

Automated Cyber-Readiness Evaluation (ACE)

Rotem Guttman

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0004109

DoD Challenge Problem

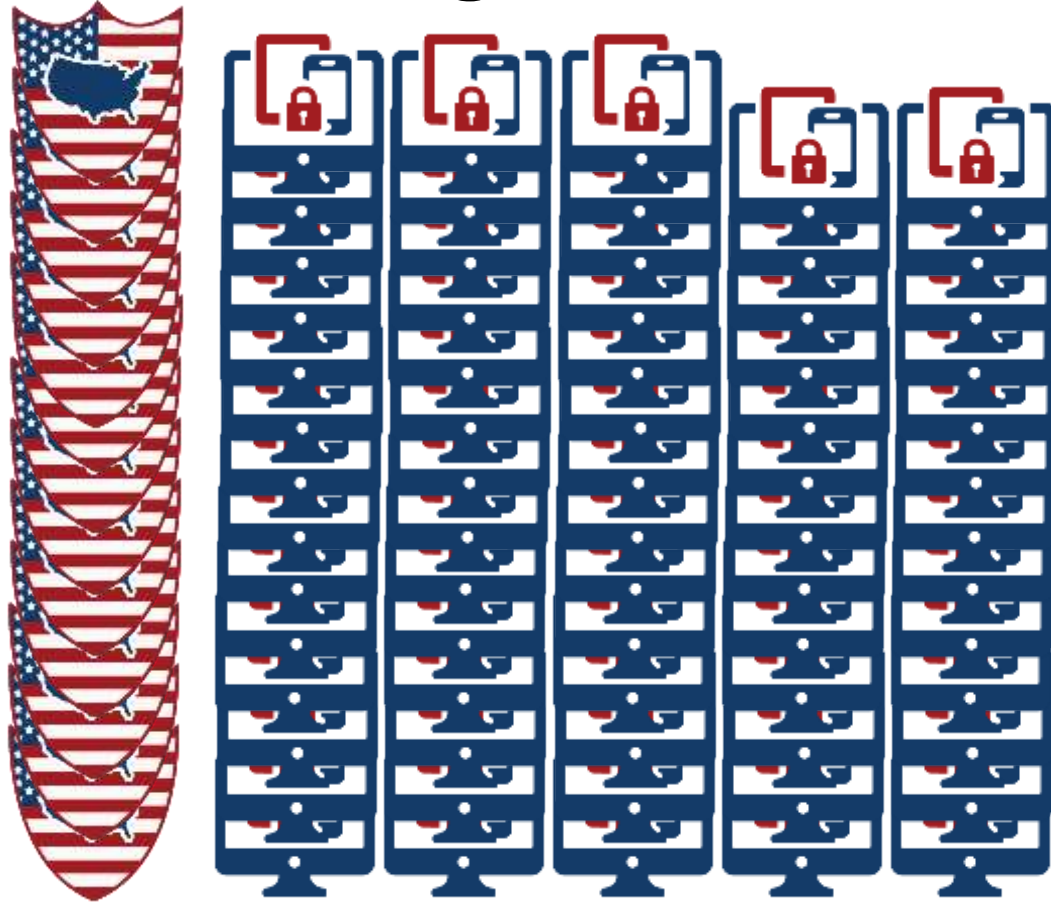


**13 National Mission Teams
(Defend the Nation)**

Evaluating Mission-Readiness for Cyber Operators at Scale

- **Scalable**
- **Objective**
