innovations
for high
performance
microelectronics

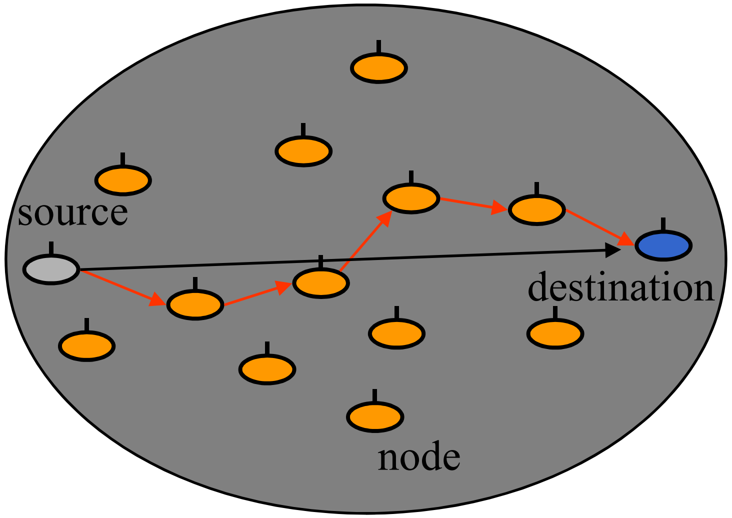
Security in Distributed Wireless Sensor Networks

Hon. Prof. Dr. Peter Langendörfer & Prof. Dr. Ing. Rolf Kraemer

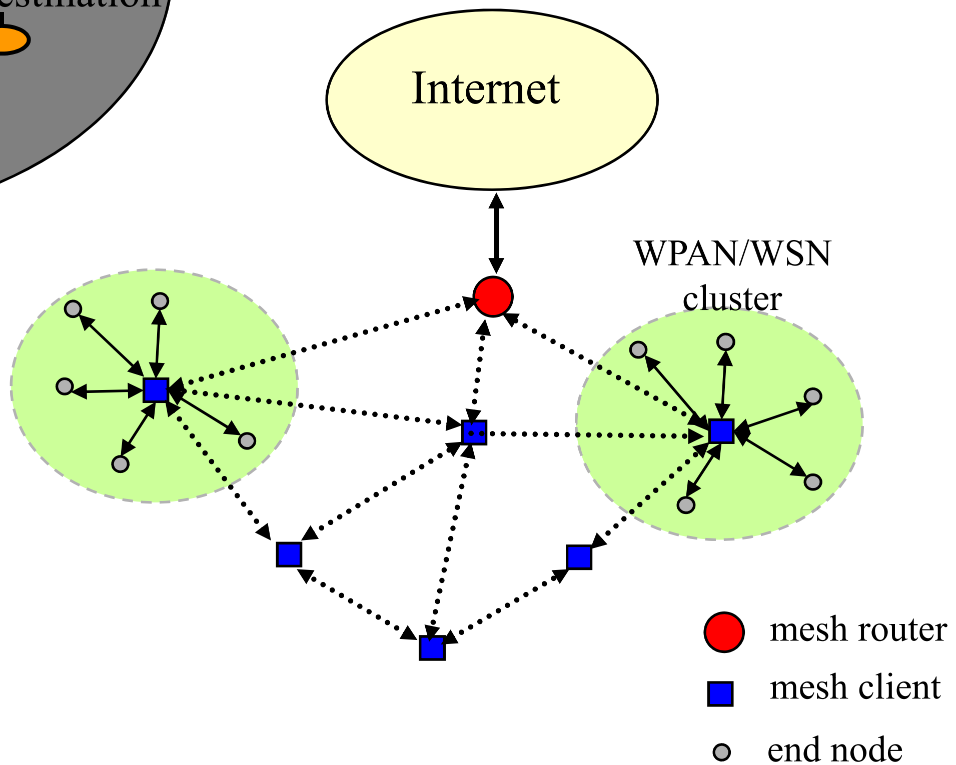
Outline

- Wireless Sensor Networks and Security
- Security Engineering
- Secure Sensor Node Architecture
- Conclusion

Wireless Sensor Networks



Multihop Network



Clustered Network

BAN or PAN Network

Security Fundamentals

- **Confidentiality**

  Information should only be revealed to authorized entities; any other entity should not be able to discover the information from eavesdropping or from read in memory

- **Data Integrity**

  The receiver of information wants to be sure that data is not modified in transit, either intentionally or be accident.

- **Accountability**

  The entity requesting a service, triggering an action, or sending a packet must be uniquely identifiable

- **Availability**

  Legitimate entities should be able to access a certain service/information and to enjoy proper operation

- **Controlled Access**

  A service or information access should only be granted to authorized entities

Security features

- **Authentication (data and source authentication (data integrity))/non repudiation**
  - Does not help against insider attacks
  - Intrusion detection (identification of compromised nodes)

- **Secrecy**
  - Use of appropriate cipher means

- **Service Integrity**
  - Plausibility check of sensor readings

- **Availability**
  - Denial of service may cause serious harm
  - Graceful degradation needed

Basic Threads

- **Eavesdropping**

  Listening to a communication to get unauthorized information
- **Masquerading**

  Pretending to have another entity identifier
- **Authorization Violation**

  Using services without being allowed to use them
- **Provoking loss or modification of information**
- **Forgery**

  Creating new or false information
- **Repudiation**

  Denial that one participated in or was the origin of communication
- **Sabotage**

Classification of Threats

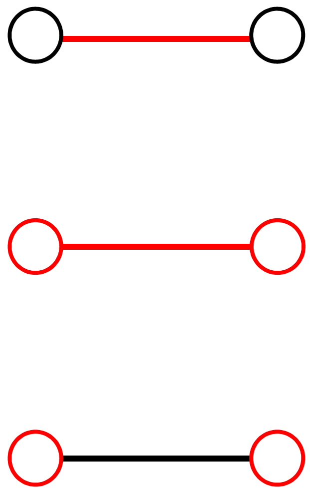
- **Outsider attacks**
  - Eavesdropping
  - Jamming
  - Alter packets
  - Destroying nodes
- **Insider attacks (Compromised sensor nodes; laptops)**
  - Authorized participant
  - Steal secrets or disrupt normal functioning
- **Base station/cluster head as point of trust?**
  - Powerful device;
  - Tamperproof HW;
  - Scalability may become a serious problem
  - Battery power of nodes around the base station

