Tool for Supporting a Common Criteria Evaluation

9th International Common Criteria Conference
Jeju, Korea – 25th September 2008

Motivations

- Automatize process and repetitive tasks
- Focus the evaluator effort on processes which require cognitive skills
- Understand potential automation in CC evaluations
- Learn about how XML and XSL transformations can assist in the process of automation
- *Not just less work, but smart work*

Index

1. Automation
    1. Why
    2. How
    3. With What
2. Tool
    1. Inputs
    2. Processing
    3. Outputs
3. Current Status
4. Future Work

Automation

- Reduce human intervention to a minimum
  - checking consistency
- Synchronize the results obtained for each evaluator
- Support the sponsor in avoiding typical mistakes
- Generate documentation using less time and effort
  - ETR from work units
  - OR from problems

Why Automation?

Evaluators

- Reduce evaluation time and cost
- Detect errors earlier
- Focus on vulnerability search
- Track the evidences produced during the evaluation process

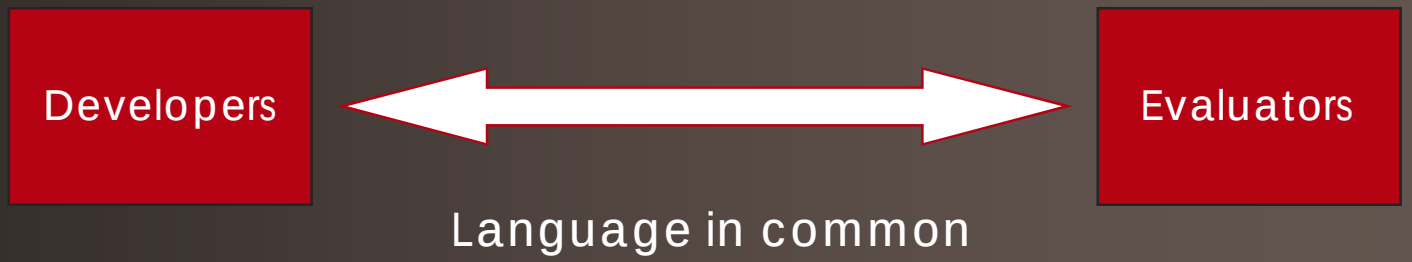
Why Automation?

Developers

- Help sponsor to reduce common errors in documents
  - Check common errors before sending documentation
- Reduce the sponsor effort (time and cost)
- Improve sponsor satisfaction

Why Automation?

- Agree on a language in common between Developer and Evaluator team
  - Establish fluent communication
  - Process automatically

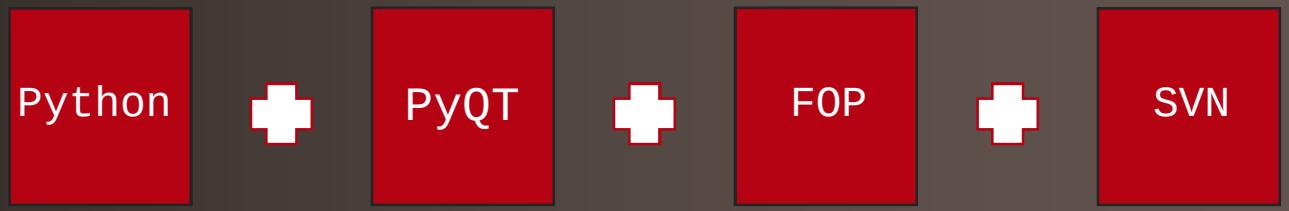


How Automation?

