

# Ten years of Layered Assurance at Galois, lessons learned, and looking forward

Dylan McNamee  
Galois, Inc.

*dylan@galois.com*

Layered Assurance Workshop

December 7, 2015

| galois |

- How Galois got here
- Some lessons we learned
  - implementation language factors
  - decomposition surprises
  - managing theorem proving
  - complex path to market
- Some challenges we see

# Market opportunity: bad reference monitors



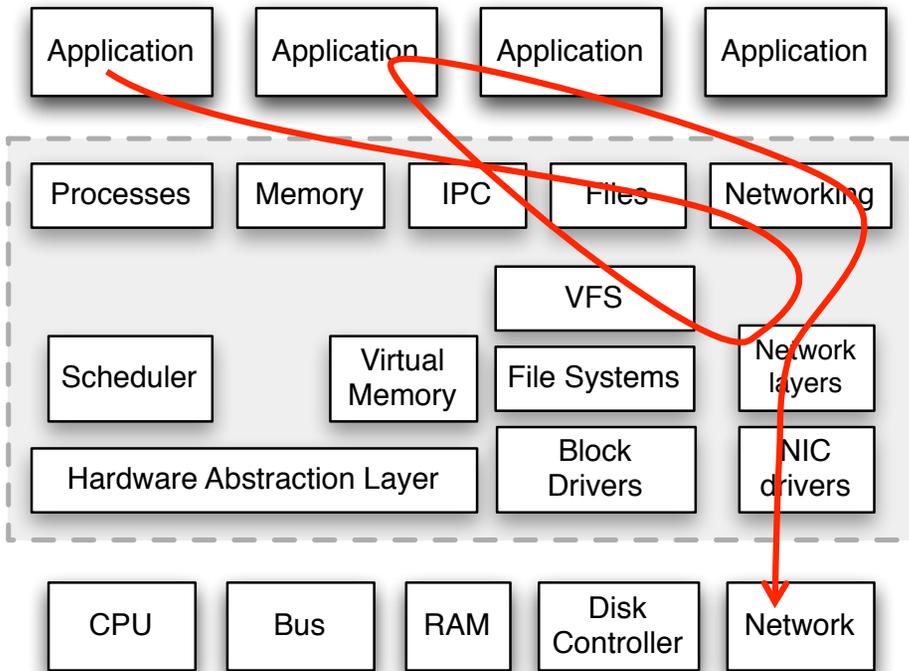
# Another bad reference monitor



# Motivation for MILS' approach to reference monitors

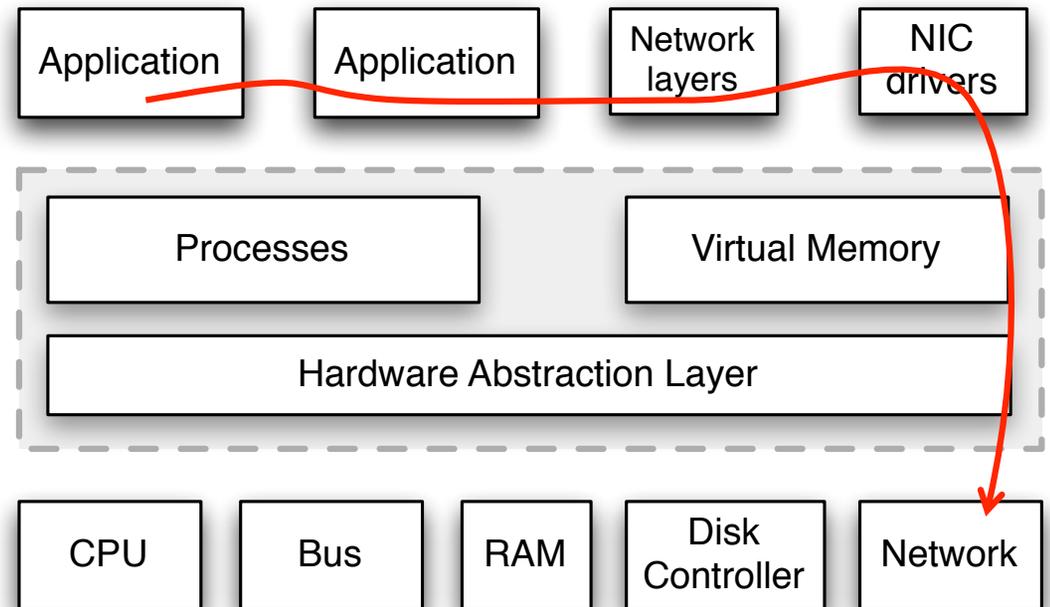
## Monolithic OS approach

**Secure domain**

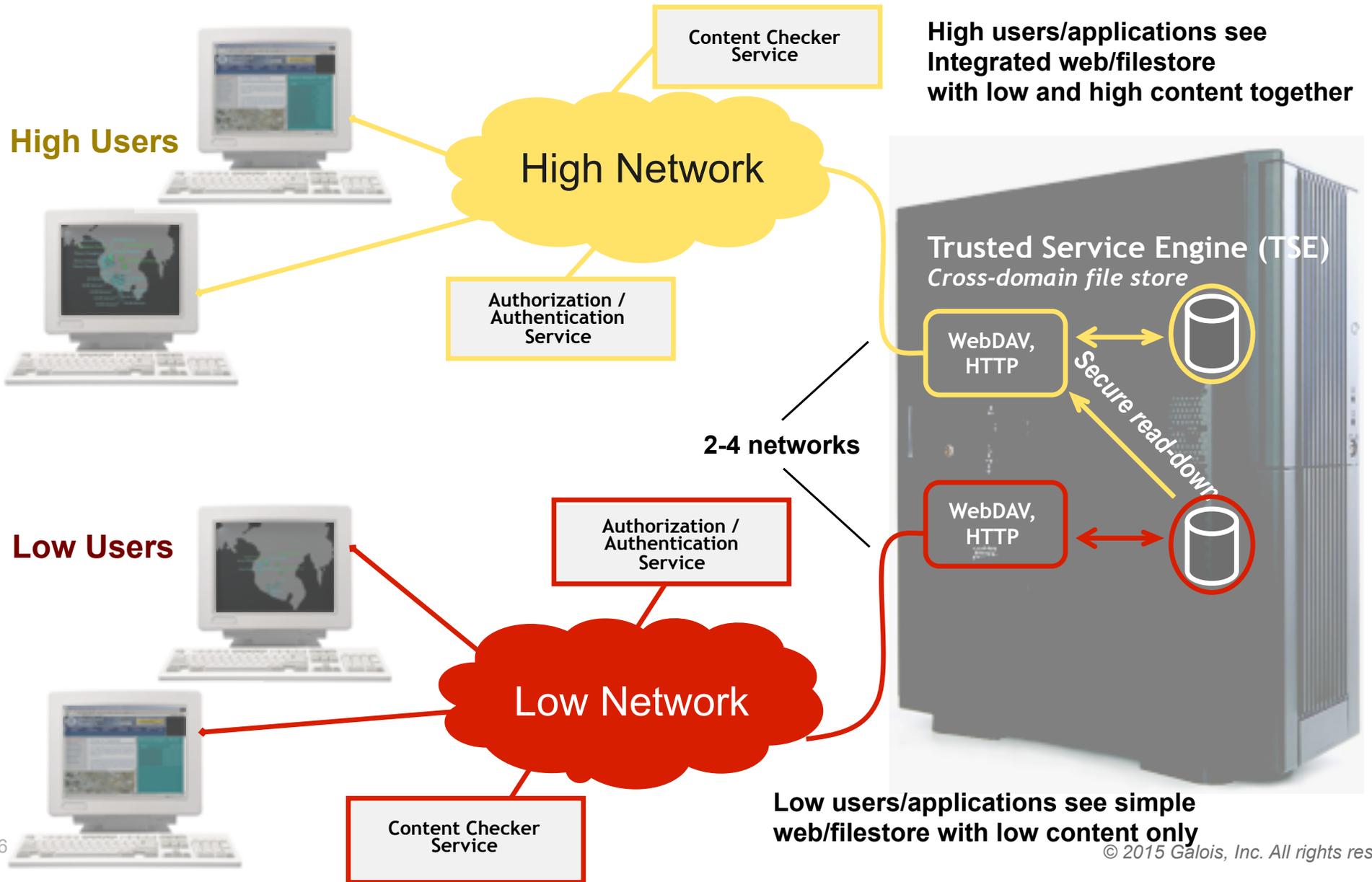


## MILS approach

**Secure domain**



# The Trusted Services Engine (TSE)



- *breathtaking demo goes here*

The screenshot shows a web browser window displaying the DHS Threats & Protection portal. The browser's address bar shows the URL `http://192.168.66.128:8010/portal.html`. The page features the DHS logo and the text "Homeland Security". A "THREAT ADVISORY" banner indicates an "ELEVATED" risk of terrorist attacks. A navigation menu includes links for "DHS Org", "Emergencies & Disasters", "Travel & Transportation", "Immigration & Borders", "Research & Technology", "Threats & Protection", "Working with DHS", and "Press Room". The "Threats & Protection" section is active, displaying a sub-header "Threats & Protection" and a main heading "Synthesizing and Disseminating Information". Below this, there are two paragraphs of text describing the department's mission and responsibilities. To the right, a "LATEST NEWS" section contains a link to "Read More" regarding a press conference. On the far right, a directory listing for threats is shown, listing document names and their associated networks.