- **Reliable**
- **Valid**

DoD Challenge Problem

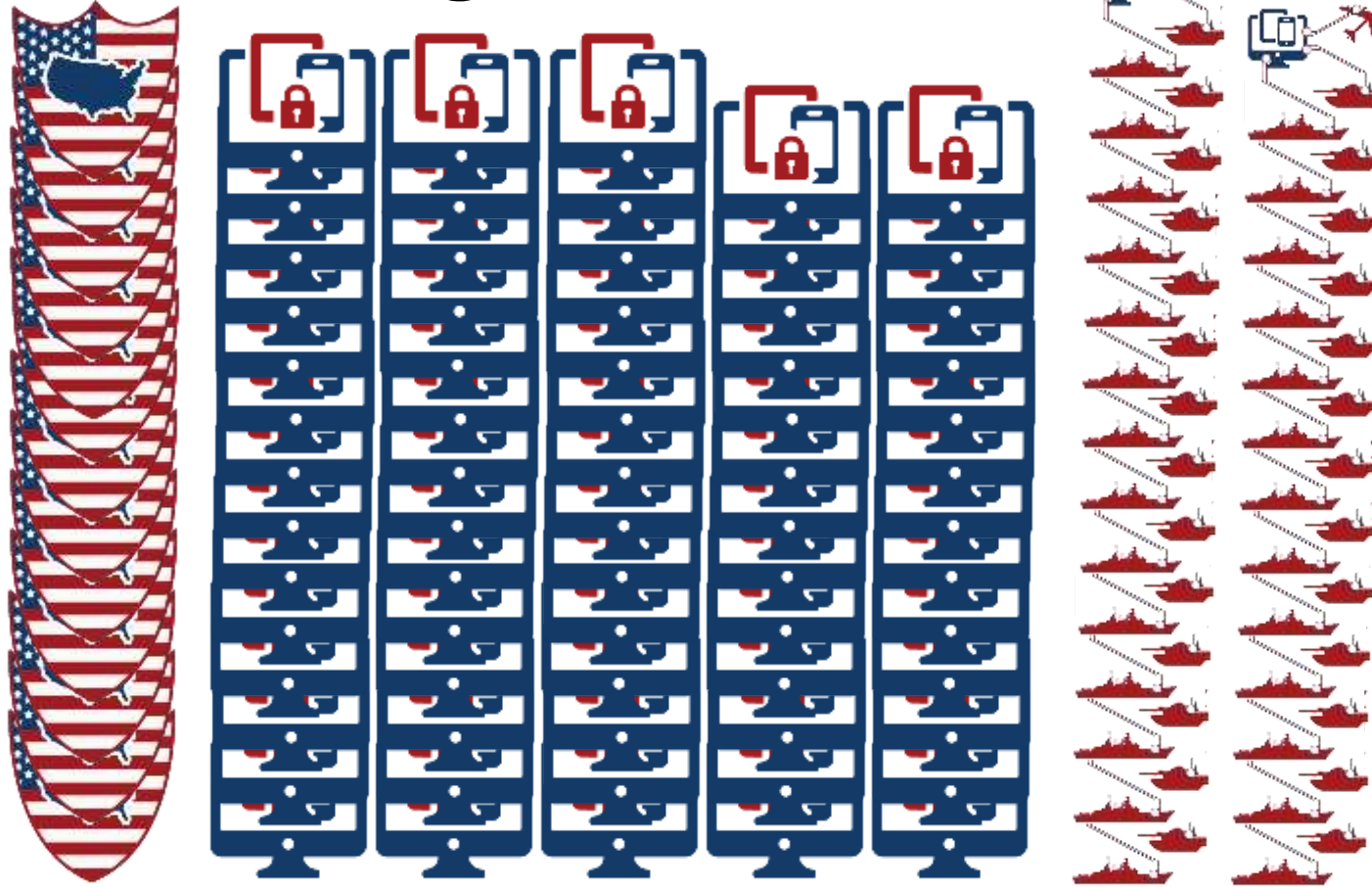


**68 Cyber Protection Teams
(Defend DoD Networks)**

Evaluating Mission-Readiness for Cyber Operators at Scale

- **Scalable**
- **Objective**
- **Reliable**
- **Valid**

DoD Challenge Problem

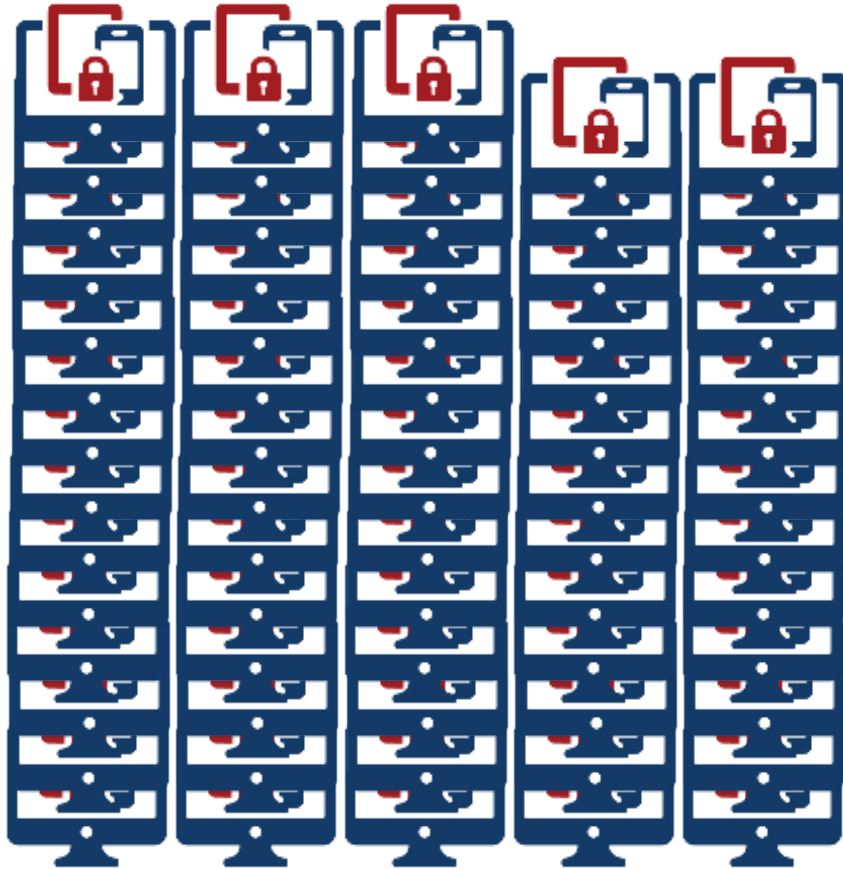