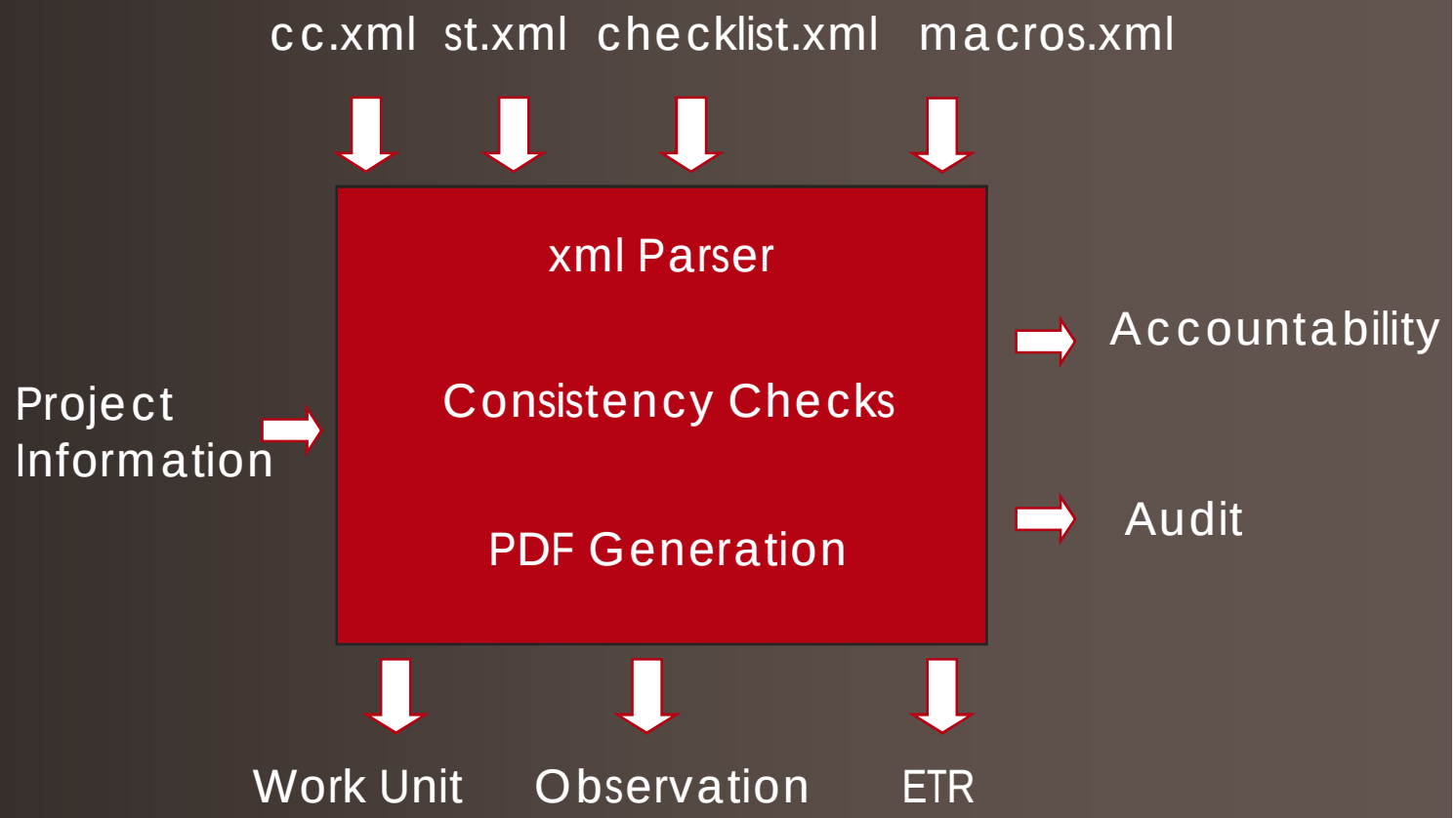
- XML
  - Structure independent from presentation
  - Source human and machine readable
  - Flexible markup language
  - Platform independent
  - Negotiated language between the man and the machine
- XSL Transformations
- Python Processing
- SVN
  - Open source version control system
  - Allow integration between evaluators

What Tools?