**THREAT ADVISORY**  
**ELEVATED** Significant Risk of Terrorist Attacks.

**Threats & Protection**

**Synthesizing and Disseminating Information**

The Department of Homeland Security merges under one roof the capability to anticipate, preempt and deter threats to the homeland whenever possible, and the ability to respond quickly when such threats do materialize.

The department is responsible for assessing the vulnerabilities of the nation's critical infrastructure and cyber security threats and takes the lead in evaluating these vulnerabilities and coordinating

**LATEST NEWS**

Remarks by Secretary of Homeland Security Tom Ridge, Governor of New York George Pataki and Mayor of New York City Michael Bloomberg at a Press Conference Regarding Security at the Republican National Convention  
[Read More](#)

**Directory listing for : Threats/**

Name	Networks/<Cla
<a href="#">LOW!SA04-184A.doc</a>	<COALITION
<a href="#">LOW!SA04-196A.doc</a>	<COALITION
<a href="#">LOW!SA04-208A.doc</a>	<COALITION
<a href="#">LOW!SA04-212A.doc</a>	<COALITION
<a href="#">LOW!SA04-243A.doc</a>	<COALITION
<a href="#">LOW!SA04-258A.doc</a>	<COALITION
<a href="#">LOW!SA04-261A.doc</a>	<COALITION

The screenshot shows a web browser window with two tabs. The active tab is at `http://192.168.197.128:8010/LOW!portal.html`. The browser's address bar shows the URL `192.168.197.128:8010/LOW!portal.html`. The page header features the DHS logo and the text "Homeland Security". A search bar contains the text "keyword". A "THREAT ADVISORY" box displays "ELEVATED" with a color-coded bar and the text "Significant Risk of Terrorist Attacks." Below the header is a navigation menu with links for "DHS Org", "Emergencies & Disasters", "Travel & Transportation", "Immigration & Borders", "Research & Technology", "Threats & Protection", "Working with DHS", and "Press Room". The "Threats & Protection" section is active, showing a sub-header "Threats & Protection" and a main heading "Synthesizing and Disseminating Information". The text below explains the department's role in anticipating and responding to threats. A "LATEST NEWS" section contains a link to "Remarks by Secretary of Homeland Security Tom Ridge, Governor of New York George Pataki and Mayor of New York City Michael Bloomberg at a Press Conference Regarding Security at the Republican National Convention" with a "Read More" link. On the right, a "Directory listing for : Threats/" section lists various document files with their names and network paths. At the bottom, an aerial photograph of an industrial or military facility is visible, with a file path `192.168.197.128:8010/Threats/SA04-254D-note.doc` overlaid at the bottom left.

**THREAT ADVISORY**  
**ELEVATED** ■ ■ ■ ■  
 Significant Risk of Terrorist Attacks.

- DHS Org
- Emergencies & Disasters
- Travel & Transportation
- Immigration & Borders
- Research & Technology
- Threats & Protection
- Working with DHS
- Press Room

- Threats & Protection**
- ▶ Advisory System
- ▶ Security & Protection
- ▶ Critical Infrastructure
- ▶ Home & Community
- ▶ Banking & Finance
- ▶ Health & Safety

## Threats & Protection

### Synthesizing and Disseminating Information

The Department of Homeland Security merges under one roof the capability to anticipate, preempt and deter threats to the homeland whenever possible, and the ability to respond quickly when such threats do materialize.

The department is responsible for assessing the vulnerabilities of the nation's critical infrastructure and cyber security threats and takes the lead in evaluating these vulnerabilities and coordinating with other federal, state, local, and private entities to ensure the

