MobilePass

Mobile Border Control
Requirements, Challenges and potential Improvements

D.I. Bernhard Strobl
Department Safety and Security
AIT – Austrian Institute of Technology

Overview

- MobilePass Project Overview
  - Consortium
  - Objectives
- Device ergonomics and derived image processing challenges
  - The optimal device ?
  - User Interface
- Social and Ethical Considerations -> (See Talk Irma van der Ploeg)
- Three Components Solution
  - Document Reader
  - Face-, Fingerprint- Capture and Display device
  - Workflow processing system
- Fingerprints Capturing Process -> FhG (see Talk Eduardo Monari)
- Face Capturing Process -> Videmo (see Talk Keni Bernardin)
- Security Issues
  - Network & Communication Issues
  - Device
- How Increase processing power
  - Multicore vs. Ghz vs. FPGA and High Level Synthesis of C-Code (HLS)

MobilePass

A secure, modular and distributed mobile border control solution for European land border crossing points

Proposal	MobilePass - 608016
Funding	Security Call, 7th Framework Programme
Topic	SEC-2012.3.2-3: Mobile Equipment at land border crossing points
Type	CP – Capability Project
Duration	2.5 Years
Budget	~ 4.2 M€
	Develop new technologies needed in mobile scenarios and embed them in the actual border crossing workflow. Bring together system- and component producers, research institutions and governmental authorities. The entire innovation process, from development to integration, will continuously be evaluated by border guard authorities.
Coordinator	MobilePassCoordinator@ait.ac.at; +43 (0) 664 815 78 42

Why MobilePass ?

Where stationary systems can’t be used

- Facial, Fingerprint Capture necessary
- Document Security Features check necessary
- Cars, busses, trains
- Control in the outback, manhunt, Interpol
- Additional mobile systems at airports

MobilePass

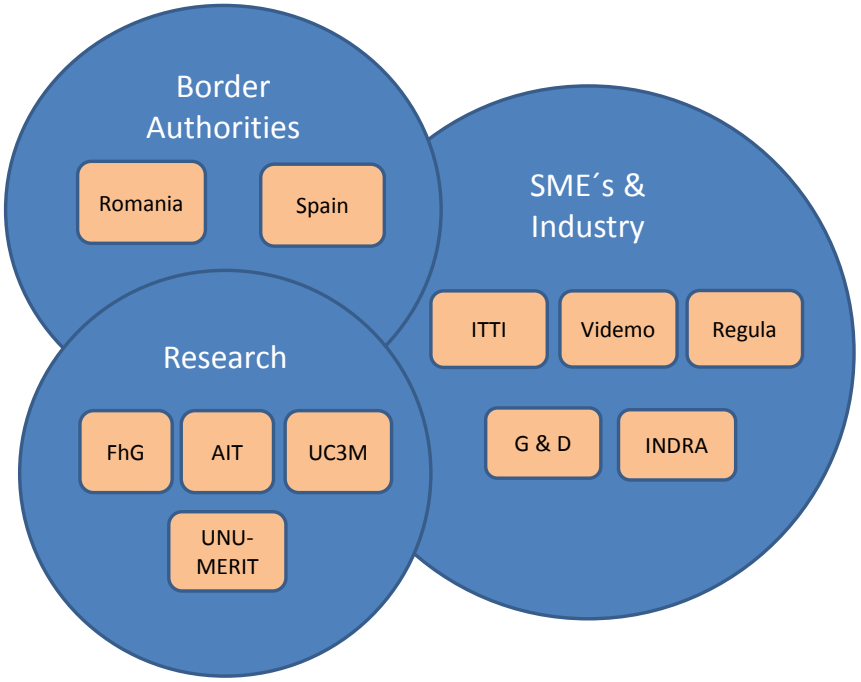
A

secure, (TPM, re-engineering, remote attestation, access control)
modular, (embedded hardware, used only as a scanner, interfaces, API´s)
distributed, (communication, wireless connectivity, nat./int. DBs, certificate stores)
and mobile (usability, battery, robustness, HMI, requirements)
border control solution (processes, workflows)

