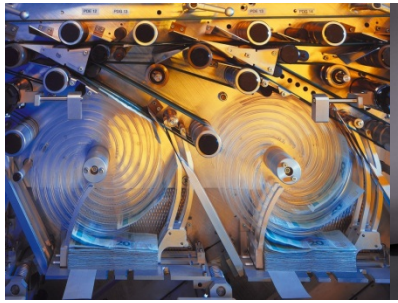
# Development and Industrial Application of Multi-Domain Security Testing Technologies

Case Study Experience Sheet
Banking Case Study from Giesecke & Devrient



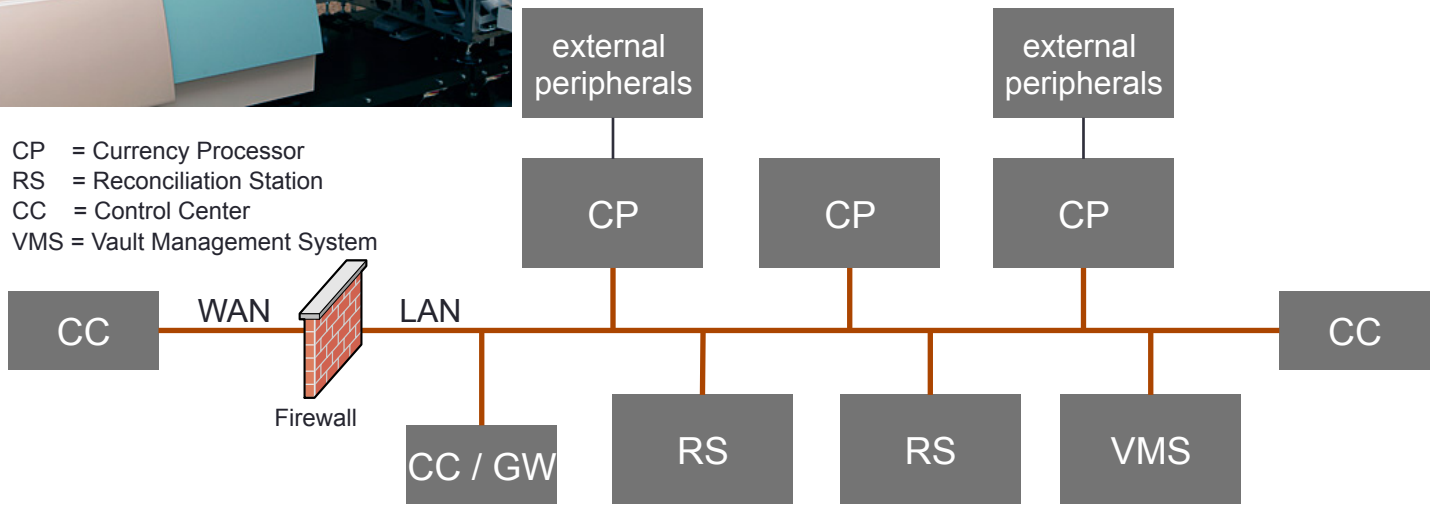

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

© DIAMONDS Consortium 2010-2013

# Banking Case Giesecke & Devrient

## Case study characterization

Banknote processing machine that counts, sorts and assesses banknotes by their currency, denomination, condition and authenticity.




ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT
Giesecke & Devrient
© DIAMONDS Consortium 2010-2013

# Banking Case Giesecke & Devrient
## Case study characterization

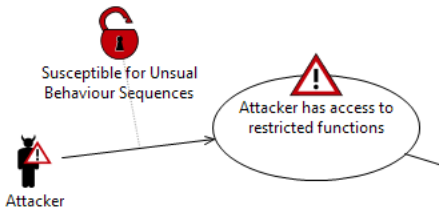
- Security challenges
  - **Restricted access to functions:** The access to functions is restricted to authorized users.
  - **Operation system access restriction:** The access to the operation system, i.e. file system, or process monitor is restricted to authorized users.
  - **Prevent Admin Hijacking:** Hijacking an administrator account is used to get the privileges of an administrator account as a user that is not assigned to the administrator group.
  - **Prevent infiltration/manipulation of software:** Software manipulation can be used to fake data or to provoke errors on the currency processor application.
  - **Prevent manipulation of application configuration:** Manipulation could possibly change the classification of banknotes.

