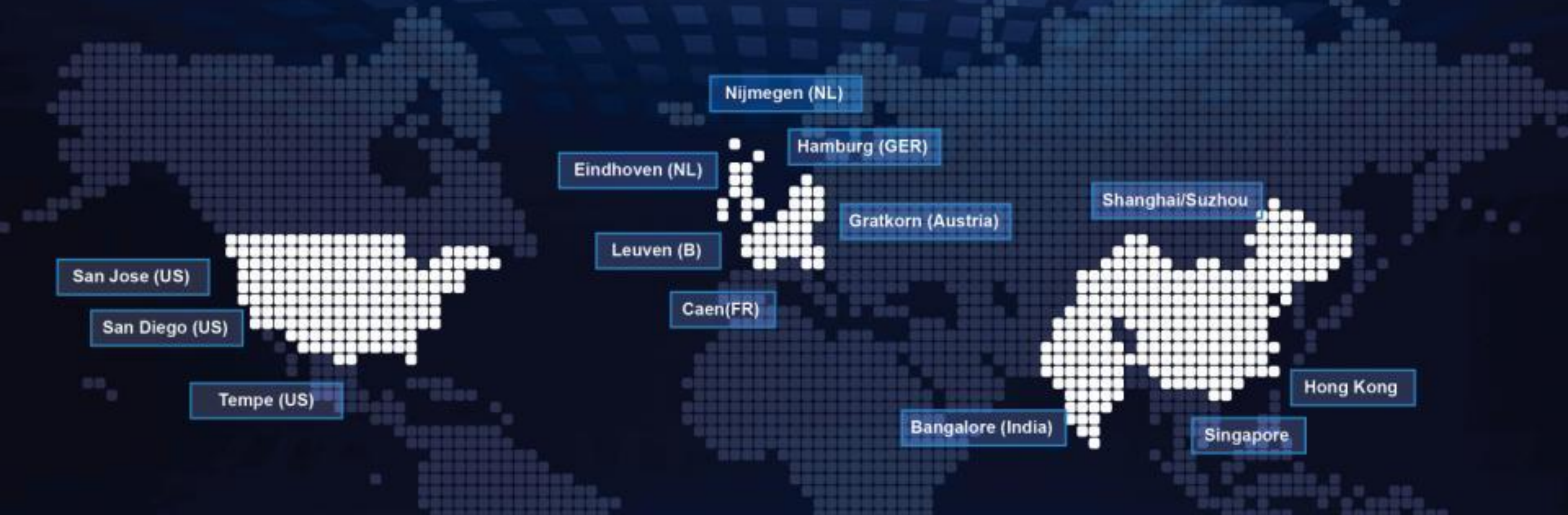
20 Years of MIFARE

From CRYPTO1 to Formal Verification

Karin Greimel & Günther Lackner
Business Unit Identification
NXP Semiconductors

NXP – a true global Player & Innovator



Distinctive Technologies:

- Full Portfolio of secure microcontrollers
- Embedded non-volatile & flash
- Power optimal RF & NFC
- Mixed signal processing

Strong Innovation Pipeline:

- over $550M / year in R&D
- down to 40nm processes
- >3,200 engineers worldwide
- >11,000 granted patents

We bring Security & Convenience

NXP is #1 with over 8B units shipped

Source: NXP

NXP is the Identification Industry’ s #1 Semiconductor Supplier

#1

eGovernment

#1

Reaching

Bank Cards

#1

Smart Mobility & Access Management Cards

#1

Tags & Authentication

#1

Smart Readers

#1

Mobile Devices

> 1,200 engineers dedicated to tamper resistant secure, high-performance solutions

Leading IP position: 700+ patent families in the Identification market

MIFARE – a success story since almost 20 years

in 1994, first MIFARE card & reader solution invented and launched by NXP engineers