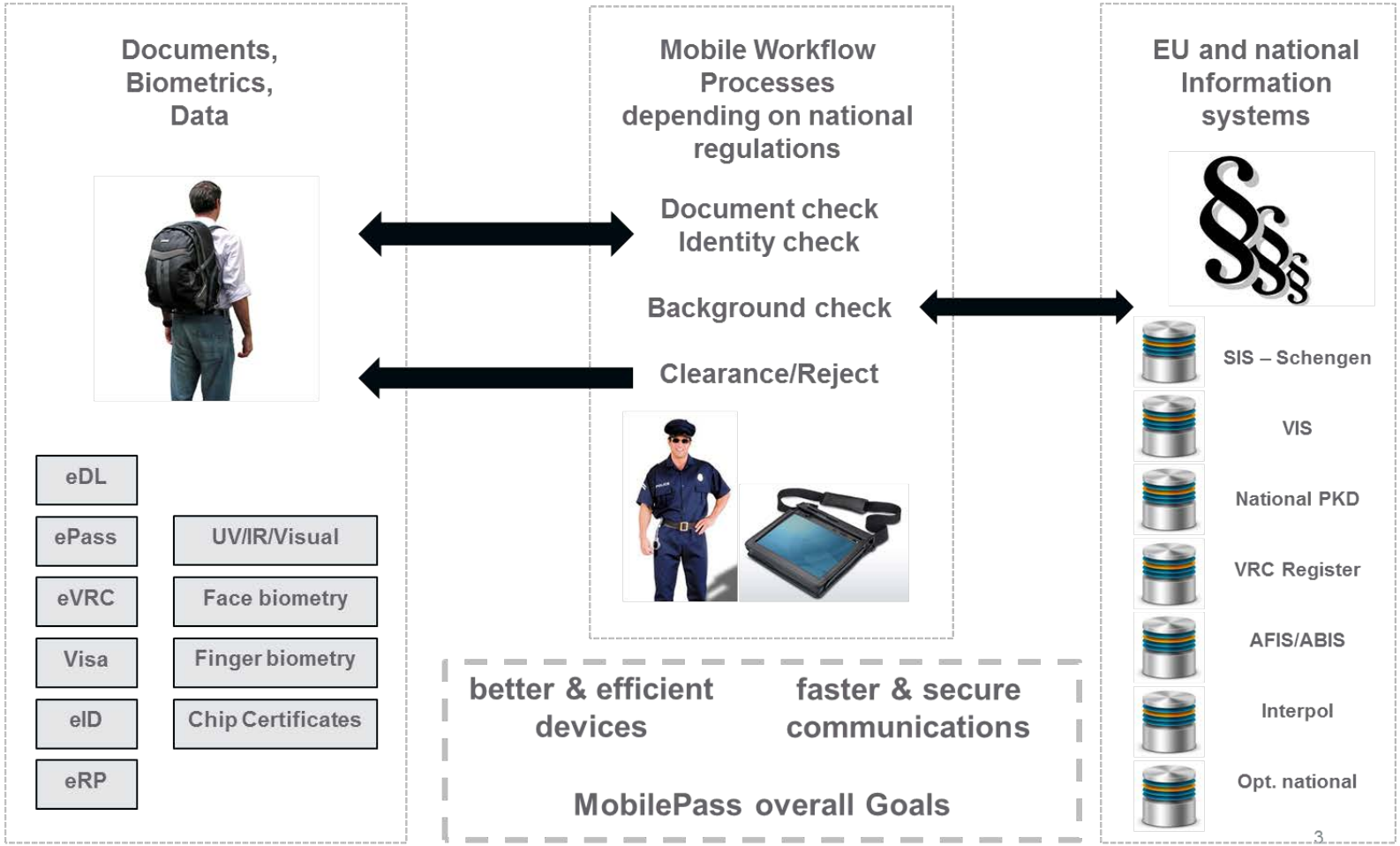
for European land border crossing points.