Security Threat Analysis for sensor nodes

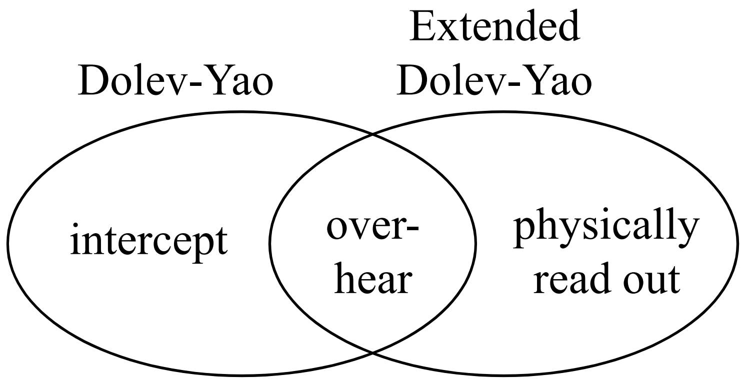
Dolev-Yao (known) :

Extended Dolev-Yao:
(WSN relevant)

Paradox
State of the art:



Threat-Model with up to 5 years delay



Options for security improvement:

- **Tamper-resistant nodes (⇒ too expensive)**
- **“Probabilistic” security (⇒ attacker receives only limited gain)**

Physical Attacks & Security

- **Device classes** (FIPS 140-02 level1-level4)
  unprotected (L1 u. L2)
  partly protected (L3)
  tamper resistant (L4)

- **Attacker**
  clever outsider (<5000 EUR)
  “insufficient knowledge of the system”
  knowledgeable insider (>5000 EUR)
  “substantial technical education/experience”
  funded organisation (several 100 KEUR)
  “teams of specialists”

WSN Security Tomography

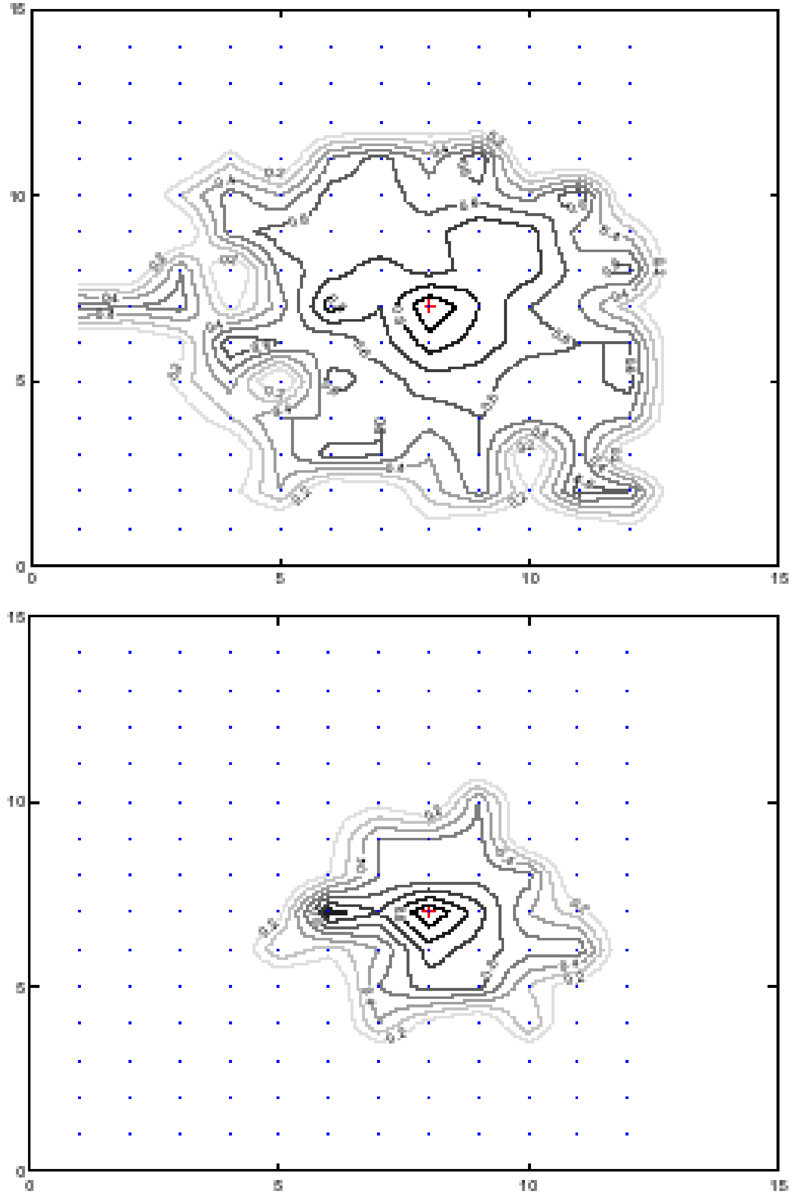
Attacks	Layer	Layer	Attacks
	Apps	Transport	send erroneous data, inje wrong control packets, se changed data, duplicate data, eavesdrop
sensed data injection, access sensed data, service disruption, etc.	Middleware	Network	routing loop, black hole gr holes, wormhole, injecting network partitioning, etc
exploiting backdoors, buffer overflows, remote node programming, direct programming, denial of service attacks	OS	MAC	eavesdropping, man-in-th middle, replay, spoofing
	Sensor / HW	RF	complete jamming, selective/partly jamming, eavesdropping, replay attacks