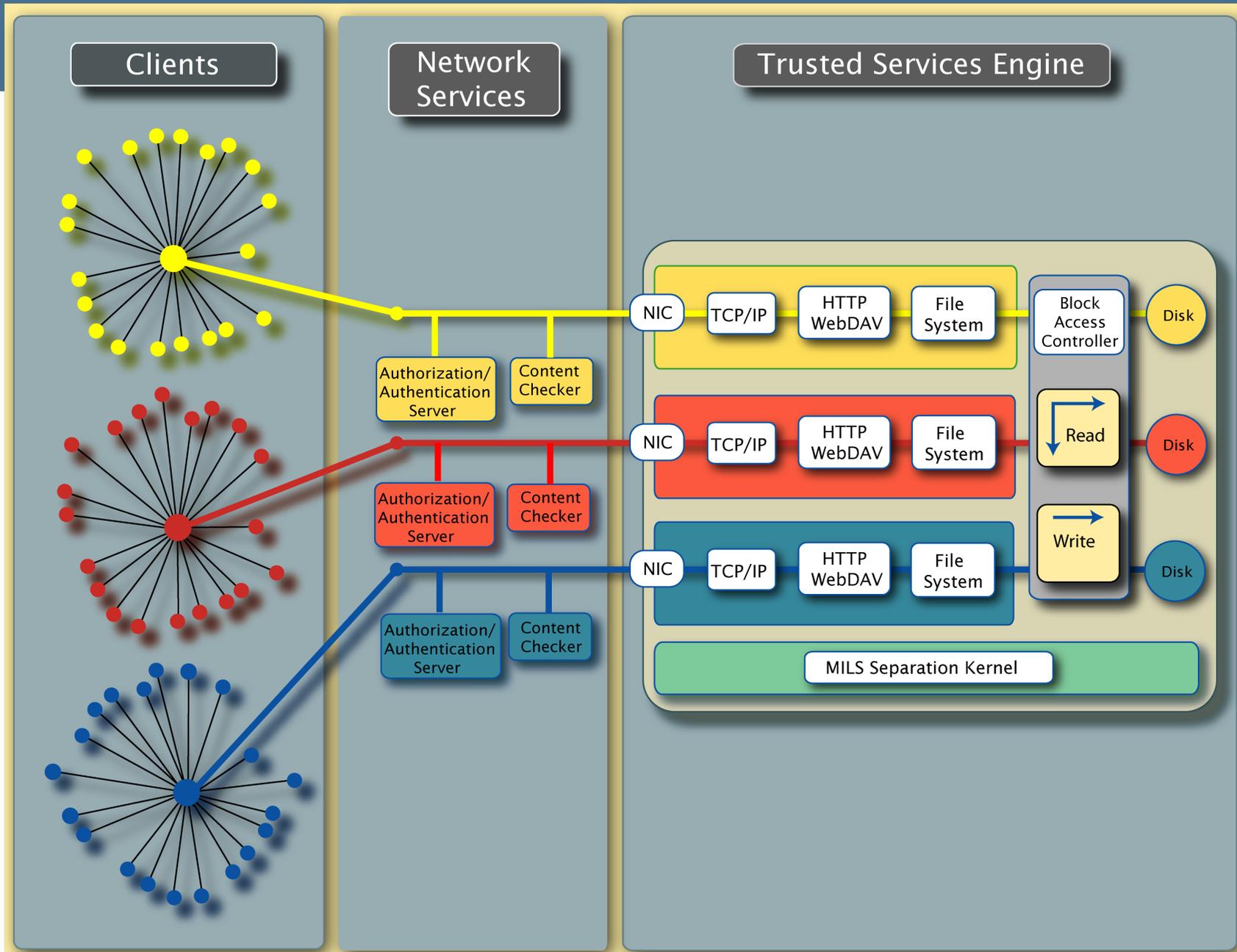
### LATEST NEWS

Remarks by Secretary of Homeland Security Tom Ridge, Governor of New York George Pataki and Mayor of New York City Michael Bloomberg at a Press Conference Regarding Security at the Republican National Convention  
[Read More](#)

