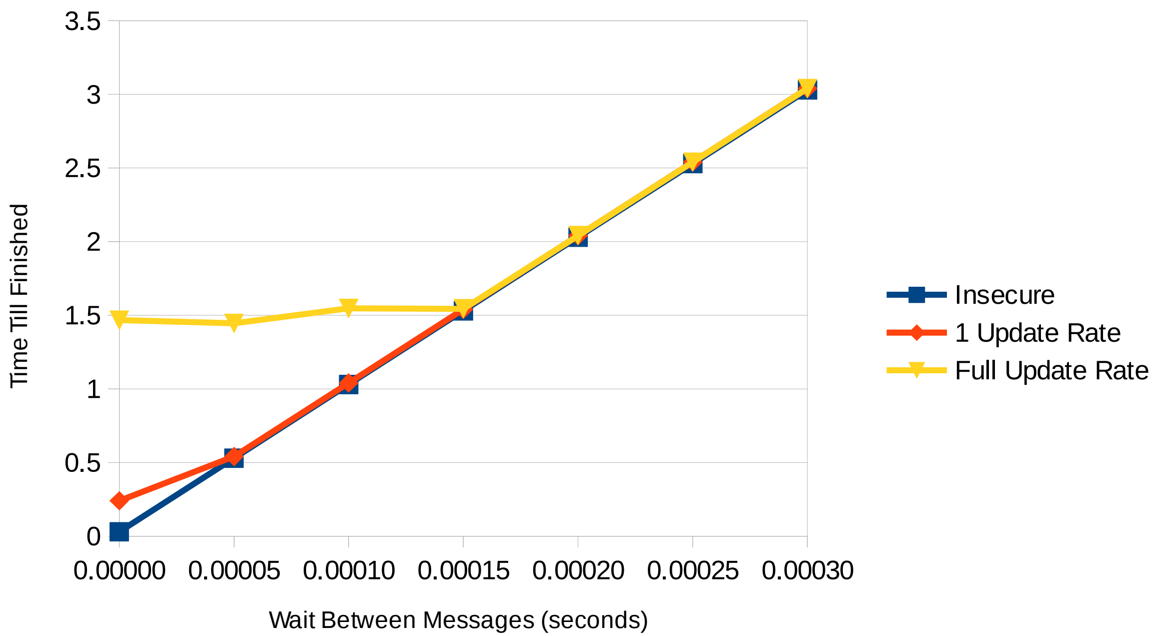


- Device
  - Creates random messages from table.
  - No waiting, full speed.
- SBox
  - Prepares coded message
  - Updates table for next message.



- Production affected by simulation noise.
- 1 Update slightly affected by table size.
- Full Update highly affected by table size.

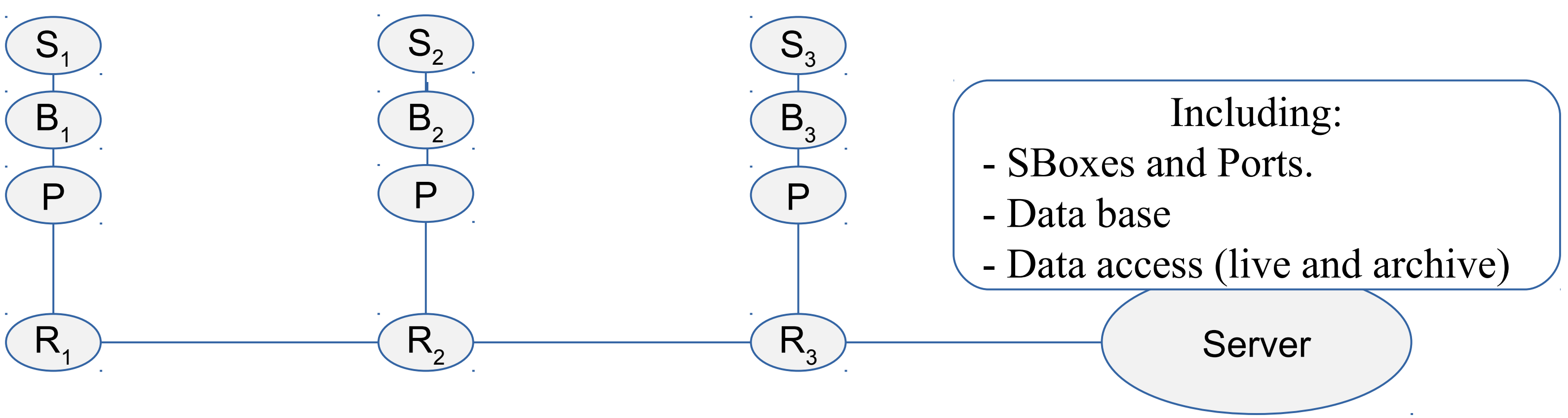
Simulation



- F > 20000 m/s : Insecure is faster then the others.
- 6666 m/s < F < 20000 m/s : 1 Update becomes instant.
- F < 6666 m/s : Full Update becomes instant.