Consortium

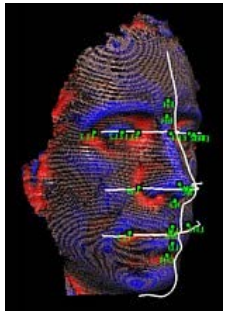
- University and Research Centers
  - AIT (Embedded systems, Architecture on mobile devices)
  - FhG (2/3D Capture and image enhancement)
  - UC3M (Identification technologies, Fingerprint Biometry, standards and evaluations)
  - UM-MERIT (Ethics)
- SMEs
  - Regula (Fullpage Passport Reader)
  - ITTI (communication systems)
  - VIDEMO (Face Biometry)
- Industry
  - G&D (Integrator)
  - INDRA (Integrator)
- National Service Provider, National Authorities
  - RBP Rumanian Border Police
  - SBP Spanish Border Police



Overview


Documents, Biometrics, Data
eDL
ePass
eVRC
Visa
eID
eRP
UV/IR/Visual
Face biometry
Finger biometry
Chip Certificates
Mobile Workflow Processes depending on national regulations
Document check
Identity check
Background check
Clearance/Reject
EU and national Information systems
SIS – Schengen
VIS
National PKD
VRC Register
AFIS/ABIS
Interpol
Opt. national
better & efficient devices
faster & secure communications
MobilePass overall Goals
3

Modular System Architecture
Objective: 1



Fast, Mobile
UV/IR, fullpage
Passport scanner

Fast, Mobile
face verification
camera

Fast, Mobile, contactless
fingerprint
scanner/camera

Advanced Components, Objectives: 2,3,4

Terminal Devices

Information systems

Fast, Reliable, Secure communication Objective: 5

Device approach (birds eye view)

Symbolic image

- Camera for MRZ, OCR-B Text (at a distance)
- Face Capture & Verification (integr. Illumination)
- Fingerprint Capture & Verification (contactless)
- 2-way connectivity
  - 3G,4G,LTE : Information Systems
  - BT,WIFI: other Scanners
- RFID ePassport Reader
- Secure Operating System and Application
- 3 Factor Authentication of User
- Pipeline Operation
- “Zero” - handed Operation
- Open API´s

Device approach

The “optimal” Device ?

Display,
Communication &
Control Unit

Face capture unit

Fullpage passport
scanning

Fingerprint capture unit

Vehicle Identification
Number

Three Components

- Document check device
  - Mobile, man worn, lightweight, battery operated
  - RFID reader, electronic security feature check
  - Camera, UV,IR, optical document security feature check
  - Radio connectivity
- Display, Face- and Fingerprint Reader device
  - Mobile, man worn, lightweight, battery operated
  - Sunlight readable display
  - 2-way radio connectivity (3G/4G/LTE + WIFI/BT)
  - Secure operating system (signed boot image)
  - Attached to forearm (hands free!)
  - De-tachable
  - Capture face
  - Capture fingerprints
- Base Station
  - Manages Workflow (needed checks on passenger)
  - Communicates with 2 devices