>650 cities
>50 countries
adopted MIFARE solutions

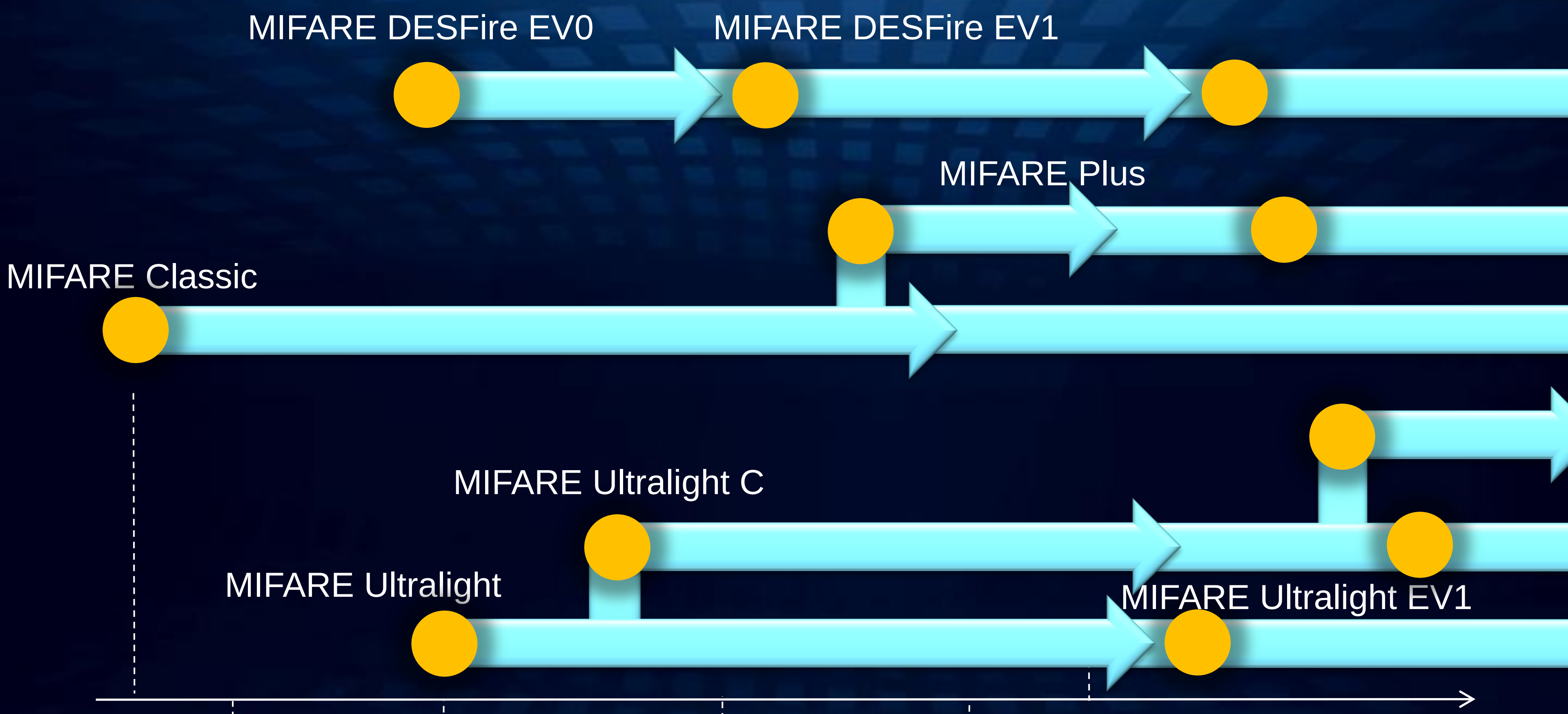
>5000m cards and tickets ICs
>50 m reader ICs
distributed in the market