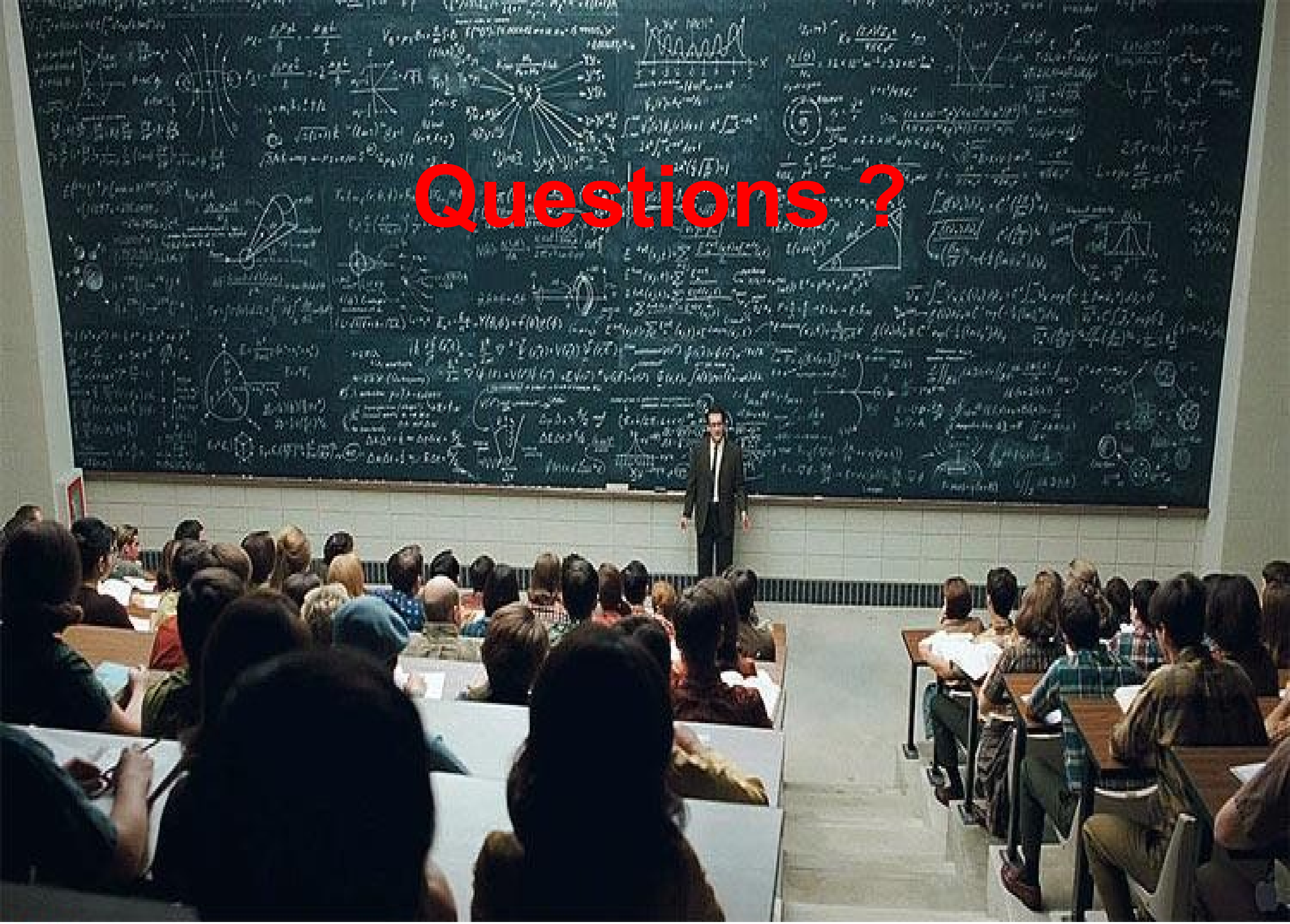
Future Work

- Improving Simulations
  - Simplifying choices and options.
  - Improving code execution and performance.
  - Dynamic behavior depending on commands.
  - Improved resend/reset/..
- Realistic scenario based on multiple simulated devices.
- Physical implementation on embedded devices.
- Robustness analysis of design and implementation.
- Actual implementation on SMART Cable System.



Conclusion

- Concept studied and improved over a year.
- Proved useful at research level.
- Simulation and application still in early stages.
- Room for improvements.
  - Security level.
  - Performance.
  - Simulation.
- ENVRI+
  - Case study with industrial participants of the JTF Smart Cable?
  - Simulation of one of the potential demonstrators?
  - Interaction with ENVRI+ community.
  - Validating the compatibility with advanced scientific data management?


Questions ?