Sensor: tamper with sensor, falsified sensor reading

HW: invasive attacks, semi-invasive attacks, non-invasive attacks

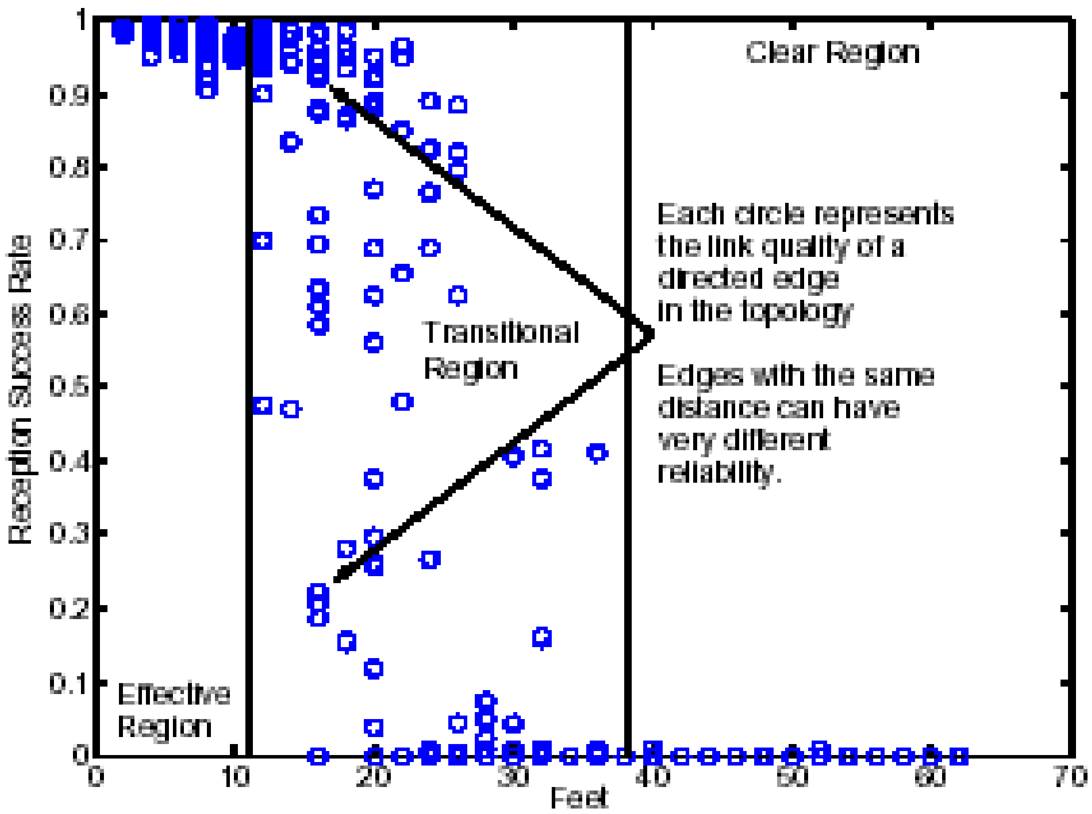
Real Life Connectivity

- Figures show WSN deployed on a flat parking lot
- Expected: simple, circular shape of "region of communication" – not realistic
- Instead:
  - Correlation between distance and loss rate is weak; iso-loss-lines are not circular but irregular
  - Asymmetric links are relatively frequent (up to 15%)
  - Significant short-term PER variations even for stationary nodes


(a) (b)

Three regions of communication

- *Effective region*: **PER consistently < 10%**
- *Transitional region:* **anything in between, with large variation for nodes at same distance**
- *Poor region*: **PER well beyond 90%**



Open issues: Detection of compromised nodes

- Secure routing protocols
- Secure & efficient time synchronisation
- Secure localization
- Efficient cipher means
- Secure misbehaviour detection
- Means for non security experts to design secure WSNs

Security Engineering

Security Engineering in WSN

- **Limitations:**

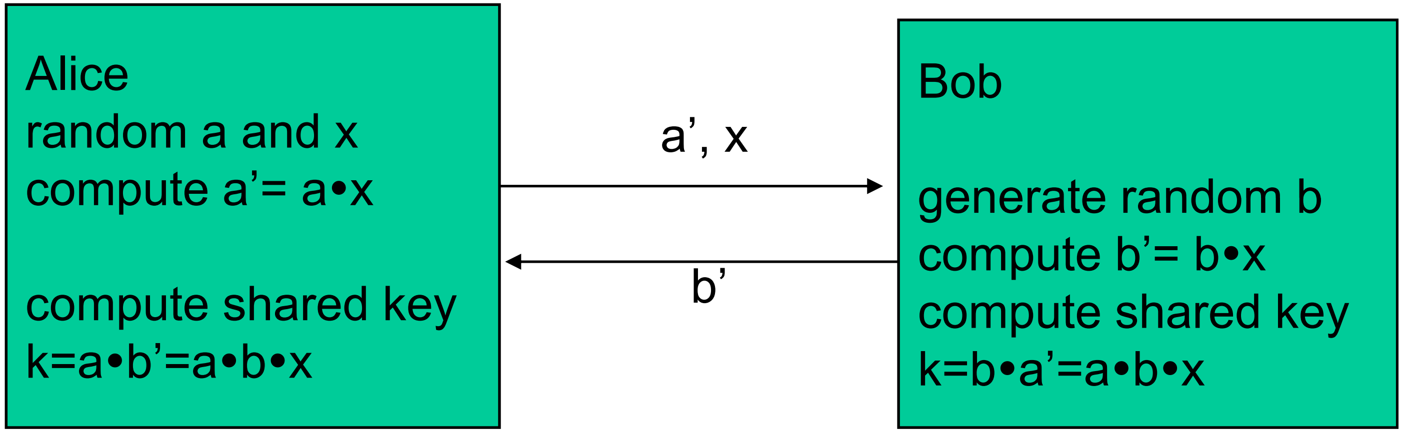
Processing power :	8 or 16 bit µC
Memory :	16 to 256 kByte
Energy resources :	typical small batteries 1000-5000 mAh
	energy harvesting
Active Time:	1-15 years
Cost :	1-100 $
Security:	open to security critical

How to distribute secret keys in networks

- **Secure channel**
  - Pre-deployment
- **Third party**
  - security authority
  - Transitivity of trust (If node A and B trust C, C can generate key for A and B)
- **Public key based key establishment**
  - Computation of session key based on a unique public/private key pair
- **Key agreement based on one way functions**
  - Diffie-Hellman

Diffie-Hellman Key Establishment

- **If we have a one-way-function:**
  - **y=a•x, it is infeasible to compute a for given x and y**
  - **a•b•x= b•a•x (commutative)**