© DIAMONDS Consortium 2010-2013

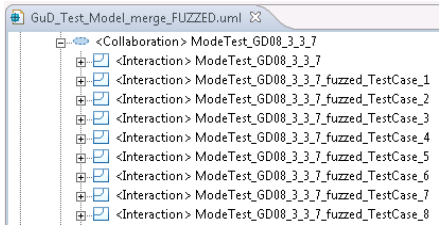
# Banking Case Giesecke & Devrient

## Testing approach: risk-based security testing

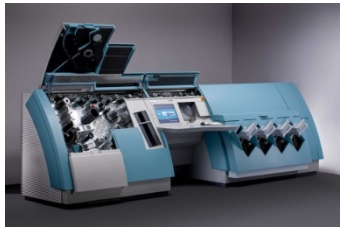
**CORAS Risk Analysis**
Deliverable D1.WP2*




**Behavioural Fuzzing**
Deliverable D2.WP2* (see also next slide), D3.WP2*




**Data Fuzzing with TTCN-3**
Deliverable D3.WP3*



Risk Analysis (CORAS) → Security Test Pattern Identification → Test Generation → Test Code Generation (TTCN-3) → Test Execution

| Pattern name | Usage of Unusual Behavior Sequences |
|---|---|
| Context | Test pattern kind: Behavior<br>Testing Approach(es): Prevention |
| Problem/Goal | Security of information systems is ensured in many cases by a strict and clear definition of what constitutes valid behavior sequences from the security perspective on those systems. For example… |
| Solution | Test procedure template:<br>1. …<br>2. … |
| Known uses | Model-based behavioural fuzzing of sequence diagrams is an application of this pattern |

**Security Test Pattern Catalogue**
Deliverable D3.WP4.T1*

```
testcase ModeTest_GD08_3_3_7_fuzzed_TestCase_219 ()
runs on Comp_CP_RS
system System_CP_RS
{
    var integer i, v_total, v_rjc;

    f_mtcSetup_CP_RS(CPRSStartingMode:All);

            f_CP_logon("OP1");
            f_CP_selectProcessingModeUS(Processi
```

*project deliverables are available at www.itea2-diamonds.org "publications"

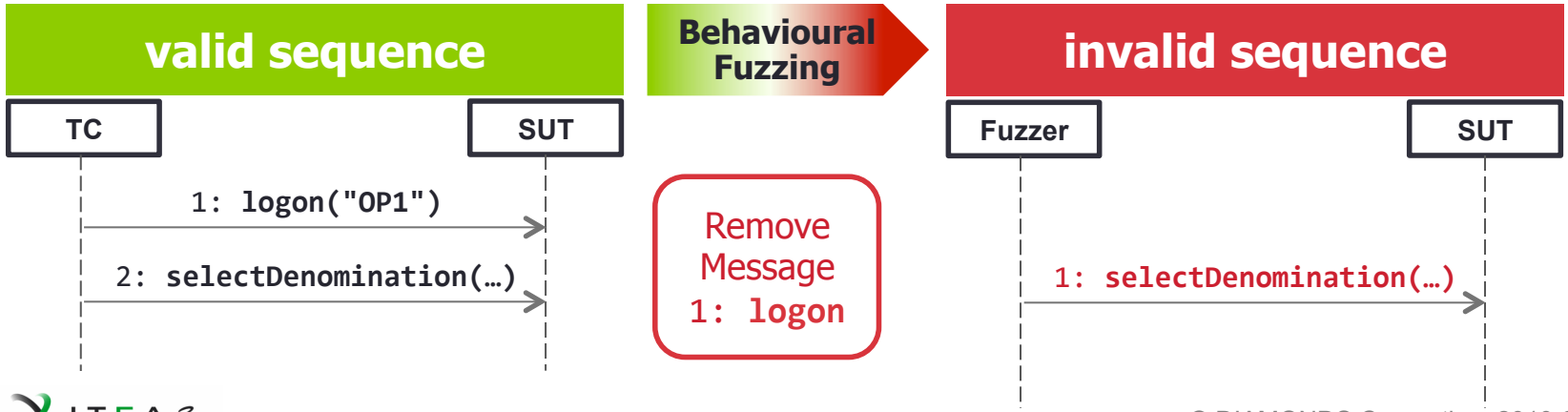
ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

© DIAMONDS Consortium 2010-2013

# Banking Case Giesecke & Devrient

## Testing approach: behavioural fuzz testing

- Test cases are generated by **fuzzing one or more valid sequences.**
- This concrete fuzzing of behaviour is realized by changing the order and appearance of messages in two ways:
  - **By rearranging messages directly**. This enables straight-lined sequences to be fuzzed. Fuzzing operators are for example remove, move or repeat a message.
  - **By utilising control structures of UML 2.x sequence diagrams**, such as combined fragments, guards, constraints and invariants. This allows more sophisticated behavioural fuzzing that avoids less efficient random fuzzing.
- By applying one ore more fuzzing operators to a valid sequence**, invalid sequences (= behavioural fuzzing test cases)** are generated.