**27 Combat Mission Teams
(Support Combatant Commands)**

Evaluating Mission-Readiness for Cyber Operators at Scale

- Scalable
- Objective
- Reliable
- Valid

DoD Challenge Problem



+25 Support Teams

Evaluating Mission-Readiness for Cyber Operators at Scale

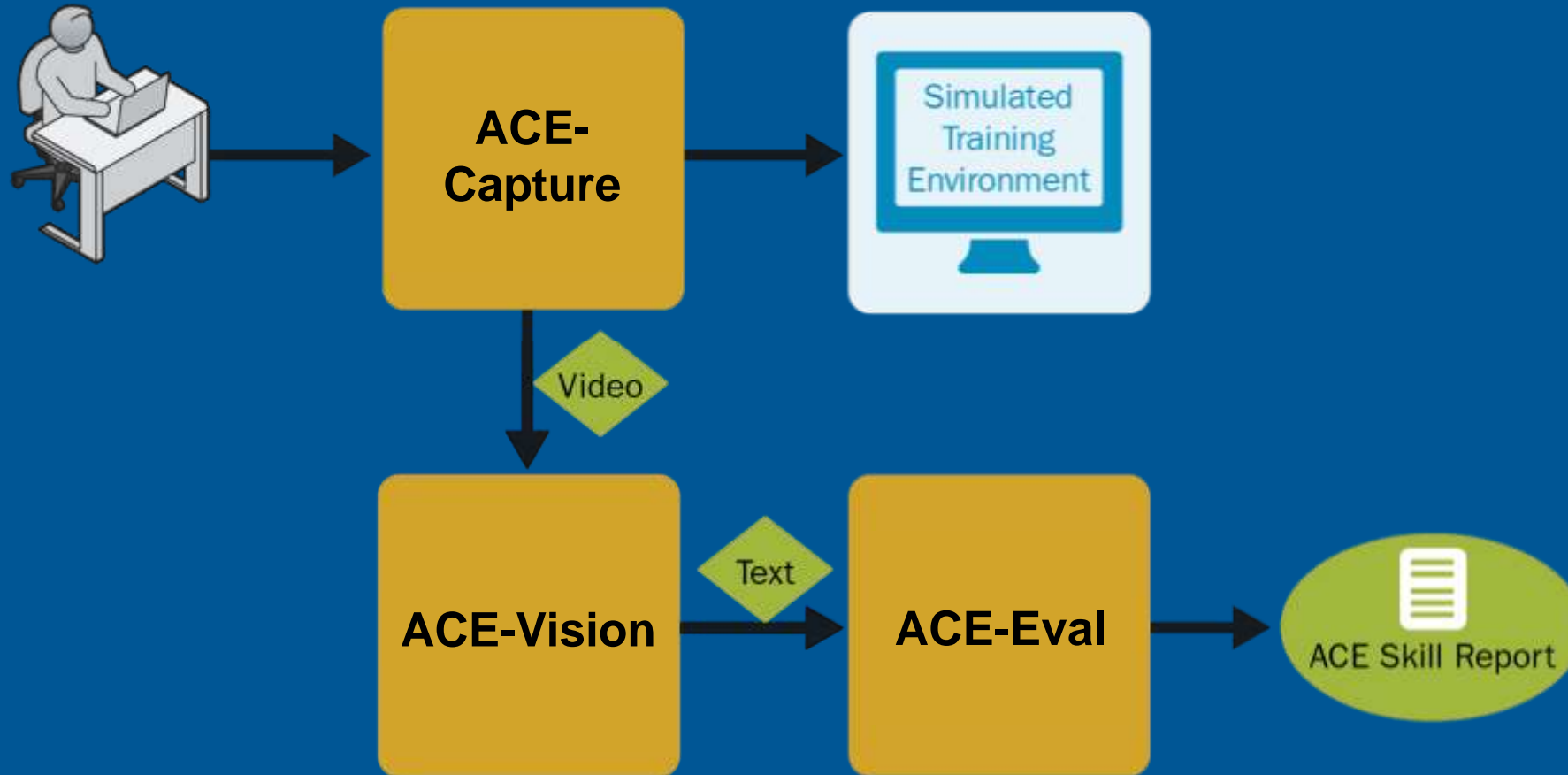
- Scalable
- Objective
- Reliable
- Valid