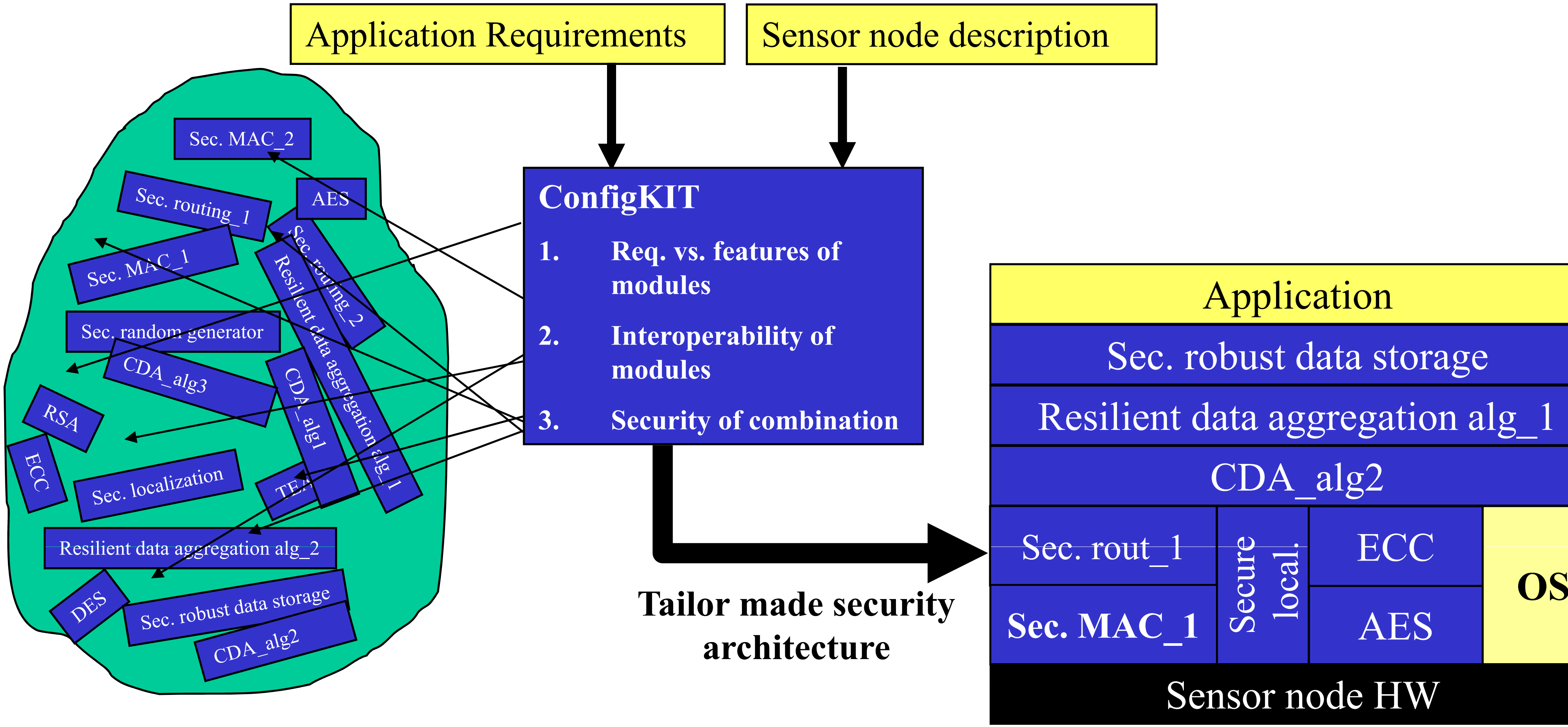


- **Advantages:**
  - **Simple protocol**
  - **Key agreement of peers without prior knowledge**
- **Problems:**
  - **One-way-function (Elliptic curve cryptography, discrete logarithm) is computationally expensive**
  - **Authentication between Alice and Bob is not supported**

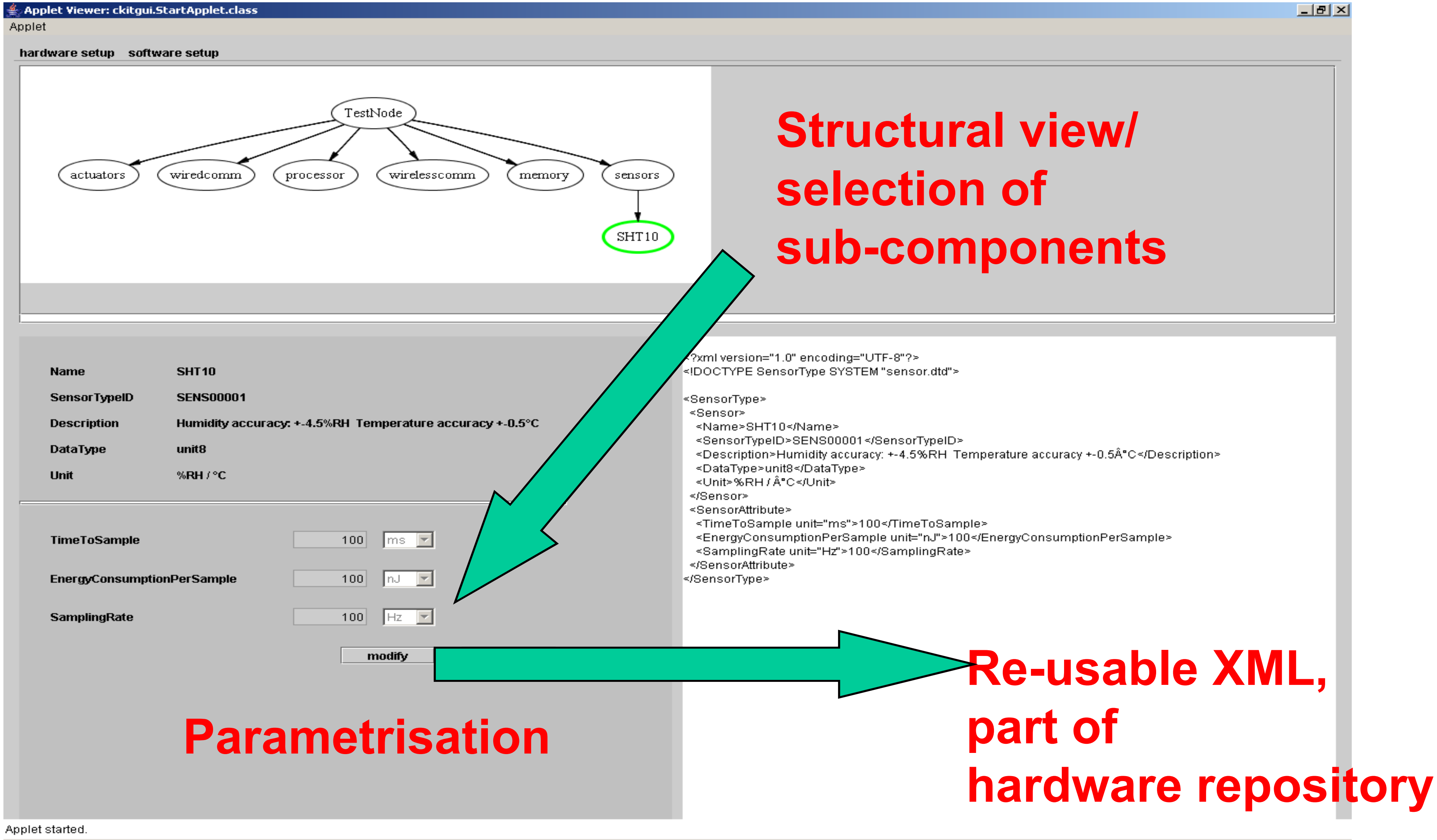
Authentication: How to prove that Alice is Alice