- Python: Data processing
- PyQT: User Interface
- FOP: XSL Transformations to PDF files
- SVN: Configuration management tool



SECT: Security Evaluation CC Tool



SECT: Inputs

- Common Criteria Part 1-3 and CEM (from CCN, Spain)
  - cc.xml
  - cc2.xml

```
<m-workunit eal="all">
    <ae-dc-element id="acm_aut.1.2c"/>
  <para type="normal">
    The evaluator shall check the CM documentation for
    automated means to support generation of the TOE from
    its implementation representation.</para>
  <para type="normal" id="pgfId-710262">
    In this work unit the term ``generation''
    applies to those processes adopted by the developer to
    progress the TOE from its implementation to a state
    ready to be delivered to the end customer.</para>
  <para type="normal" id="pgfId-710263">
    The evaluator should verify the existence of automated
    generation support procedures within the CM
    documentation.</para>
</m-workunit>
```

SECT: Inputs

- Security Target
  - st.dtd (from CCN, Spain)

```
<!ELEMENT introduction      (identification,overview,cc-claim)>

<!ENTITY % parasequence "(biblioentry|figure|glossentry|para|subclause|table)*">

<!ELEMENT identification    (st-reference,toe-reference)>
<!ELEMENT overview      (%parasequence;)>
<!ELEMENT cc-claim      (%parasequence;)>

<!ELEMENT st-reference      (st-title,st-version,st-revision,st-author,st-publication-date)>
<!ELEMENT toe-reference     (developer,toe-name,toe-version)>

<!ELEMENT st-title              (#PCDATA)*>
<!ELEMENT st-version            (#PCDATA)*>
<!ELEMENT st-revision           (#PCDATA)*>
<!ELEMENT st-author         (#PCDATA)*>
<!ELEMENT st-publication-date       (#PCDATA)*>
<!ELEMENT developer         (#PCDATA)*>
<!ELEMENT toe-name          (#PCDATA)*>
<!ELEMENT toe-version           (#PCDATA)*>
```

SECT: Inputs

- Checklists for each work unit
  - checklist.xml

```
<assessment-method type="Examine">
    <select-from>
        <ol>
        <li>
            <foreach operation="=">
                <item>label.packagingOrMedia</item>
                <item>label.guidance</item>
                <item>label.operationalTOE</item>
            </foreach>
        </li>
        <li>
            <foreach operation="=">
                <item>reference.TOE</item>
                <item>TOEreference.ST</item>
            </foreach>
        </li>
        <li>
            <foreach operation="=">
                <item>label.operationalTOE</item>
                <foreach operation="+">
                    <item>label.operationalTOEComponent</item>
                </foreach>
            </foreach>
        </li>
        </ol>
    </select-from>
</assessment-method>
```