ACE Philosophy



- **Train as you fight?**
- **Evaluate as you fight!**
 - Place cyber operators in familiar environment
 - Task cyber operators with realistic mission
 - Understand actions taken within scenario
 - Verifiably assess mission-readiness based on actions taken
- **Benefits**
 - Automated analysis
 - Specific deficiencies isolated
 - Automated remediation plans
 - Recording available for future review

ACE Architecture Overview



Role Choice



**Joint Cyberspace Training &
Certification Standards (JCT&CS)**

Forensic Analyst

- 2 Hours
- Existing DoD Standard*
- Self-Contained

* During the course of the project more specific readiness criteria became available

Scenario Development



Scenario I

- **Missing Person**
 - Apartment Searched
 - Laptop Drive Recovered
 - Foul Play Suspected

Scenario II

- **Classified* Documents Exfiltrated**
 - Documents In Enemy Hands
 - Source Organization Drives Imaged
 - Multiple Layers
 - APT1
 - USB
 - Personal Email

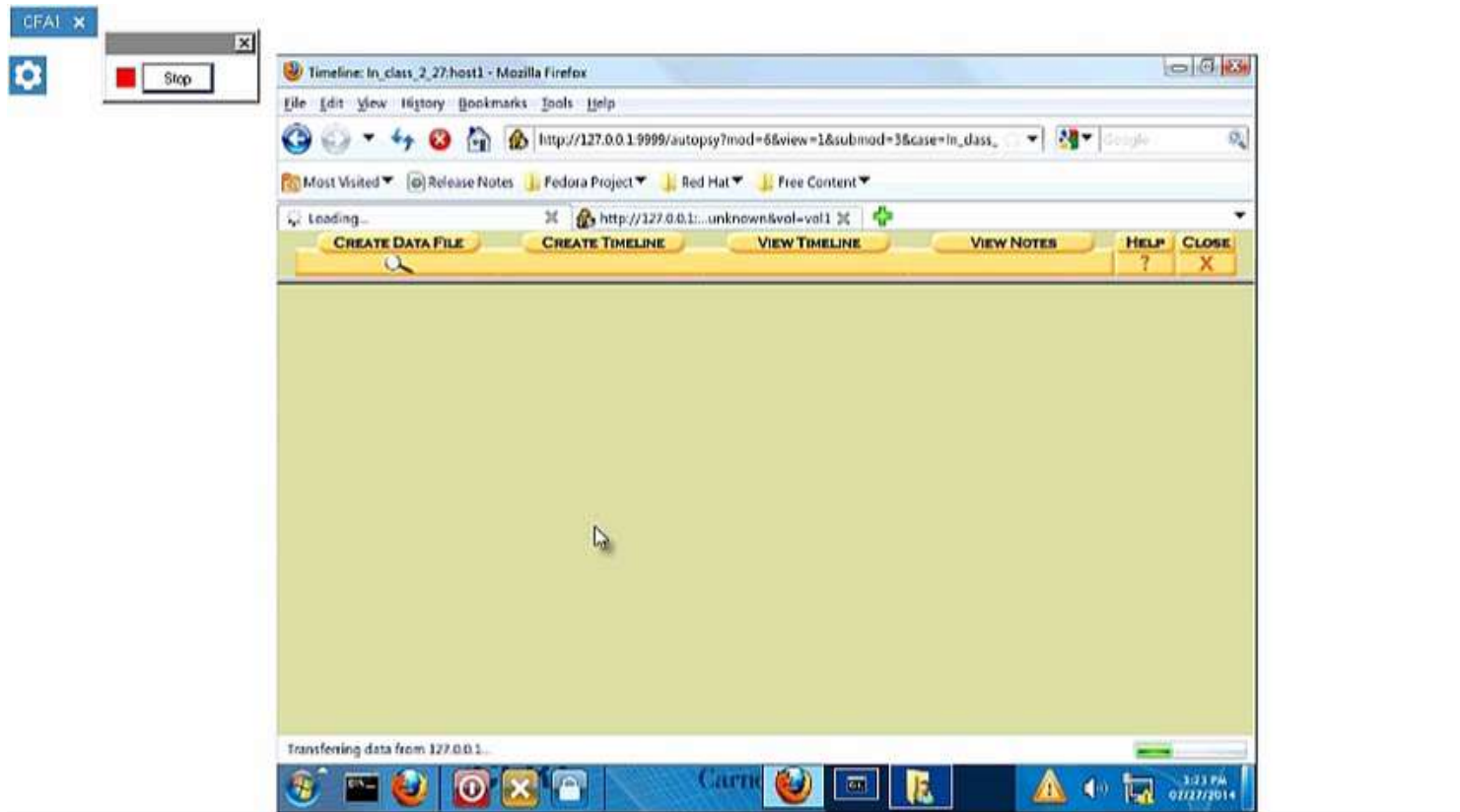
* Classified for evaluation use – not actual classified information.