- **By Third Party**
  - Security Authority
  - Transitivity of trust
- **By Secret keys**
  - Alice and Bob share a secret key
- **By Inverted hash key chains (e.g. TESLA)**
  - If H(x) is a not-invertible hash function
  - Authentication with tuple $(x_n, H(x_{n+1}))$; trust anchor $H(X_n)$
  - x_n authenticates the one who sent $H(x_n)$ earlier
  - Problem:
    - lot of storage (for each communication previous hash keys)
    - initial trust (how can I authenticate the first message)
- **Signed certificates**
  - →needs public key cryptography
  - →Offline certification
  - Problem:
    - computational expensive

Combining Security & Embedded Systems Design

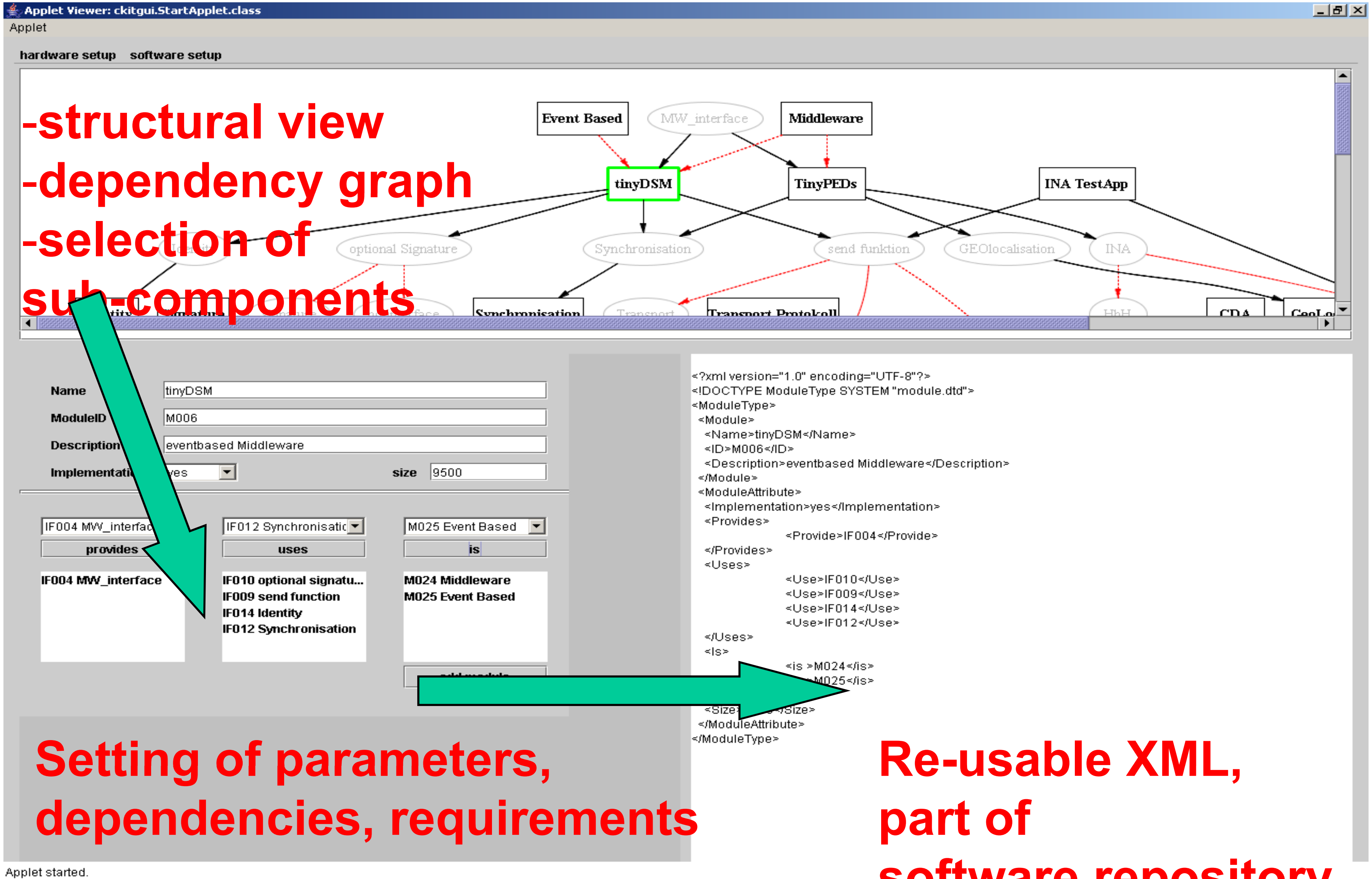


Setup of Hardware Repository



Setup of Software Repository

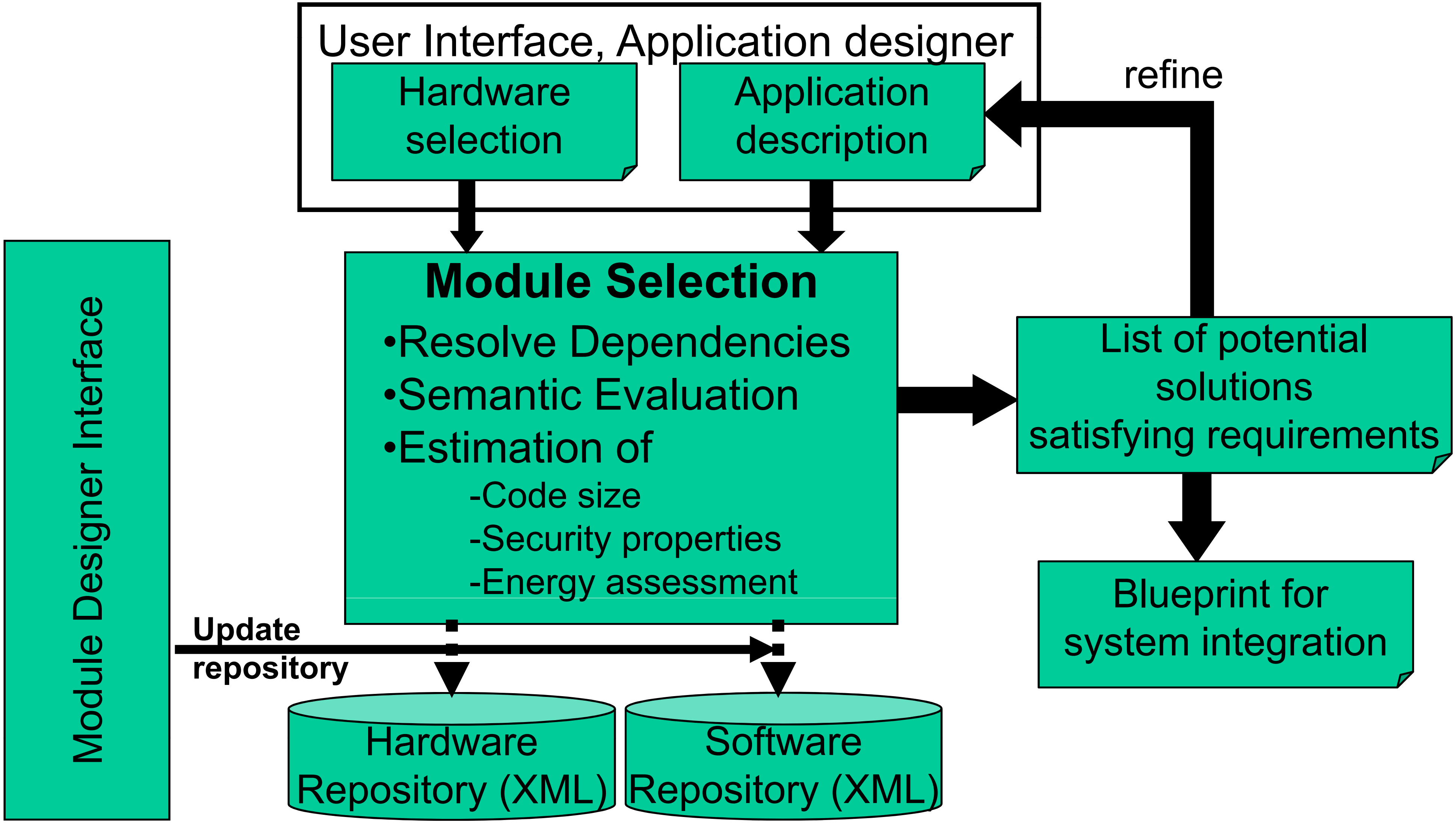
- -structural view
- -dependency graph
- -selection of sub-components



Setting of parameters, dependencies, requirements

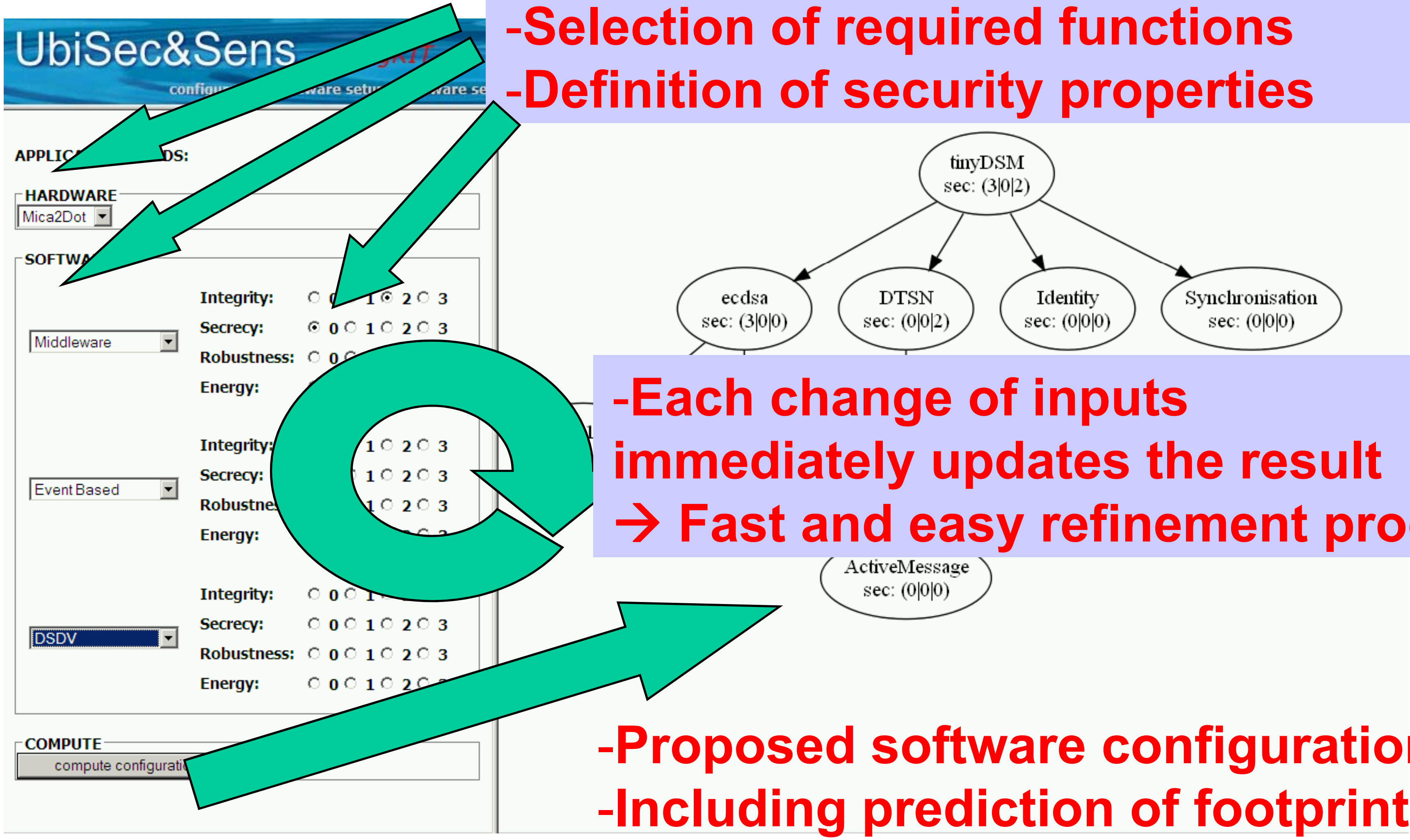
Re-usable XML, part of software repository