>1000 partners registered on www.MIFARE.net

>40 application areas deployed across industry categories

>10 breakthrough innovations developed with first time to market

MIFARE™ – Nearly 2 decades of innovation



MIFARE DESFire EV0

MIFARE DESFire EV1

MIFARE Plus

MIFARE Classic

MIFARE Ultralight C

MIFARE Ultralight

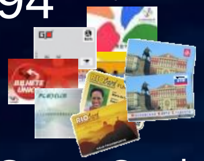
MIFARE Ultralight EV1

1994

2011

2013

2014



Smart Cards

Smart Paper Tickets

Banking Cards

Mobile Phones

MIFARE Crypto1

Evolution of security protocols

- In the 90s, proprietary cryptographic protocols have been the state-of-the-art

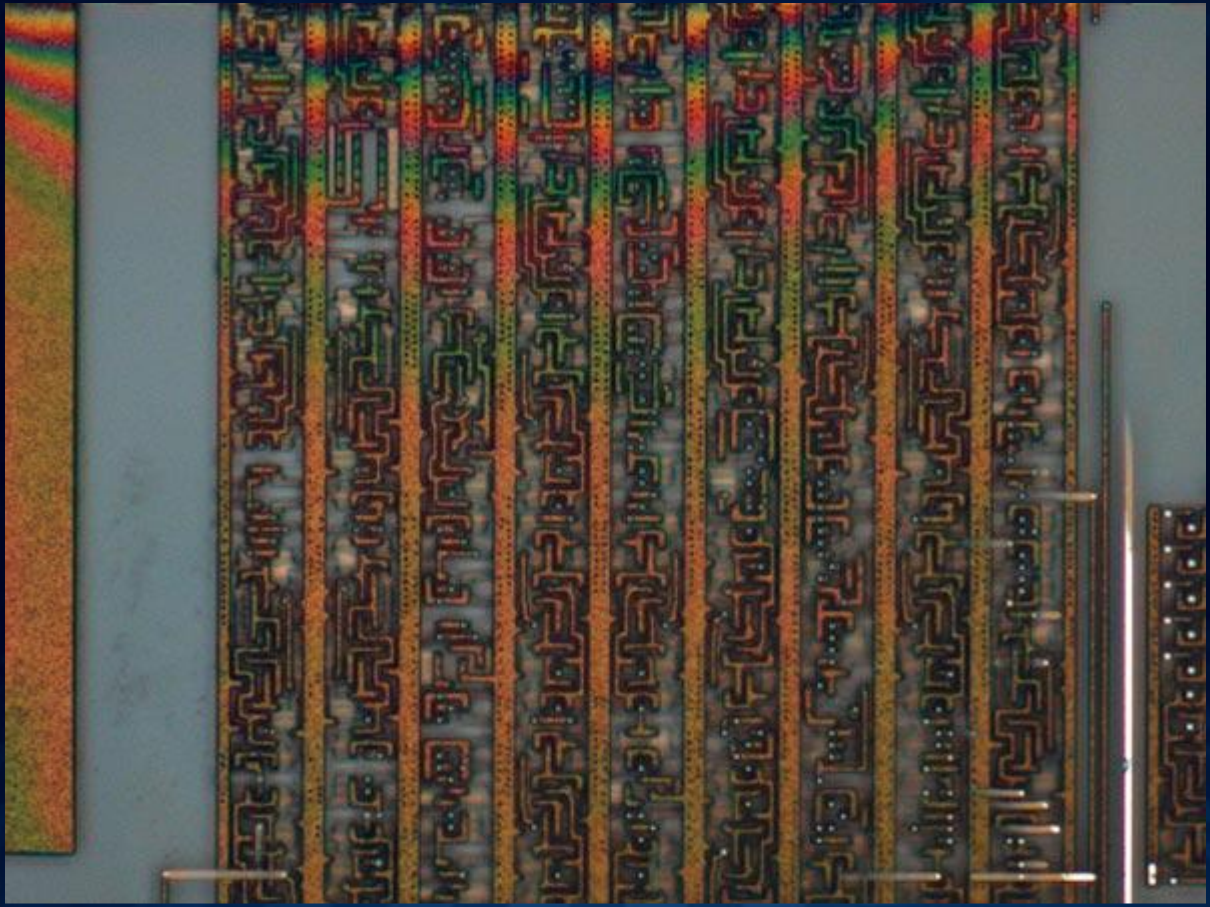
- DVD encryption CSS introduced in 1996 – hacked in 1999