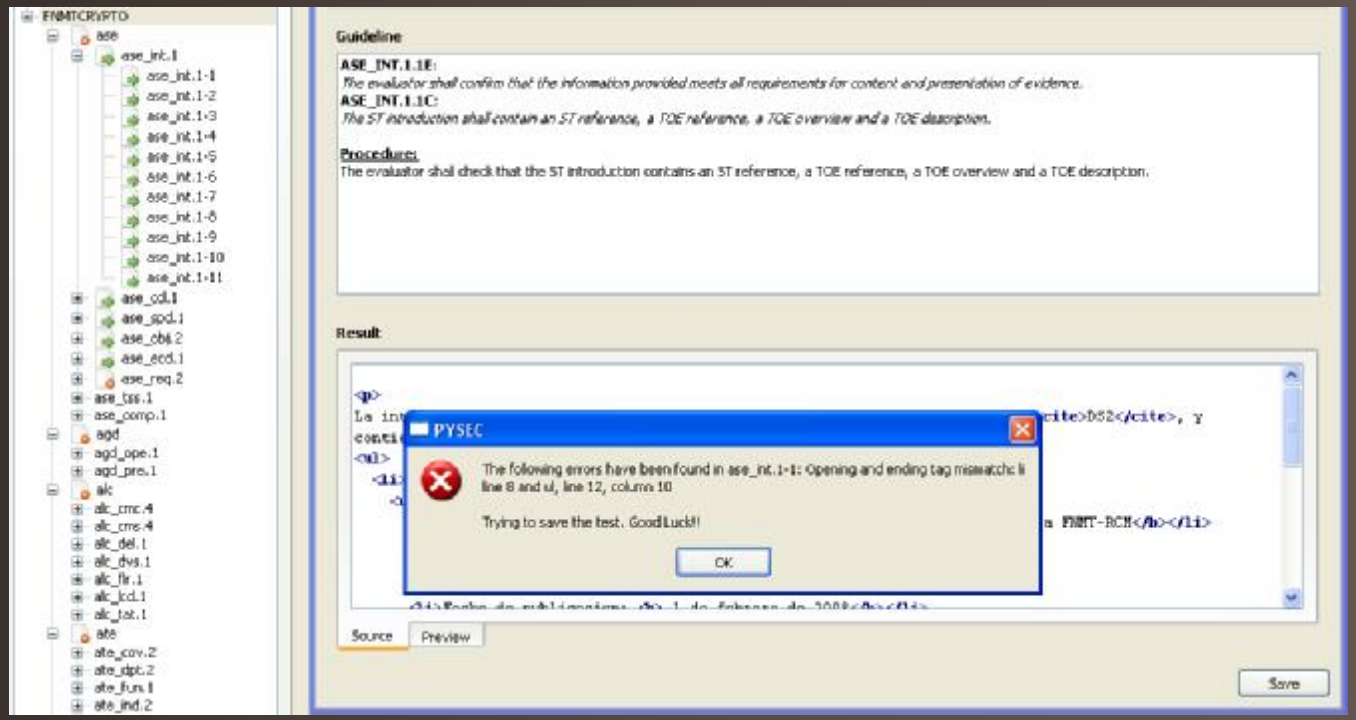
SECT: Inputs

- Macros
  - macros.xml

```
<basic>
    <ProductS>FNMT Crypto</ProductS>
    <ProductL>************************************</ProductL>
    <ProductV>***</ProductV>
    <ProductC>***********</ProductC>
    <EALLevel>EAL 4</EALLevel>
    <EALAumentado><ul><li>ALC_FLR.1</li><li>AVA_VAN.5</li></ul></EALAumentado>
    <SponsorS>FNMT-RCM</SponsorS>
    <SponsorL>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda</SponsorL>
    <SponsorA>FNMT-RCM<br/>Calle Odonnel<br/>28090 Madrid</SponsorA>
    <DeveloperS>FNMT-RCM</DeveloperS>
    <DeveloperL>Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda</DeveloperL>
    <DeveloperA>FNMT-RCM<br/>Calle Odonnel<br/>28090 Madrid</DeveloperA>
    <CBS>CCN</CBS>
    <CBL>Centro Criptológico Nacional</CBL>
    <CBA>Organismo de Certificación<br/>Avda. Padre huidobro s/n<br/>28023 Madrid<br/>http://
    <CCV>3.1 R2</CCV>
    <CEMV>3.1 R2</CEMV>
    <EvalLevel>EAL4+ AVA_VAN.5 y ALC_FLR.1</EvalLevel>
    <startDate>12-02-2008</startDate>
</basic>
```

SECT: Processing

- Parsing XML: User writes in xml vs dtd
  - Using a XML parser (Python)



SECT: Processing

- Checking consistency
  - ASE_REQ.2-3: The evaluator *shall examine* the ST to determine that all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined.
  - ASE_OBJ.2-2: The evaluator *shall check* that the security objectives rationale traces all security objectives for the TOE back to threats countered by the objectives and/or OSPs enforced by the objectives.
  - ASE_ECD.1-2: The evaluator *shall check* that the extended components definition defines an extended component for each extended security requirement.

