Developing a CC EAL7 Multi-Level Security Capability

By Chris Walsh

Developing a CC EAL7 Capability

- Concept
- Evaluation Strategy
- Evaluation Outcome
- CC Issues

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Tenix Datagate, Inc.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1) ISO/IEC 15408 and supplemented by CCEVS approved methodology for components above EAL 4. This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Interactive Link Data Diode Device
Version 2.1 (P/N FID003)
Evaluation Platform: Not Applicable
Assurance Level: EAL 7 Augmented AVA_CCA.3

Name of CCTL: COACT, Inc. CAFE Laboratory
Date Issued: 30 August 2005
Validation Report Number: CCEVS-VR-05-0119
Protection Profile Identifier: None

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Information Assurance Director
National Security Agency

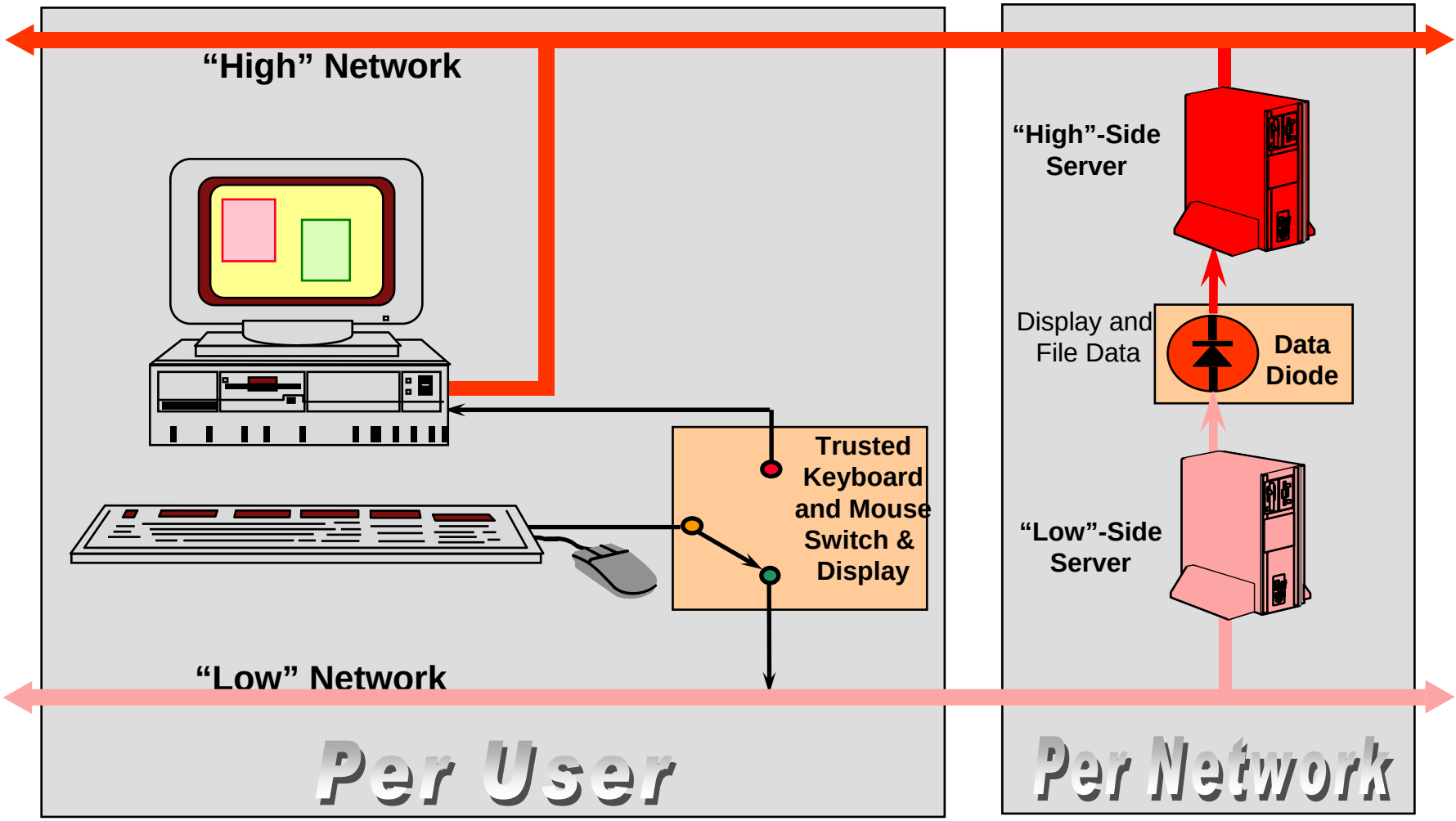
Concept

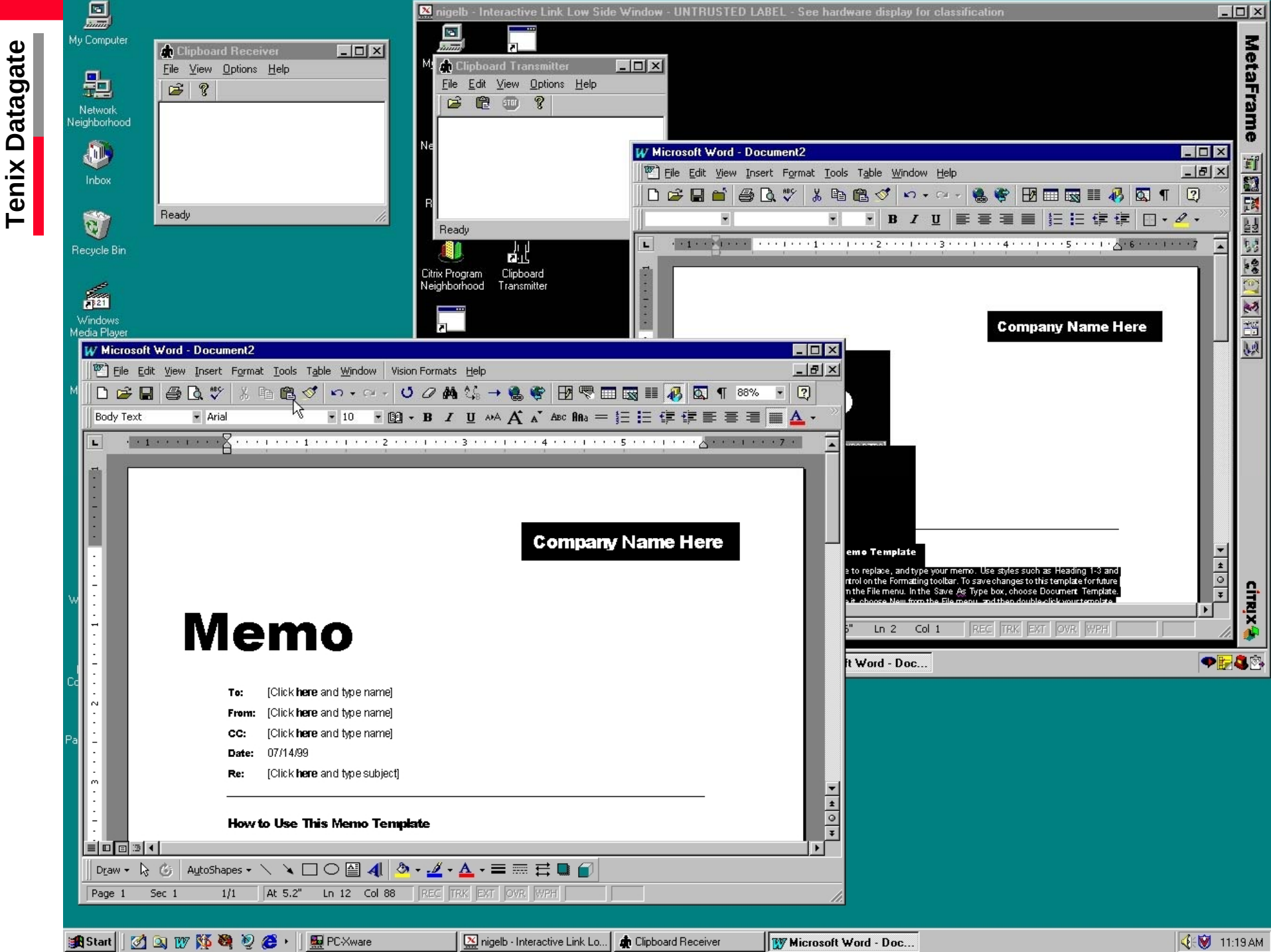
- **Requirements**
  - **Australian Defence Force**
    - **Starlight Program**
  - **Highest Levels of Assurance**
  - **Functionality based on Multiple Single Layers**
  - **Provide High Assurance Secure Solution with COTS Systems**
  - **Clip-on Security products.**