configKIT-approach



configKIT for Application Designers

- -Selection of hardware
- -Selection of required functions
- -Definition of security properties

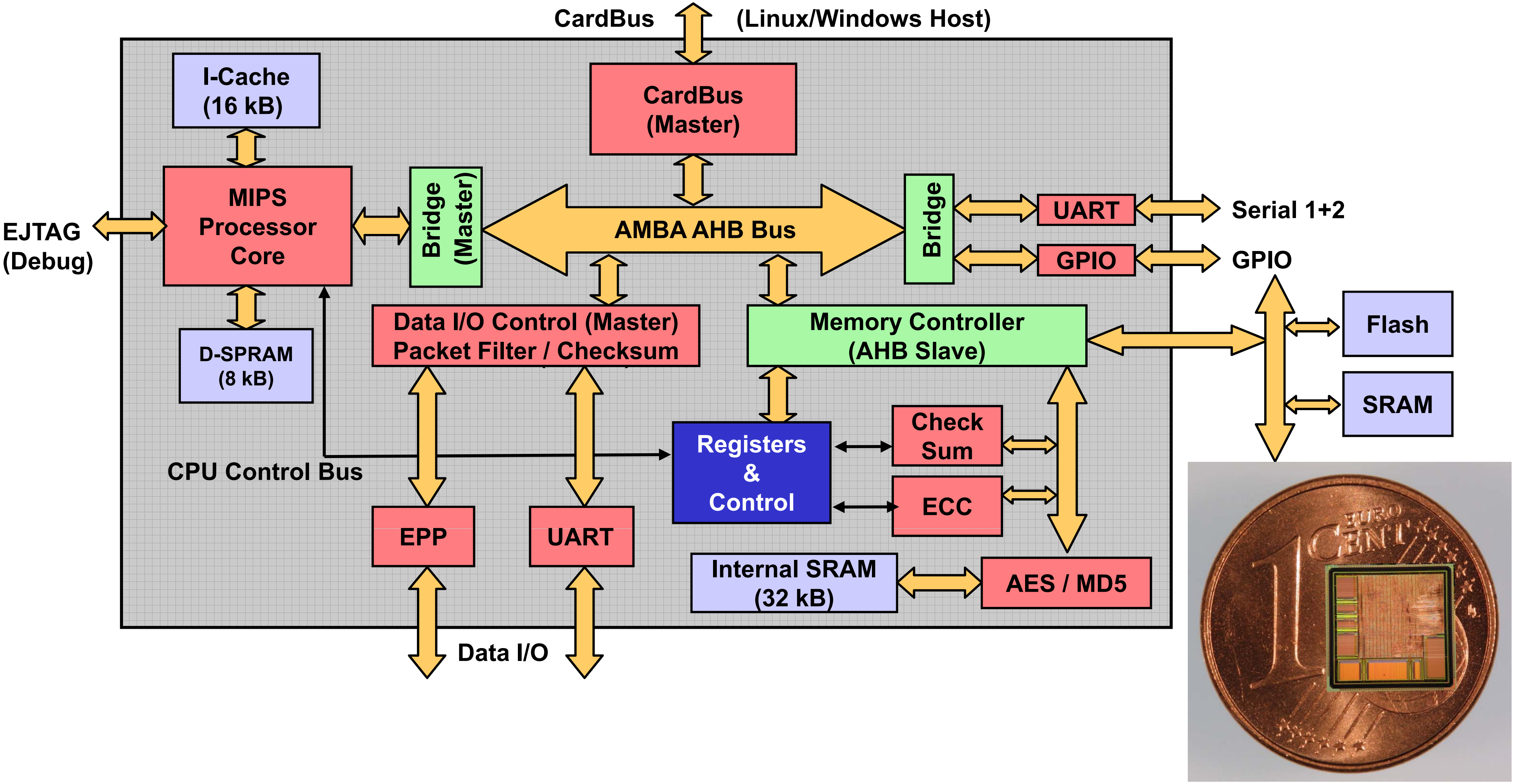


- -Each change of inputs immediately updates the result
- → Fast and easy refinement process

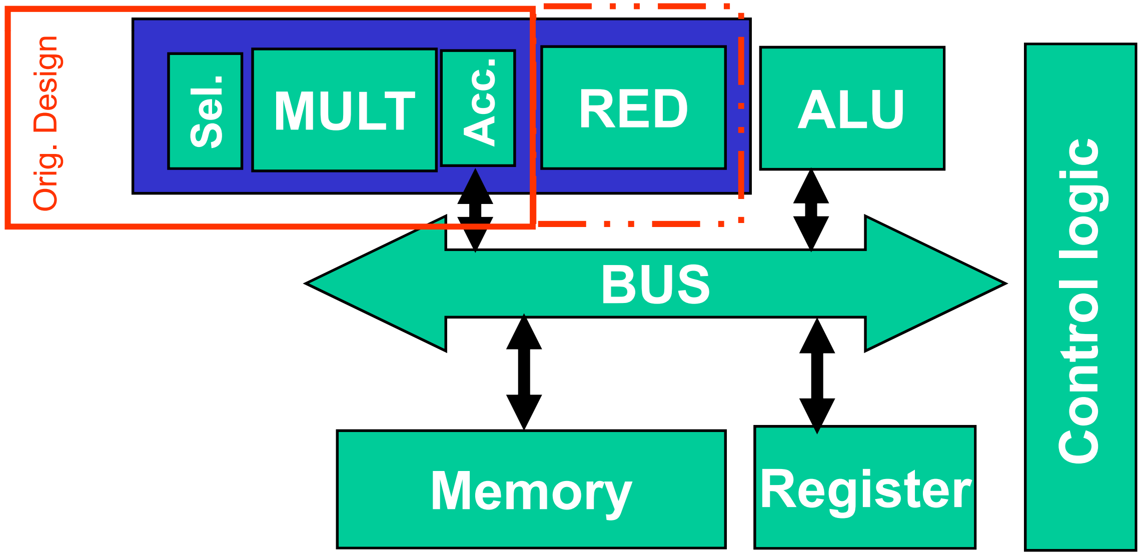
- -Proposed software configuration
- -Including prediction of footprint