- MIFARE Crypto1 developed in 1998 – hacked in 2009

- WiFi WEP introduced in 1999 – hacked in 2001

Security concept based on Obscurity

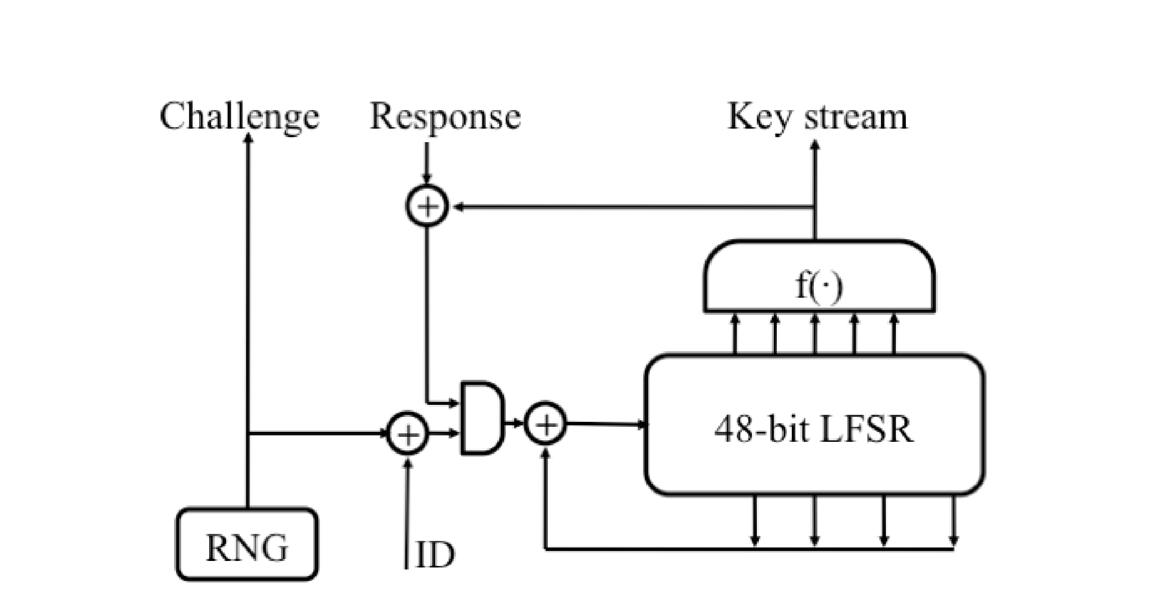
- Violation of Kerckhoff‘s priciple.



MIFARE Crypto1

- Done by Karsten Nohl in 2006

- Weak RNG
- Structural waknesses



- 16-bit Random Number
- LFSR based
- Value derived from time of read
- No non-linear element in feedback function

Modern approach to Smart Card Security

Standardized Cryptography

- State-of-the-art smart cards are based on proven cryptographic algorithms.
- Depending on the application and requirements.