Interactive Link Overview

- **Enables a desktop computer/workstation connected to a High Side Network to also access a Low Side Network while maintaining the Confidentiality of the High Side Data.**

Interactive Link Architecture




Tenix Datagate
My Computer
Network Neighborhood
Inbox
Recycle Bin
Windows Media Player
Clipboard Receiver
File View Options Help
Ready
nigelb - Interactive Link Low Side Window - UNTRUSTED LABEL - See hardware display for classification
Clipboard Transmitter
File Edit View Options Help
Ready
Citrix Program Neighborhood
Clipboard Transmitter
Microsoft Word - Document2
File Edit View Insert Format Tools Table Window Help
Company Name Here
Microsoft Word - Document2
File Edit View Insert Format Tools Table Window Vision Formats Help
Body Text
Arial
10
88%
Company Name Here
Memo
To: [Click here and type name]
From: [Click here and type name]
CC: [Click here and type name]
Date: 07/14/99
Re: [Click here and type subject]
How to Use This Memo Template
Draw
AutoShapes
Page 1 Sec 1 1/1 At 5.2" Ln 12 Col 88 REC TRK EXT OVR WPH
Ln 2 Col 1 REC TRK EXT OVR WPH
MetaFrame
CITRIX
Start
PC-Xware
nigelb - Interactive Link Lo...
Clipboard Receiver
Microsoft Word - Doc...
11:19 AM

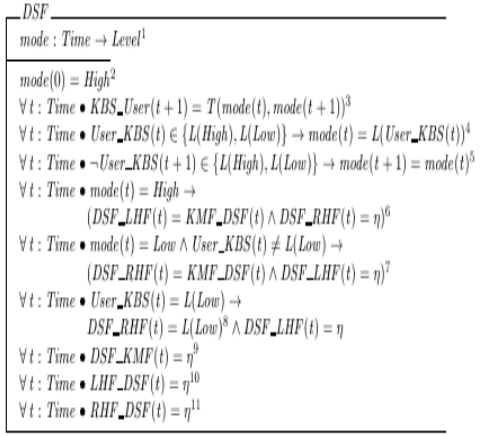
Evaluation Strategy

- **Development Model**
  - **Approach Consecutive vs Concurrent**
  - **Development environment**
    - **Programming Language**
    - **Configuration Management**
    - **Developers Security**
  - **Lifecycle Model**
    - **The hardware was developed based on Waterfall model with feedback.**
    - **The software was developed based on the Boehm Spiral Model**

Evaluation Strategy (Cont.)

Development Model (Cont.)

- **Structured Analysis**
  - **Using the Yourdon method as opposed to a Top down or Bottom up approach.**
  - **The original concept was mapped to the Yourdon functional layer.**
  - **Formal Methods**
    - **Isabella**
    - **Z**



DSF

$mode : Time \rightarrow Level^{1}$

$mode(0) = High^{2}$

$\forall t : Time \bullet KBS\_User(t+1) = T(mode(t), mode(t+1))^{3}$

$\forall t : Time \bullet User\_KBS(t) \in \{L(High), L(Low)\} \rightarrow mode(t) = L(User\_KBS(t))^{4}$

$\forall t : Time \bullet \neg User\_KBS(t+1) \in \{L(High), L(Low)\} \rightarrow mode(t+1) = mode(t)^{5}$

$\forall t : Time \bullet mode(t) = High \rightarrow (DSF\_LHF(t) = KMF\_DSF(t) \wedge DSF\_RHF(t) = \eta)^{6}$

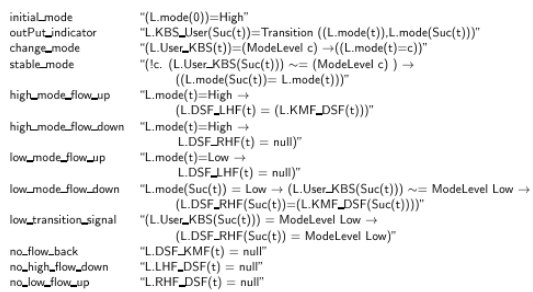
$\forall t : Time \bullet mode(t) = Low \wedge User\_KBS(t) \neq L(Low) \rightarrow (DSF\_RHF(t) = KMF\_DSF(t) \wedge DSF\_LHF(t) = \eta)^{7}$

