ICALEPCS 2015

International Conference on Accelerator
& Large Experimental Physics
Control Systems

Open-source fuzzing testing
for critical equipment robustness

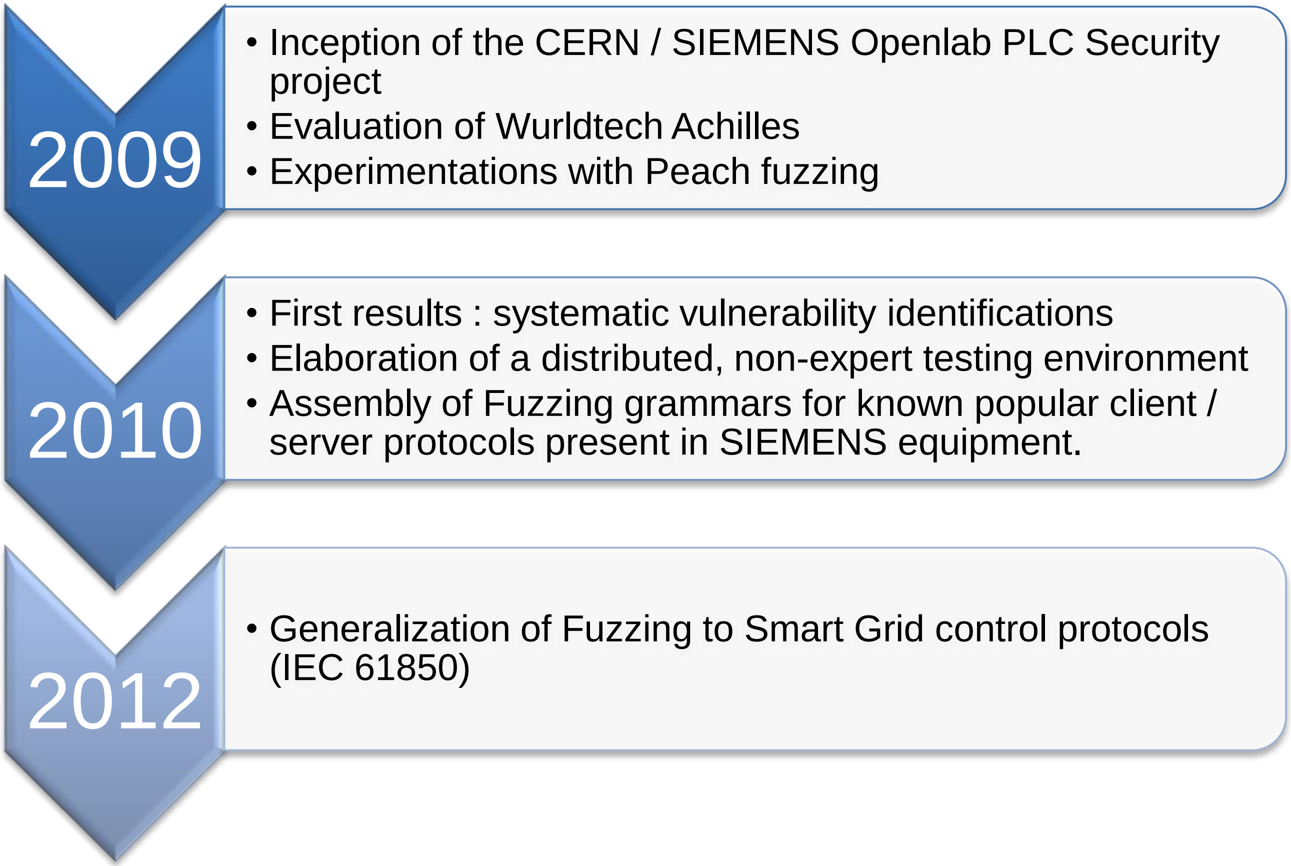
Brice Copy
Engineering Department
CERN, Switzerland

(CS)2/HEP Workshop
18th October 2015, MCEC

ICS cyber-security : A giant with feet of clay ?

- We now have IEC / ISA 99 standards.
- We now have awareness thanks to high-profile events published in the news.
- We now have device vendors with decent practices :
    - Vulnerability reports and assessments.
    - Systematic CVE identification.
- Yet :
    - Many vulnerable devices still in the wild.
    - We have still little visibility over which control devices are more robust from a cyber-security standpoint.
    - Vulnerabilities keep rearing the heads up via regressions.