Three Components

Base Station Side

Border Side

Information Systems

Workflow Engine „Server Application“

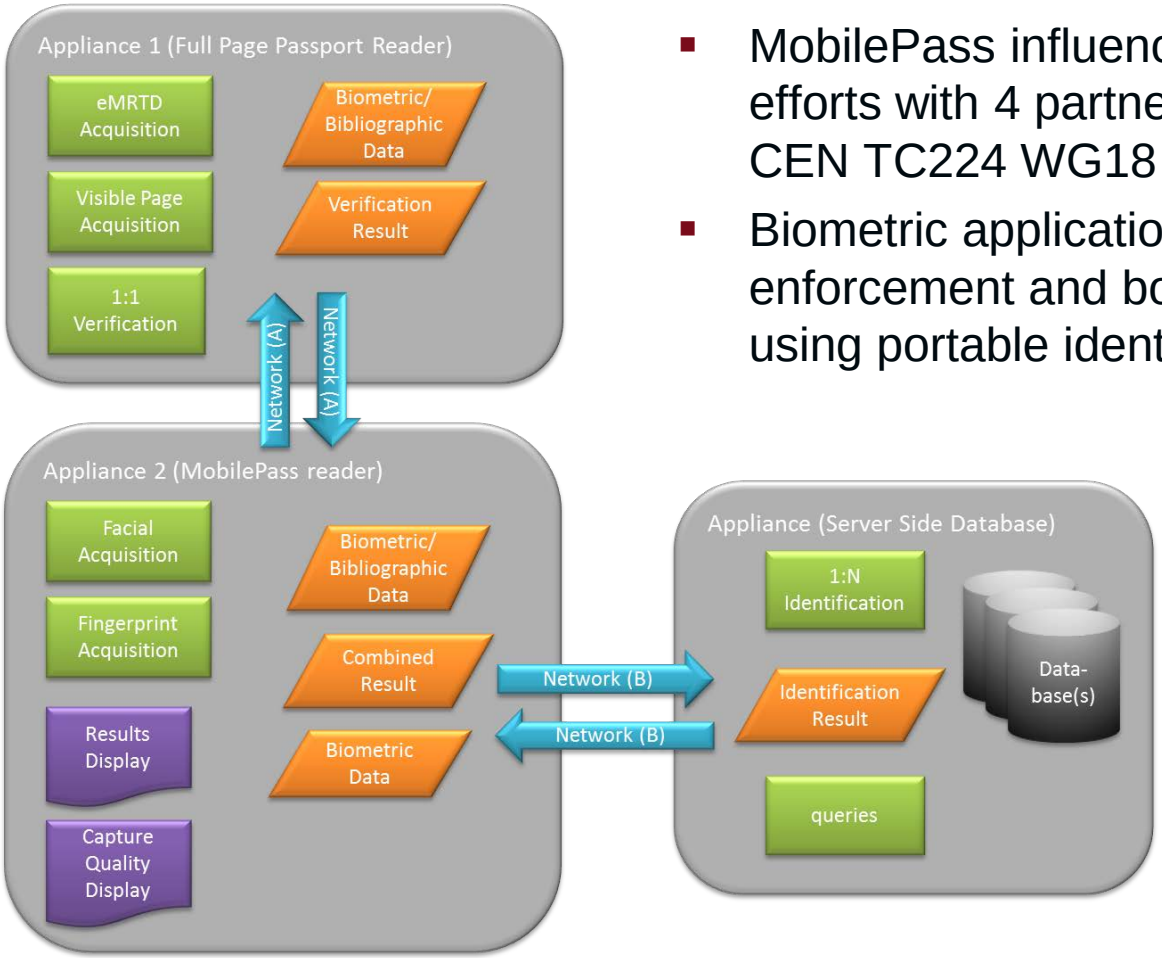
- Fullpage UV/IR Reader
- Hip worn
- MRZ + Visa scanning
- eMRTD scanning
- works in combination with main device

WiFi

- MobilePass Device
- Wrist worn
- Shows potential of camera
  - MRZ + Visa scanning at a distance
  - Contactless fingerprint scanning
  - Fast facial capture
- Uses modern powerful “handy” components
- works in combination with main device
- Potential to replace main device