3K3DES

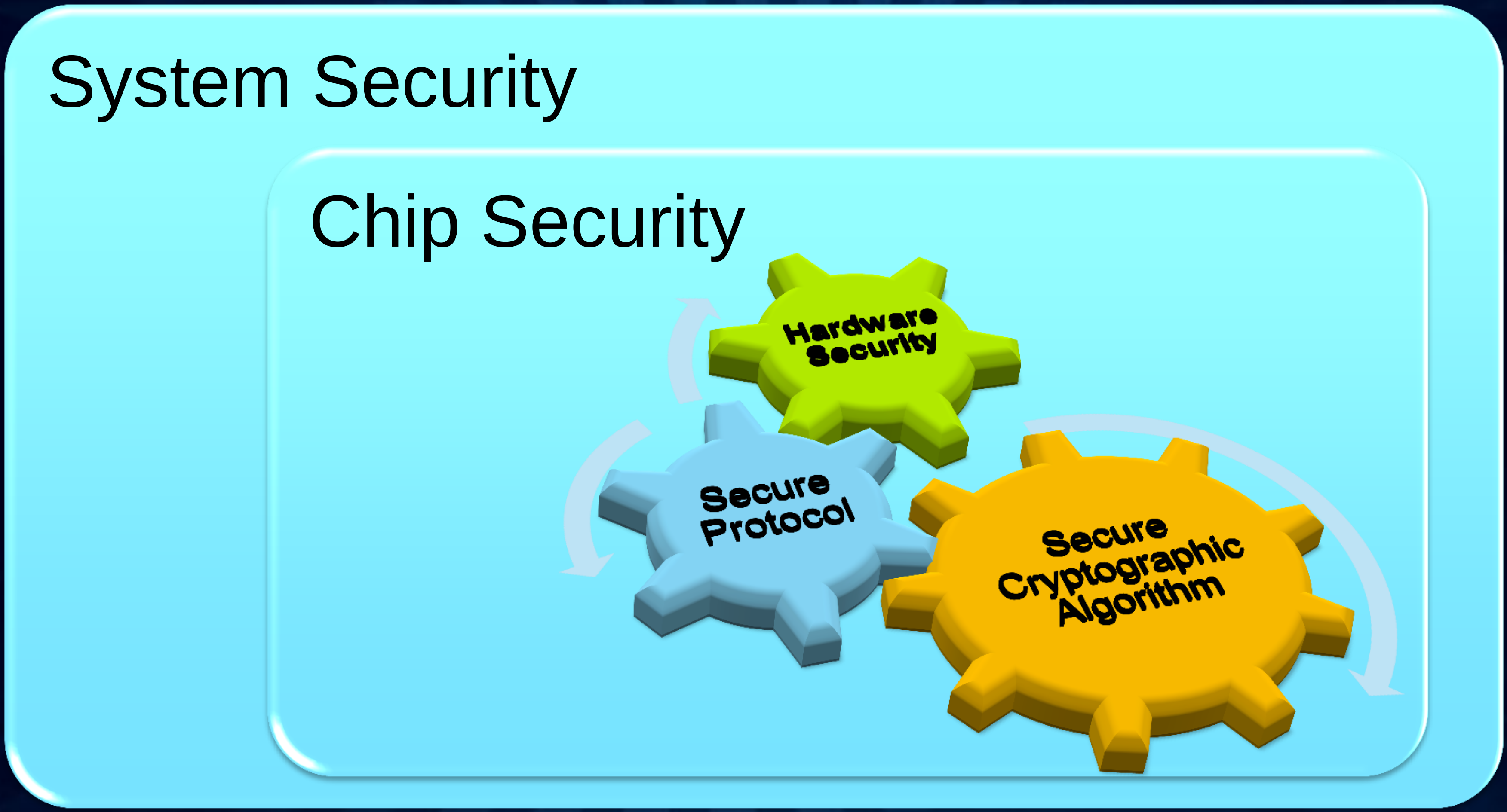
AES

ECC

RSA

SHA-256

Dimensions of security for Smart Card systems



System Security

Chip Security

Hardware Security

Secure Protocol

Secure Cryptographic Algorithm

Common Criteria

- Certification by independent 3rd party
- to allow for compareability
- The Security Target (ST) defines ***what*** to certify
- The Evaluation Assurance Level (EAL) defines ***how*** to certify
- Higher assurance level -> ‚deeper‘ investigatíon of the security
- Starting with EAL6 a formal model is required

Formal Methods

Def.: Includes all mathematical techniques to specify and verify security and/or correctness of software or hardware.

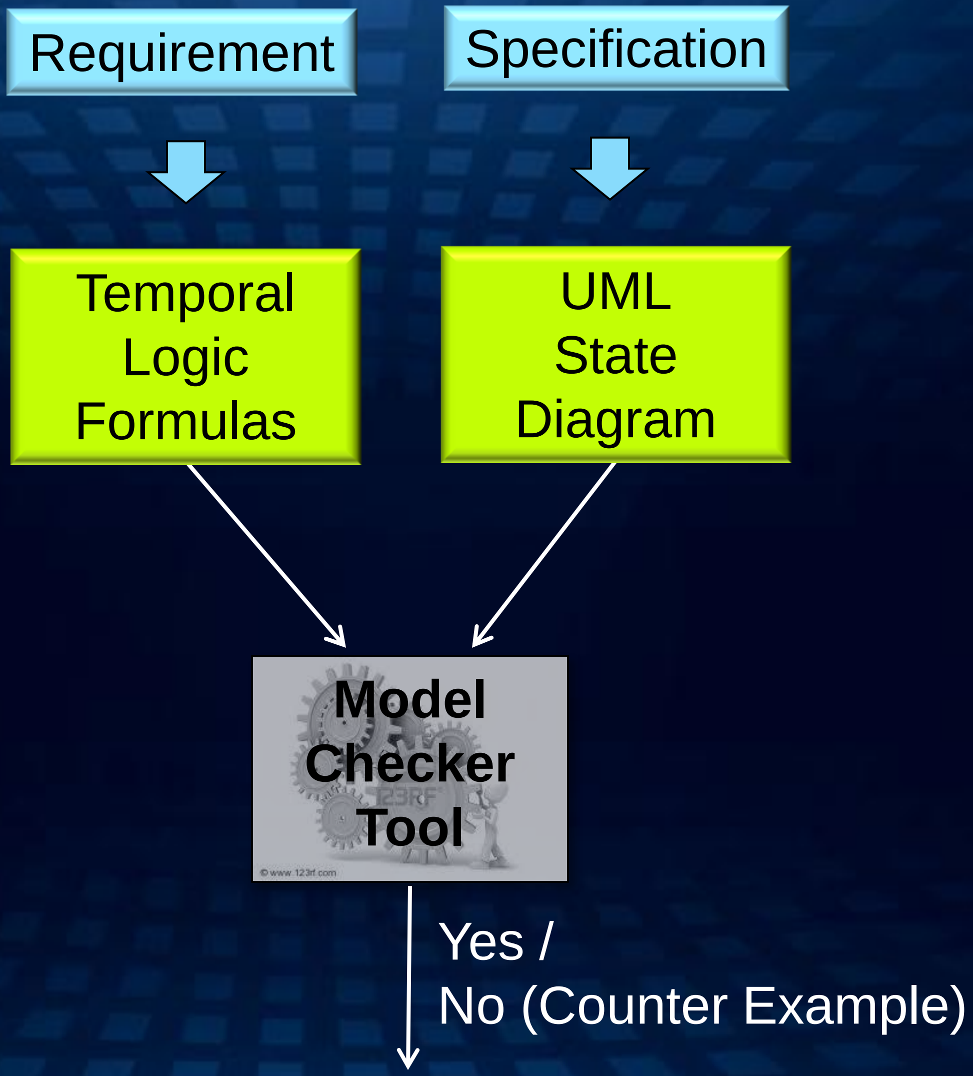
Common Criteria EAL6::