PLC Robustness testing at CERN : A timeline



2009

- Inception of the CERN / SIEMENS Openlab PLC Security project
- Evaluation of Wurldtech Achilles
- Experimentations with Peach fuzzing

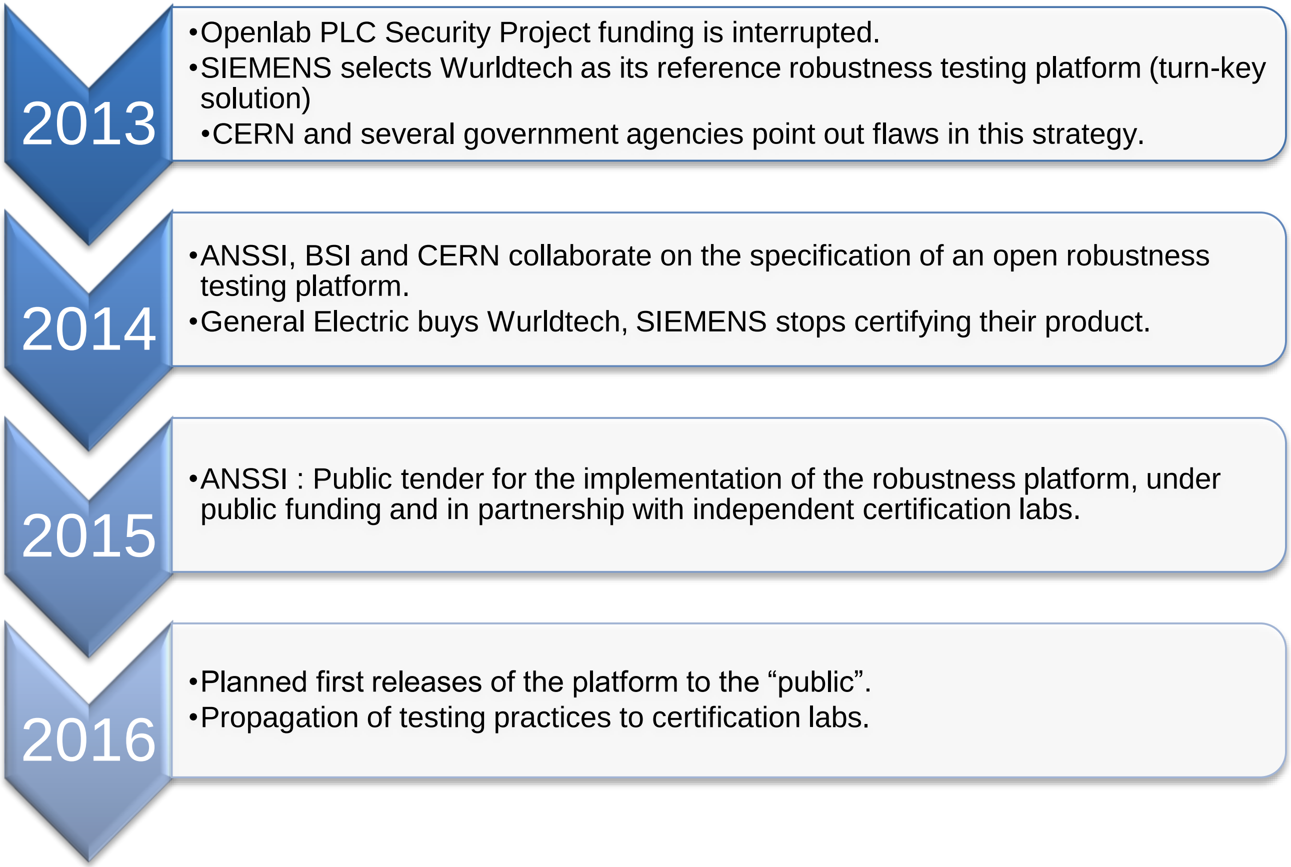
2010

- First results : systematic vulnerability identifications
- Elaboration of a distributed, non-expert testing environment
- Assembly of Fuzzing grammars for known popular client / server protocols present in SIEMENS equipment.

2012

- Generalization of Fuzzing to Smart Grid control protocols (IEC 61850)

PLC Robustness testing at CERN : A timeline (2)



2013

- Openlab PLC Security Project funding is interrupted.
- SIEMENS selects Wurldtech as its reference robustness testing platform (turn-key solution)
  - CERN and several government agencies point out flaws in this strategy.

2014

- ANSSI, BSI and CERN collaborate on the specification of an open robustness testing platform.
- General Electric buys Wurldtech, SIEMENS stops certifying their product.