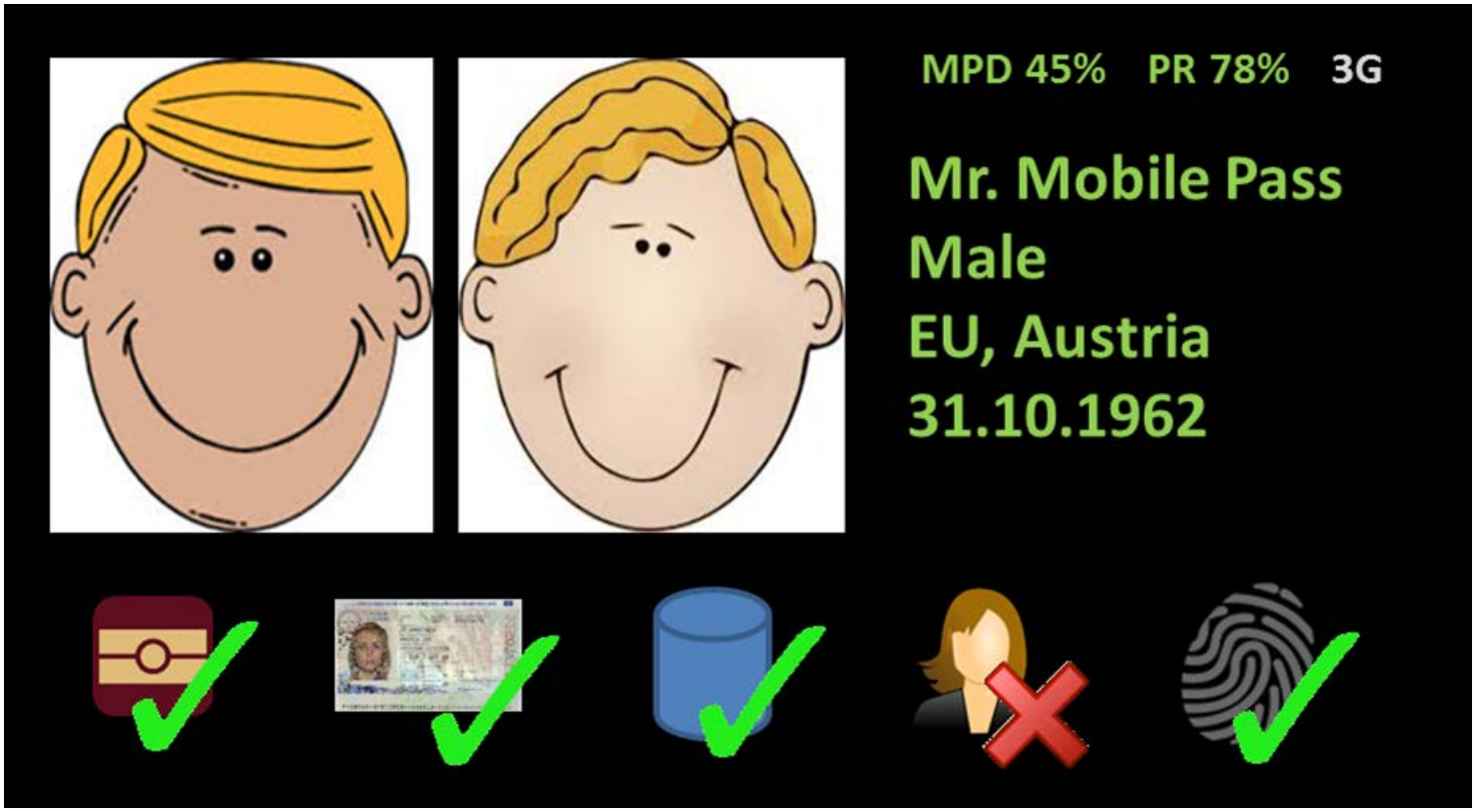
3G/4G LTE
WiFi
WMAX

Three Components on three Appliances

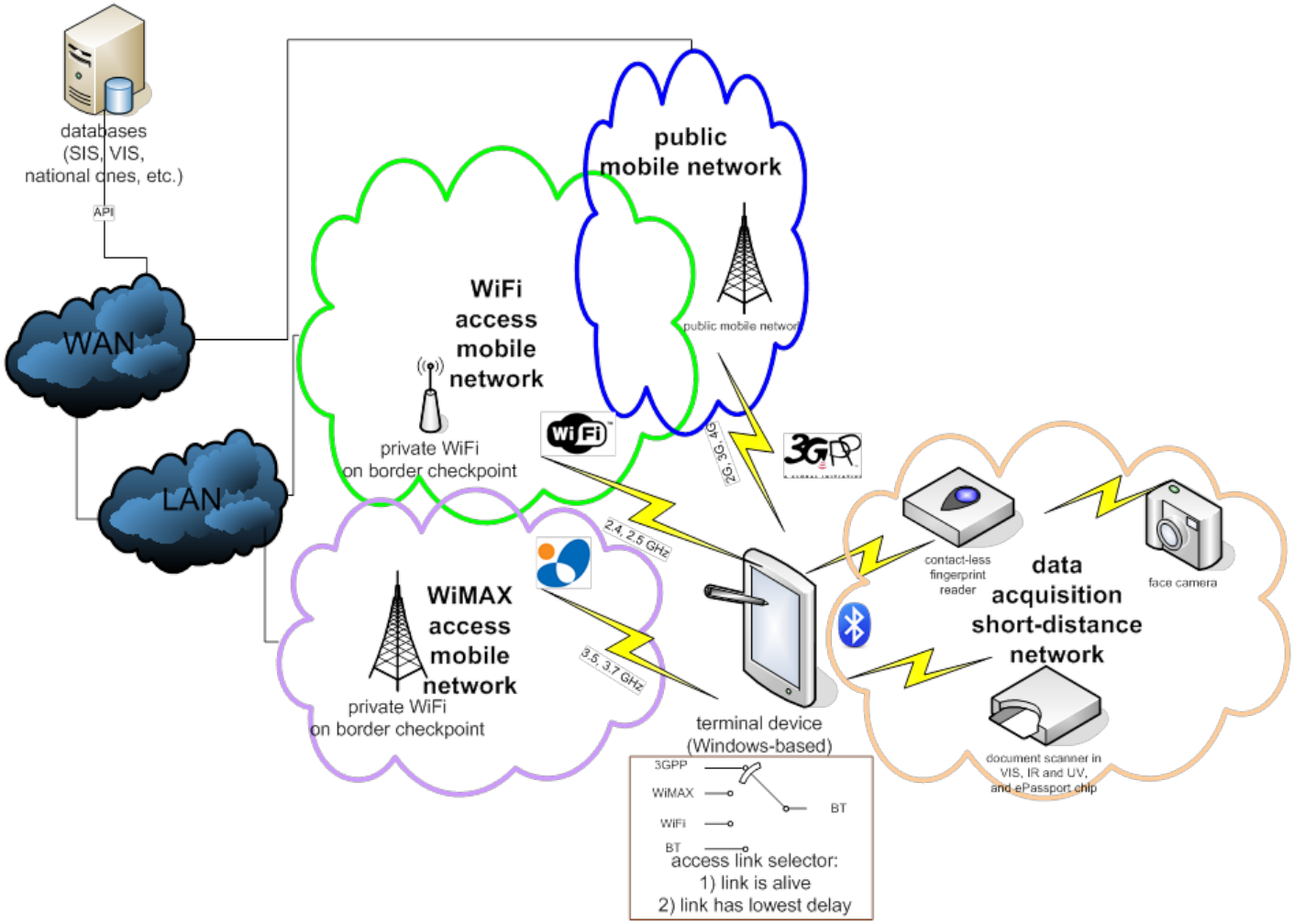


- MobilePass influences the standardization efforts with 4 partners represented in the CEN TC224 WG18
- Biometric application profiles for law enforcement and border control authorities using portable identification systems

User Interface



Device Connectivity



Communication Issues

- Transmission Security
  - Firewall (embedded), IDS (Intrusion detection system)
  - Stealth port scans
  - Common Gateway Interface (CGI) web attacks
  - Operation System (OS) fingerprinting attempts
  - Traffic flow anomalies
  - Distributed Intrusion Detection System (DIDS)
- Transmission availability
  - Automatic link selection depending on rules:
    - link is down
    - some QoS parameters are degraded: delay, throughput, transmission time
  - Accelerate the process of selection of a new link by an auxiliary table with the ranking of links used with success till now is managed
- Penetration Tests
  - Black, white and grey box tests
  - Vulnerability scanner, Security scanner, Vulnerabilities Assessment System

Progress Embedded Device

Device Security Features

- No change of Operating System or Application Software after deployment
  - Secure Boot
  - Use a TPM (Trusted Platform Module)
  - Boot Image is encrypted
  - Decryption key is “burned” into Silicon, but access mechanisms are destroyed
    -> cant be read out (except CPU itself at boot time)
- Hardware counteractive measures
  - At setup -> Electronic signal is applied to electronics and complete assembly
  - Response signal is captured and analyzed
  - In normal operation response signal is compared to stored signal
    response deviations above threshold -> denial of service (e.g. device opened)
- Denial of Service
  - If network intrusion is detected
  - No correct authentication of user
  - “Dead Man” detection
  - Movement of device in unauthorized area (with GPS and local stored operating zone)