© DIAMONDS Consortium 2010-2013

# Banking Case Giesecke & Devrient
## Results

- **Focus on risks related to**
  - unauthorized access
  - machine/configuration modification
- **Until now, no weaknesses were found**
  - confidence in the security of the system is strengthened
- **Metrics**
  - different security levels depending on the covered risks/ vulnerabilities by
    - **number of test cases (one or more) per risk/vulnerability**
      unauthorized access, configuration modification: more
    - **number of test methods to generate these test cases**
      data fuzzing and behavioural fuzzing: 2 test methods

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT
© DIAMONDS Consortium 2010-2013

# Banking Case Giesecke & Devrient
## Exploitation

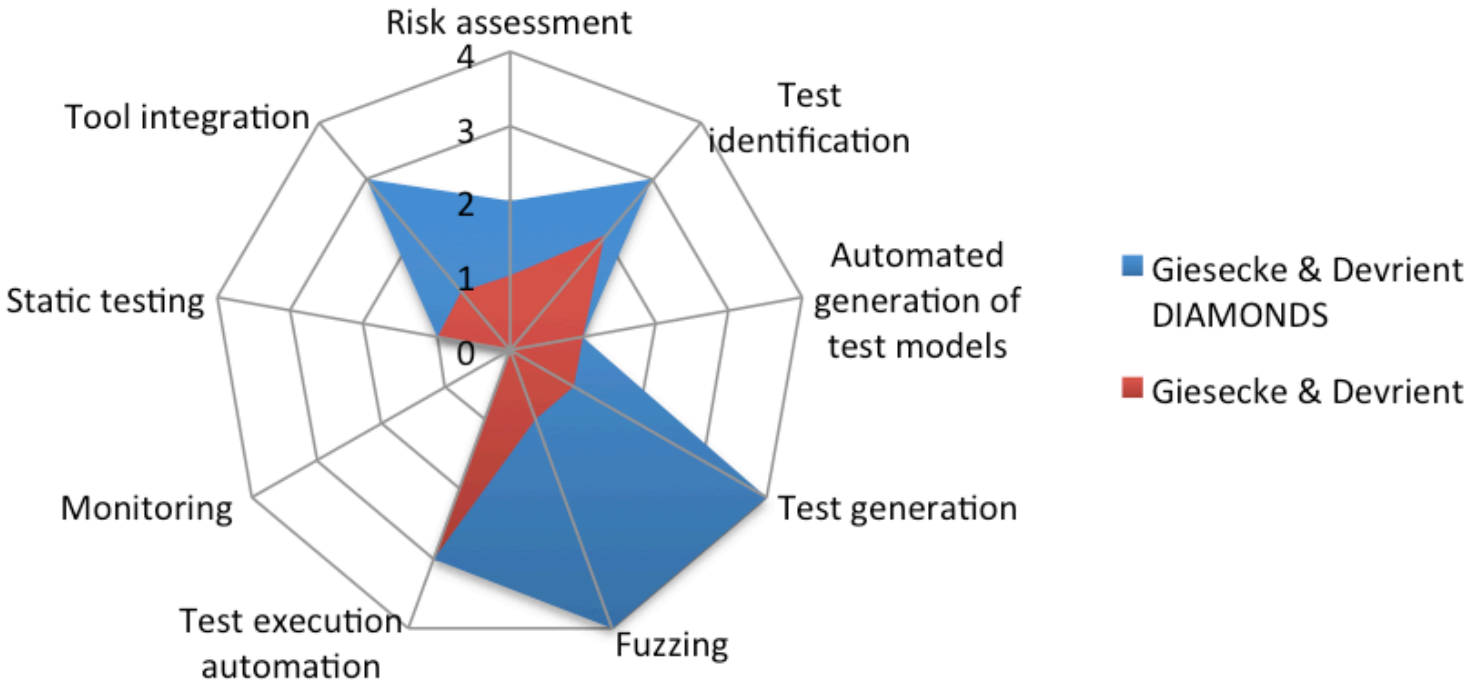
- **CORAS method for risk analysis has been proved of value**
  - graphical modelling
  - specification of assets to be protected
- **Saved resources due to**
  - reuse of functional test cases and
  - reuse of test execution environment for non-functional security testing
  - integration of data fuzzing in the TTCN-3 execution environment
    - keeps the behavioural model clean and concise
    - allows easy combination of data and behavioural fuzzing
- **Standardization of DIAMONDS results provides certification options for products with security requirements**

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

© DIAMONDS Consortium 2010-2013

# Banking Case Giesecke & Devrient
## Summary

- **Improvement gains according to DIAMONDS STIP:**




© DIAMONDS Consortium 2010-2013