$\forall t : Time \bullet User\_KBS(t) = L(Low) \rightarrow DSF\_RHF(t) = L(Low)^{8} \wedge DSF\_LHF(t) = \eta$

$\forall t : Time \bullet DSF\_KMF(t) = \eta^{9}$

$\forall t : Time \bullet LHF\_DSF(t) = \eta^{10}$

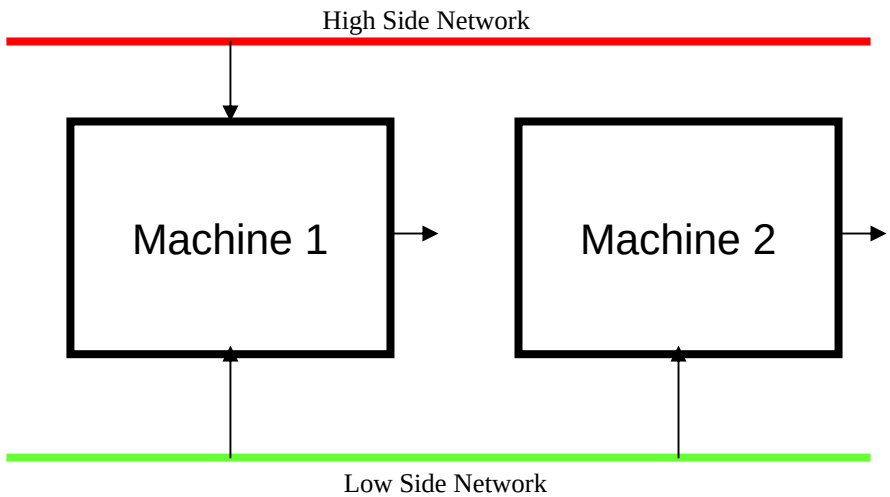
$\forall t : Time \bullet RHF\_DSF(t) = \eta^{11}$



initial_mode	"(L.mode(0))=High"
outPut_indicator	"L.KBS_User(Suc(t))=Transition ((L.mode(t)),L.mode(Suc(t)))"
change_mode	"(L.User_KBS(t))=(ModeLevel c) →((L.mode(t)=c))"
stable_mode	"(!c. (L.User_KBS(Suc(t))) ~= (ModeLevel c)) → ((L.mode(Suc(t))= L.mode(t)))"
high_mode_flow_up	"L.mode(t)=High → (L.DSF_LHF(t) = (L.KMF_DSF(t)))"
high_mode_flow_down	"L.mode(t)=High → L.DSF_RHF(t) = null)"
low_mode_flow_up	"L.mode(t)=Low → L.DSF_LHF(t) = null)"
low_mode_flow_down	"L.mode(Suc(t)) = Low → (L.User_KBS(Suc(t))) ~= ModeLevel Low → (L.DSF_RHF(Suc(t))=(L.KMF_DSF(Suc(t))))"
low_transition_signal	"(L.User_KBS(Suc(t))) = ModeLevel Low → (L.DSF_RHF(Suc(t)) = ModeLevel Low)"
no_flow_back	"L.DSF_KMF(t) = null"
no_high_flow_down	"L.LHF_DSF(t) = null"
no_low_flow_up	"L.RHF_DSF(t) = null"

Evaluation Strategy (Cont.)

- **Formal Model**
  - **Non-Interference**



- **Simple Confidentiality – Not appropriate**

Evaluation Strategy (Cont.)

- Evaluation Methodology
- Security Functionality
  - Protection Profile
  - CIA
    - Confidentiality
    - Integrity
    - Availability
  - CC Part 2
    - User Data Protection (FDP)
    - Security Management (FMT)
    - Protection of the TSF (FPT)
    - Extended Requirements (EXT)
  - Hardware

Evaluation Outcome

- Vulnerability Assessment
- Rework
- Supporting Security Functionality for Operational environments
  - Content filter
  - Firewall
  - Hardened O/S

Tenix

CC Issues

- Correlation of Formal Security Functionality and Semi-formal HLD LLD and IMP
- EAL7 security functionality implemented in Hardware
- EAL7 Security functionality – Confidentiality Only
- Can Security functions have a SoF at EAL7

Questions

Chris Walsh

Tenix Datagate Pty Ltd

chris.walsh@tenix.com

http://www.tenixdatagate.com