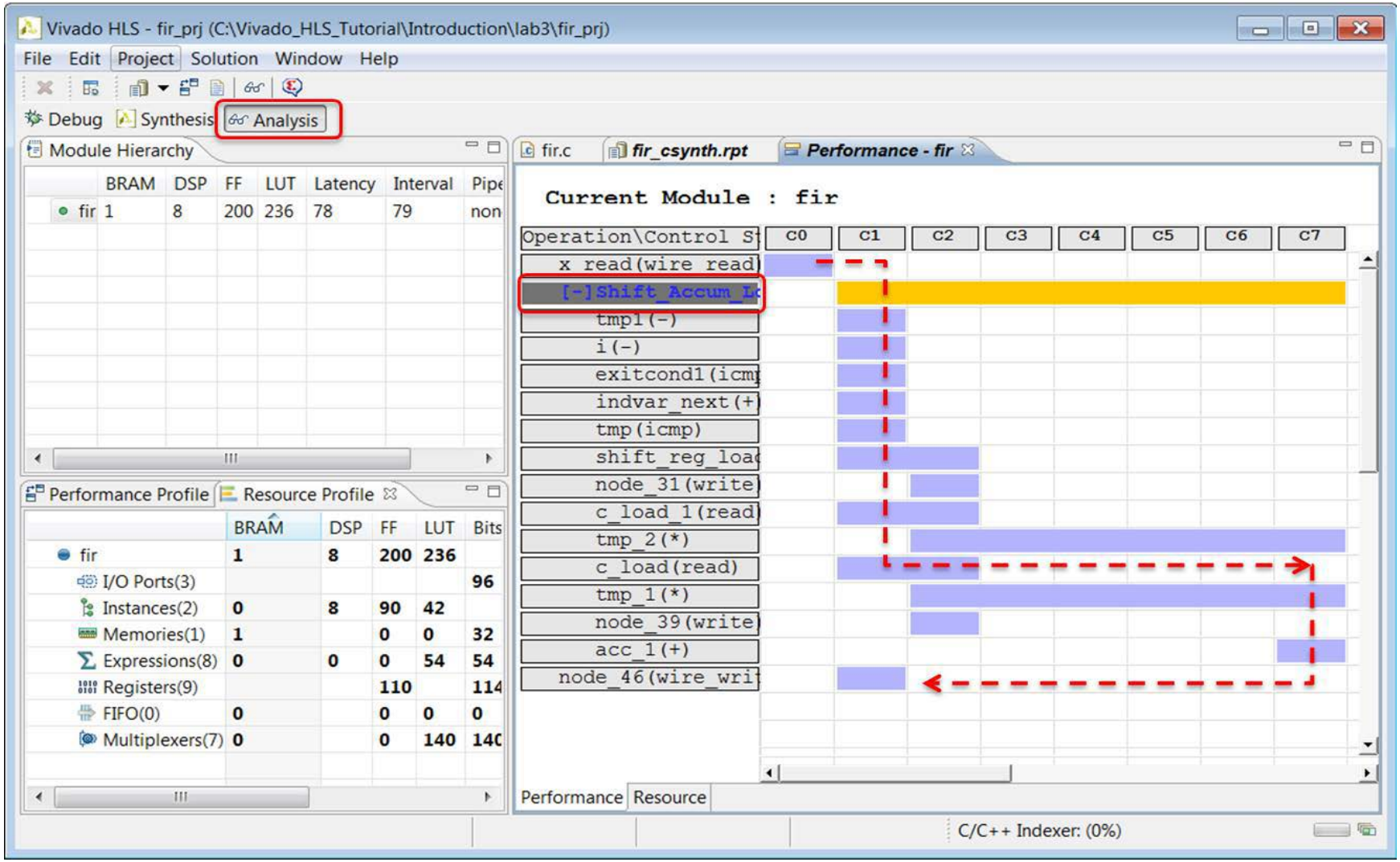
Processing Power: the old story

- Multicore CPUs
  - Power consumption (e.g. ARM M3 for music player)
  - Cool, but how to divide the algorithm ? -> big effort in SW development

- Processing Speed 2.4 Ghz and more
  - After some seconds of “full throttle” CPU is too hot and speed is automatically reduced
  - Its not only the speed (bus bandwidth, cache size, interrupt load, DRAM speed, etc.)
  - Tests and investigations showed that modern mobile CPU development toolchains
    - are not stable
    - drivers or documentation not available

- Accelerators
  - SoC from Xilinx, Altera (CPU combinations with FPGA on same chip)
  - Unfortunately only with single or dual cores
  - MobilePass develops Hardware i.MX6 (4 Core CPU plus FPGA) for a mobile Environment

Reduce development effort with HLS



AIT Austrian Institute of Technology

your ingenious partner

Coordinator: MobilePassCoordinator@ait.ac.at
Web: http://www.mobilepass-project.eu/

D.I. Bernhard Strobl
Thematic Coordinator Intelligent Camera Networks
Department Safety & Security
AIT – Austrian Institute of Technology
bernhard.strobl@ait.ac.at
+43 664 815 78 42