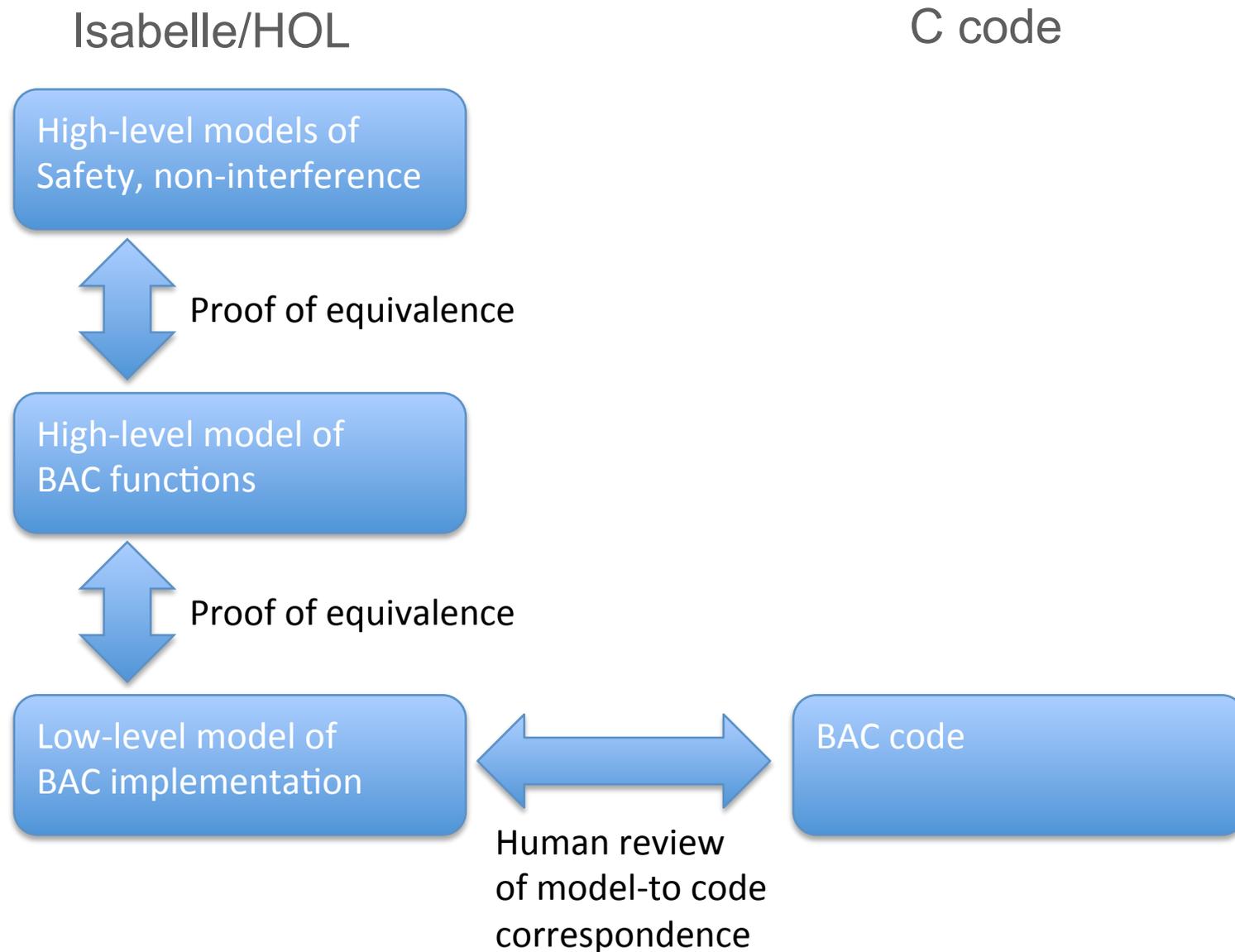
**Directory listing for : Threats/**

Name	Networks
<a href="#">HIGH!SA04-184A-note.doc</a>	<TOP S
<a href="#">LOW!SA04-184A.doc</a>	<COALI
<a href="#">LOW!SA04-196A.doc</a>	<COALI
<a href="#">LOW!SA04-208A.doc</a>	<COALI
<a href="#">HIGH!SA04-212A-note.doc</a>	<TOP S
<a href="#">LOW!SA04-212A.doc</a>	<COALI
<a href="#">LOW!SA04-243A.doc</a>	<COALI
<a href="#">MEDIUM!SA04-250A.doc</a>	<US
<a href="#">HIGH!SA04-254B-note.doc</a>	<TOP S
<a href="#">HIGH!SA04-254C-note.doc</a>	<TOP S
<a href="#">HIGH!SA04-254D-note.doc</a>	<TOP S
<a href="#">HIGH!SA04-254E-note.doc</a>	<TOP S
<a href="#">HIGH!SA04-258A-note.doc</a>	<TOP S
<a href="#">LOW!SA04-258A.doc</a>	<COALI