Secure Sensor Node Architecture

Secure Sensor Node



ECC Processor B233: Optimized Version



Design :

- Modular Architecture
- Reduction done on partial results
- Regular Structure

Area consumption: optimized vs. original ECC Processor Version

Partial Multiplier	Length of Operand [bits]	Poly. Mult. Area [mm²] optimized	Poly. Mult. area [mm²] original Version
2 segments	*128*	1.17	2.18
4 segments	*64*	0.62	1.51
8 segments	*32*	0.44	1.67

Competitive Position: ECC

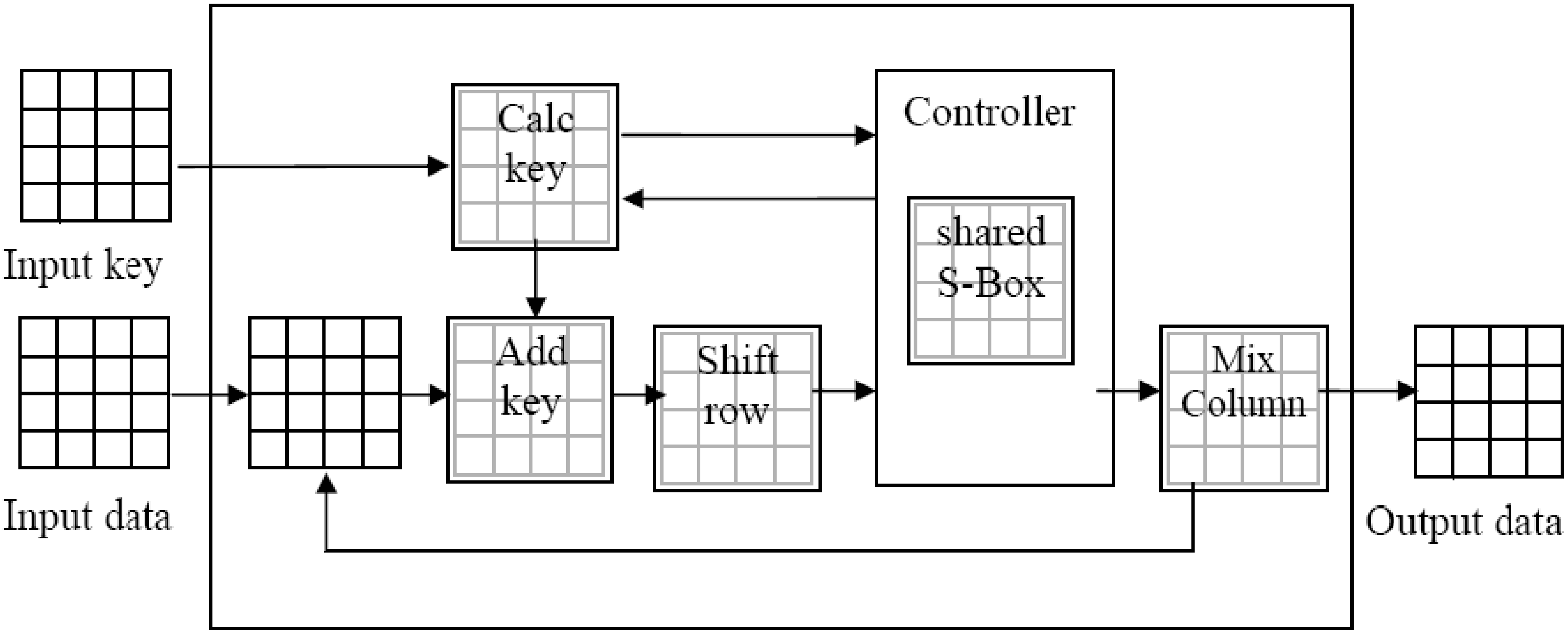
Company	Size KGates	Energy mJ	Time/Op ms	Technology used
Elliptic Semi: B-233	71	0.14	6.68	0.13µm
IHP B-233	72-42	0.02-0.04	0.08-0.35	0.25µm
IBM B-163+GF(p)	117	-	0.19	0.13µm
IHP B-163	47	0.01	0.06	0.25µm

Advantages of IHP:

- **Minimal area consumption**
- **Iterative Karatsuba approach (patent filed)**
- **Flexible ECC Designs (patent filed)**

AES

1. **Add key operation**: the incoming/outgoing data is "XORed" with the current round key
2. **SBOX**: The S-Box maps an 8-bit-input into an 8-bit-output.(result depends on the direction)
3. **Shift Row**: The shift row operation is performing a cyclic shift within a single row.
4. **Mix Column**: In the mix column operation each column is multiplied with a given polynomial



Competitive Position: AES

Company	Size Gates	Clock cycles per 128 Bit	Clock frequency	Throughput
Elliptic Semi: AES	8.000 +1.400 bit Memory	379	100 MHz	33,7 Mbit/s
IHP AES	8.450	70	66 MHz	108MBit/s
IAIK Graz	8.930	64	64 MHz	128MBit/s

Advantages of IHP:

- **Integration with ECC**
- **Integration with protocols such as TCP**
- **Results equivalent to those of the Inventor of AES (Rijmen TU Graz)**

Conclusions

Conclusions

- Security in distributed systems is still a hot issue to solve
- Several approaches have been followed and have successfully been applied to several problem areas
- Distributed wireless sensor-networks are a special class of distributed systems that do not allow rigorous means to achieve security
- We have used a combined HW/SW approach to be able to make use of high grade encryption mechanisms like AES or ECC
- We have developed a security design environment that allows to engineer security in sensor-networks as required and achievable
- The results have been demonstrated and have been patented

TANDEM: Power Switches