Data Collection Capability



- Background Data Collection
- Restricted to Environment
- Scalable

Data Collection Capability



Multiple Sources (Increase Dataset Robustness)

- CERT Staff
- CMU Graduate Students
- DoD Personnel
 - Multiple Collections
- NCFTA Personnel



Primary Collaborator:
Professor Yaser Sheik

CMU Robotics Institute, Graphics Lab

Custom Detection System

Designed for massive parallelization

Optimized for use case:

- Maximize pre-process capability
- Minimize duplicate calculations

- Original: $O(nN)$
 - Infeasible for our problem set.
- Optimized: $O(N\log N)$ time.
 - Implemented on GPU array.

Note: Our data set uses high resolution images and so $n \gg \log N$

ACE-Vision - Results



Primary Collaborator:
Professor Yaser Sheik

CMU Robotics Institute, Graphics Lab

Custom Detection System

Custom system running on octoputer hardware

- Faster-than-realtime analysis
- May allow for streaming analysis (not in scope)

ACE-Eval



Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Development

- Requires Categorized Data
 - Evaluator driven categorization (Training data)
 - Hybrid solution required
 - Differing KSA Complexity
 - Simple Binary Detection
 - Path Analysis
 - Hidden Markov Models
 - Frequency Analysis
 - Automated Anomaly Detection
 - Human Intervention

ACE-Eval



Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Development

- Data Tagging system
 - Allow subject matter experts (SME) to categorize data
- Several iterations of machine learning solutions
 - Revealed problems in dataset

ACE-Eval



Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Challenges

- Signal to noise ratio in data is much lower than expected
 - Need larger dataset
- Available personnel are very limited
 - Order of magnitude difference

ACE-Eval



Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Challenges

- Signal to noise ratio in data is much lower than expected
 - Need larger dataset
- Available personnel are very limited
 - Order of magnitude difference

Adaptation



Changing Problem

- Better standards definitions available
 - 1000/2000 Level tasks
 - Specific skills and activities isolated
- Gate-Based assessment possible
 - ML solution no longer required

Adaptation



Gate-Based Assessment

- Custom Web-app created
 - Allow capture of KSA / Level tasks
 - Nested abilities
 - Linked by Job Role
 - Reusable Templates
 - Bulk Import/Export
 - Designed for merging into evaluation pipeline

Automated Cyber-Readiness Future Work

Future Work



Transition to CPT evaluation

- Compatible for gate-based assessment
- Part of ongoing PWP work
- Job role transition simplified with specific tasking

Future Work



Stand-Alone utility

- Vision system
 - Insider threat detection
 - Analyst Support
 - Dynamic workstation thresholding
 - User study data collection
 - Experimental tool
- User friendly template generation wizard created
 - Requires no domain specific knowledge
 - Simple screen capture will do!