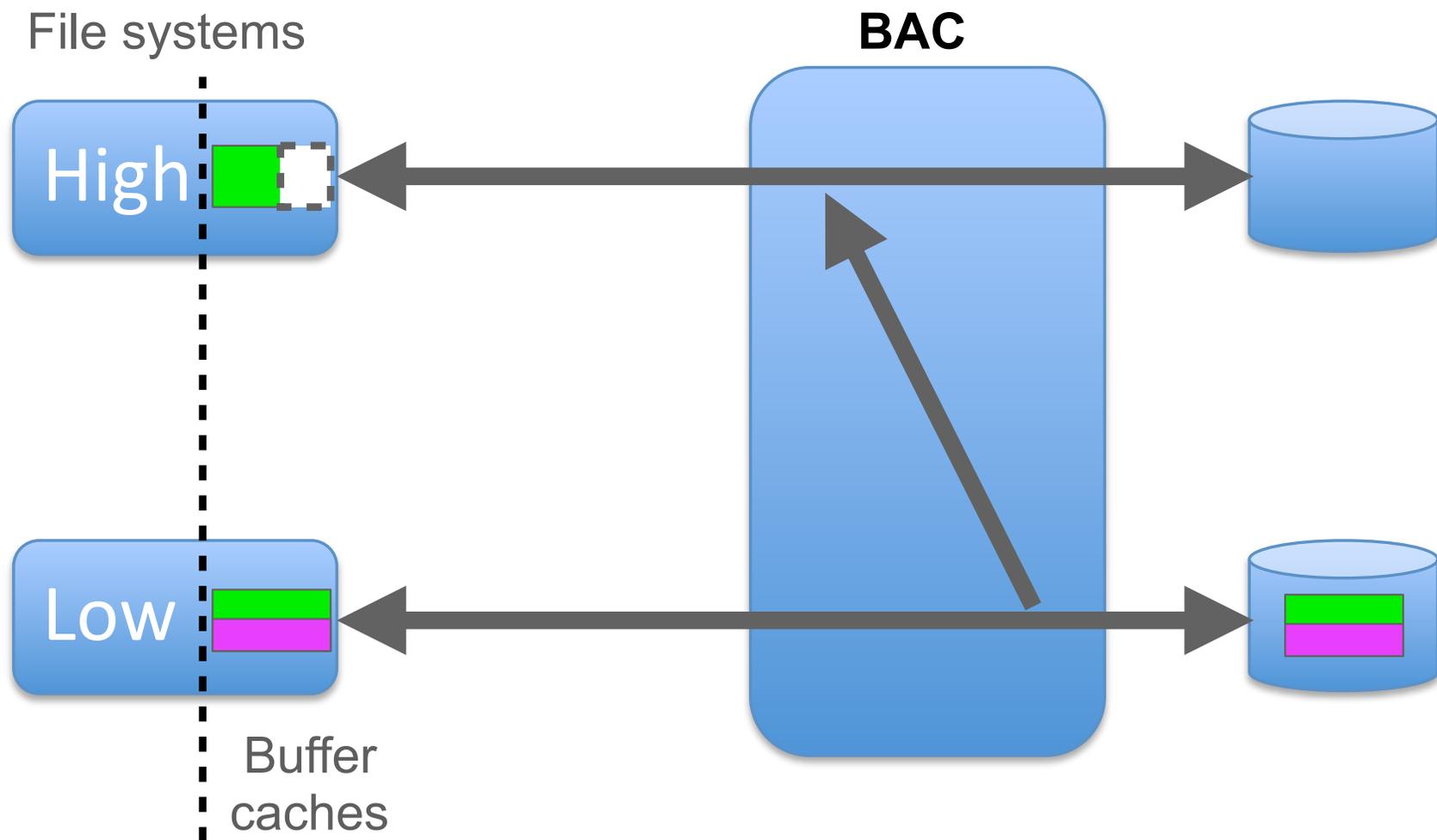




# Block Access Controller assurance



# A surprise challenge: consistency across domains



# A shifting landscape of software evaluation, certification and accreditation

1985

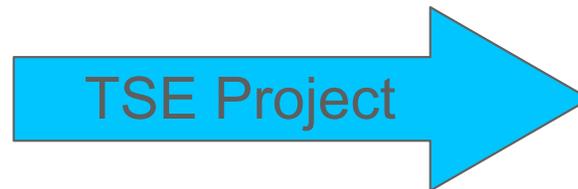


2005

**U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness**  
Version 1.03



Information Assurance Directorate



2009

NIST Special Publication 800-53  
Revision 4  
**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Security and Privacy Controls  
for Federal Information Systems  
and Organizations

JOINT TASK FORCE  
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

INITIAL PUBLIC DRAFT

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

February 2012



U.S. Department of Commerce  
John E. Bryson, Secretary

National Institute of Standards and Technology  
Patrick D. Gallagher, Under Secretary for Standards and Technology  
and Director