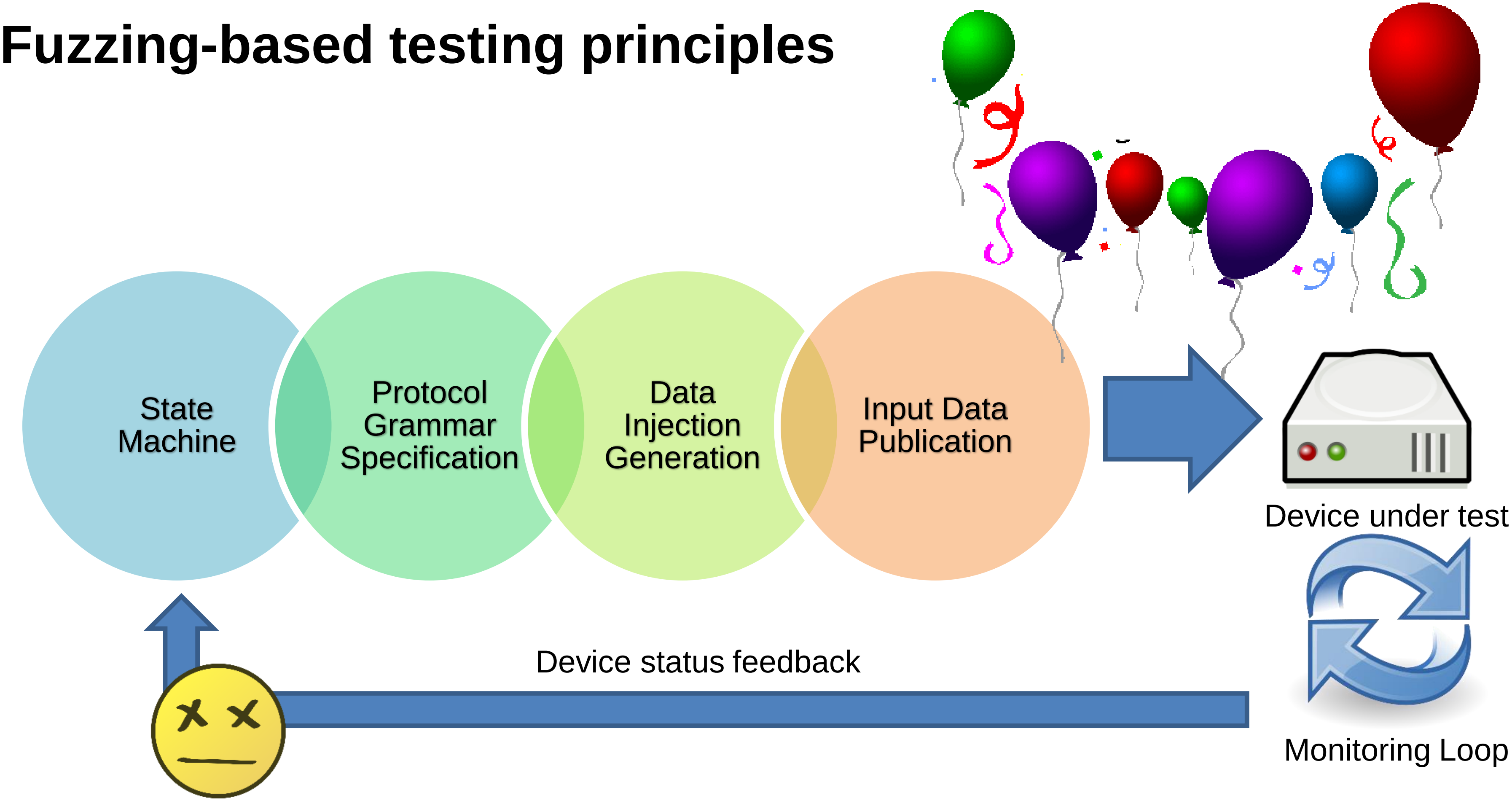
2015

- ANSSI : Public tender for the implementation of the robustness platform, under public funding and in partnership with independent certification labs.

2016

- Planned first releases of the platform to the “public”.
- Propagation of testing practices to certification labs.

Fuzzing-based testing principles



Fuzzing-based testing principles

- Automated data injection to a device under test (DUT)
- Fuzzing is semi-random:
  - Grammars make it reproducible: essential for quality processes.
  - Seeding allows to restart the testing sequence at a well-known point.
- Testing coverage can be adjusted exactly :
  - Define enough permutations to explore your protocol data domain…
  - … ensure that the testing sequence completes in acceptable time.
- Tuning: find the right balance between random inputs (domain exploration) and static specifications (areas to cover).
- The grammar and seeding can be pre-set to demonstrate a single vulnerability with surgical precision !

Requirements for a Fuzzing platform

- A common, open-source framework to inject traffic :
  - Fuzzing mechanisms must be entirely clear and stable.
  - Grammars rely on a domain-specific language, and can be prepared from protocol specification (white-box implementation) or from expert-knowledge (grey-box implementation)
- Tests can be customized by adjusting for instance :
  - Protocol header format
  - Protocol field values
  - Protocol state machine

Requirements for a Fuzzing platform (2)

- Test results are expressed in jUnit report format, for easy integration into a continuous integration process, quality reports.
- Test results are annotated with input parameters to allow reproducibility :
  - Input grammar.
  - Initial seeding, sequence ranges.
  - Input data publishing configuration.
- Compatibility with ISA Secure ISCI Device Robustness criteria.

Conclusions

- An open, public funded platform to assert device robustness.
- A transparent, white-box testing process open to extensibility.
- A third-party certification process that ensures :
    - Impartiality of the assessment process.
    - Objective assessment of devices, with a real commercial offering.
- An open community for the exchange of tests and expertise.
- The possibility to reuse the platform privately internally for continuous quality improvement purposes.

- Stay tuned…

Thank you for your attention

- Questions ?