- Mathematical proof that our specification is secure/correct
- Specification meets the requirements stated in the Security Target
- Model security policies such as access control.
- Cryptographic algorithms and protocols are currently not modeled for certification

Why Formal Methods

- avoid errors at the specification phase
- generate a common understanding of the design
- improve documentation (consistency, completeness, unambiguity)
- validation – give a mathematical proof that the functional specification meets the security functional requirements

How Formal Model



Requirement

Specification

Temporal Logic Formulas

UML State Diagram

Model Checker Tool

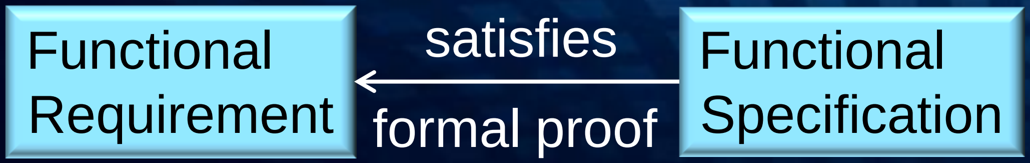
Yes / No (Counter Example)

Simplified Example – Access Control Policy

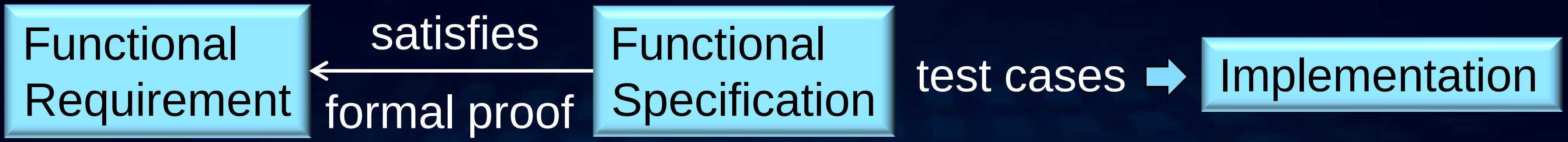
- 2 Features
- A public transport company can create/delete an application on the card (has to be authenticated with KEY = 0).
- A customer can incremented and decremented the value stored in the application (has to be authenticated with KEY = 1).

- Modeled with COSIDE (Tool by Fraunhofer)

Future Work



What about the Implementation?
We propose to automatically generate test cases from the functional specification for the implementation.



Summary

- We formally prove that the **functional specification** (UML state diagram) satisfies the **security policies** (temporal logic formula).
- Using an input language that is understood by engineers, the model helps to
  - avoid errors at the specification phase
  - generate a common understanding of the specification
  - improve documentation (consistency, completeness, unambiguity)
- Ensure high quality and security of our new products.
- Continue our success story