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# Operating system options



**GENERAL DYNAMICS**  
C4 Systems



## WIND RIVER

GNAT Pro High-Integrity for MILS



# Some lessons we learned

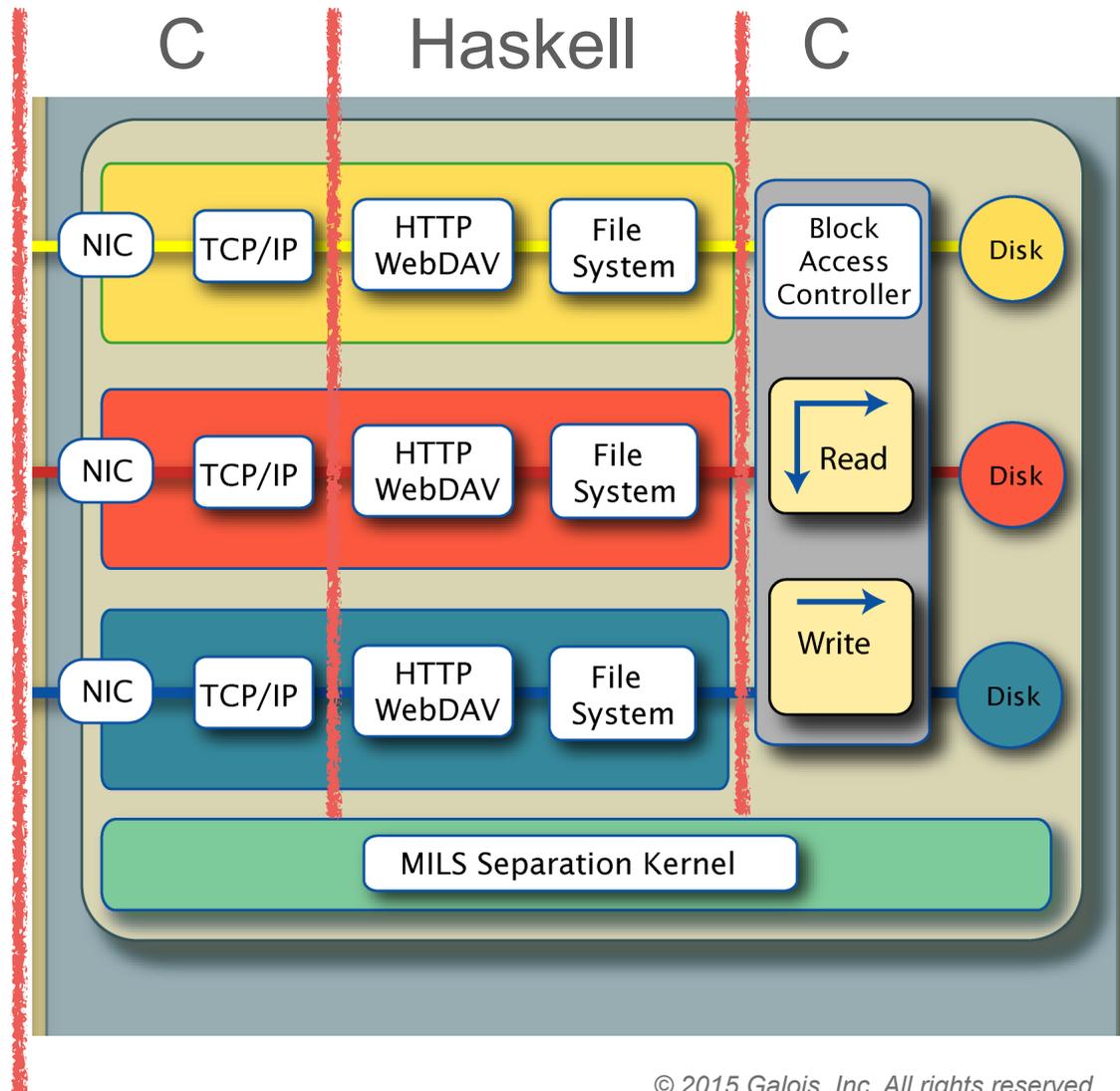
Implementation language

Decomposition can surprise

Theorem proving is hard

Communication is harder

Evaluation, certification and accreditation is bewildering



# Applying lessons learned

- Tearline wiki
- Federated search
- Separation Kernel SBIR
- Trusted handheld

# Applying lessons learned: SMACCCMPilot



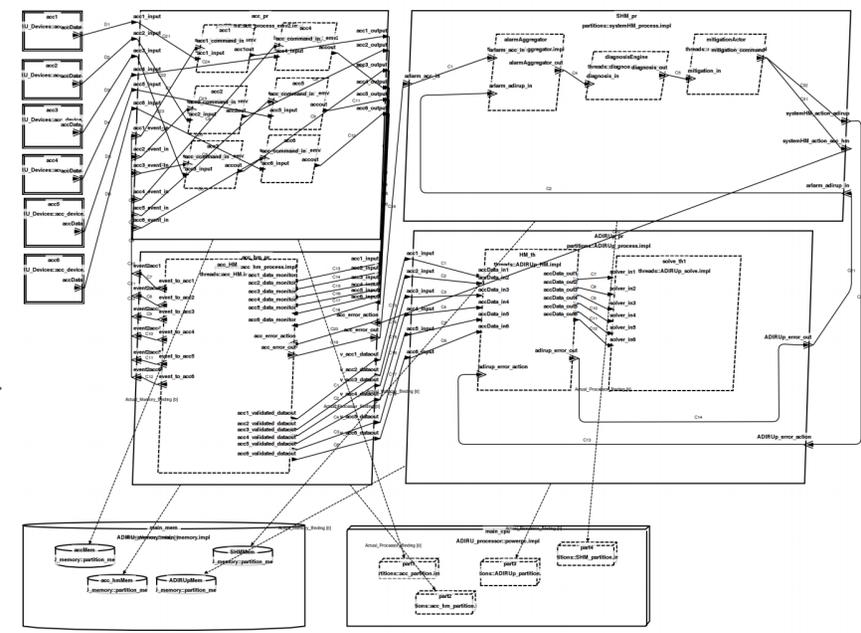
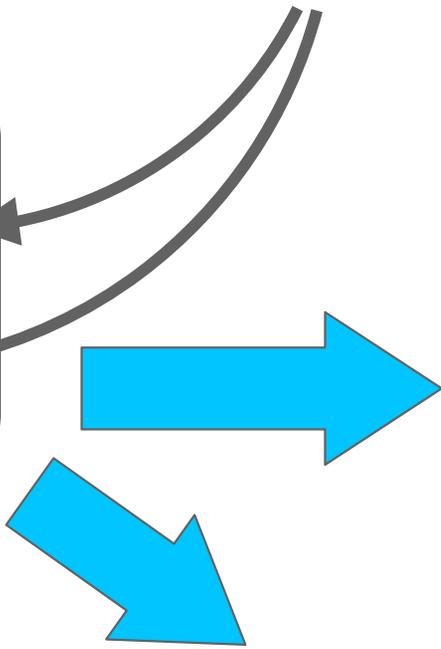
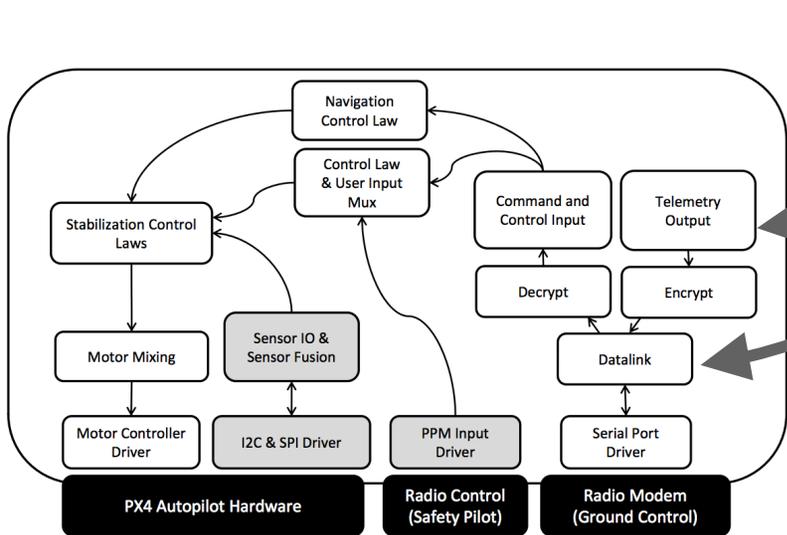
<http://www.cbsnews.com/videos/creating-drones-that-cant-be-hacked/>

# Applying lessons learned: SMACCPilot

Architecture specification in Tower

Component specifications in Ivory

Generated AADL model



Generated implementation

```

#define DBG(...)
#define LOG(...)
#define LOGE(...)
#define LOGF(...)
#define LOGI(...)
#define LOGW(...)
#define LOGD(...)
#define LOGV(...)
#define LOGN(...)
#define LOGO(...)
#define LOGP(...)
#define LOGQ(...)
#define LOGR(...)
#define LOGS(...)