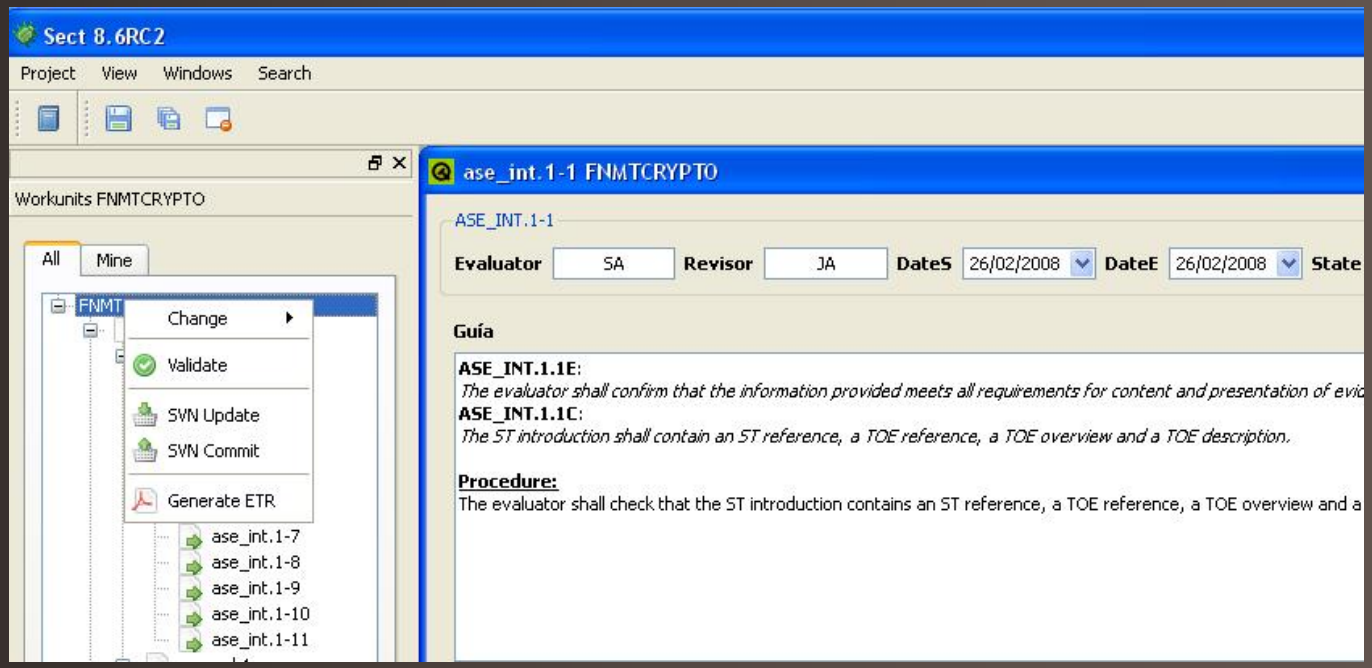
SECT: Processing

- Generating PDF (Report)
  - XSL: Using FOP

```
<?xml version="1.0" encoding="UTF-8" ?>

<!-- STYLESHEET FOR REPORTS -->

<xsl:stylesheet
  version="1.1"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:fo="http://www.w3.org/1999/XSL/Format"
  xmlns:axf="http://www.antennahouse.com/names/XSL/Extensions"
  exclude-result-prefixes="fo">

  <xsl:include href="param.xsl"/>
  <xsl:include href="attribute.xsl"/>
  <xsl:strip-space elements="table tr td program"/>

  <xsl:template match="report">
    <fo:root xmlns:fo="http://www.w3.org/1999/XSL/Format">
      <fo:layout-master-set>
        <fo:simple-page-master master-name="PageMaster"
```

SECT: Outputs

- Work Unit / Subactivity / Activity Report
- Observation Report
- Evaluation Technical Report



Current Status

- PDF Report Generation
  - Work Units
  - Observations
  - Evaluation Technical Report
- Intelligent Labels
- Work with XML Security Targets that meet a DTD
- Evaluation Process Management and Coordination
- Checklist (ALC_CMC.4)

Future Work

- Checklists (ALC site visit)
- Reports signed with electronic signatures
- Generate Plans, Procedures and Reports automatically (ATE and AVA)
- Work with XML Documents that meet a DTD (not only the ST)
- Incorporate requirements from supporting documents

Instituto Nacional de Técnica Aeroespacial

CESTI

Thank you

Maria Soraya Artiles Burgos

Security Technical Manager

artilesbs@inta.es