#define LOGT(...)
#define LOGU(...)
#define LOGV(...)
#define LOGW(...)
#define LOGX(...)
#define LOGY(...)
#define LOGZ(...)
#define LOGAA(...)
#define LOGAB(...)
#define LOGAC(...)
#define LOGAD(...)
#define LOGAE(...)
#define LOGAF(...)
#define LOGAG(...)
#define LOGAH(...)
#define LOGAI(...)
#define LOGAJ(...)
#define LOGAK(...)
#define LOGAL(...)
#define LOGAM(...)
#define LOGAN(...)
#define LOGAO(...)
#define LOGAP(...)
#define LOGAQ(...)
#define LOGAR(...)
#define LOGAS(...)
#define LOGAT(...)
#define LOGAU(...)
#define LOGAV(...)
#define LOGAW(...)
#define LOGAX(...)
#define LOGAY(...)
#define LOGAZ(...)
#define LOGBA(...)
#define LOGBB(...)
#define LOGBC(...)
#define LOGBD(...)
#define LOGBE(...)
#define LOGBF(...)
#define LOGBG(...)
#define LOGBH(...)
#define LOGBI(...)
#define LOGBJ(...)
#define LOGBK(...)
#define LOGBL(...)
#define LOGBM(...)
#define LOGBN(...)
#define LOGBO(...)
#define LOGBP(...)
#define LOGBQ(...)
#define LOGBR(...)
#define LOGBS(...)
#define LOGBT(...)
#define LOGBU(...)
#define LOGBV(...)
#define LOGBW(...)
#define LOGBX(...)
#define LOGBY(...)
#define LOGBZ(...)
#define LOGCA(...)
#define LOGCB(...)
#define LOGCC(...)
#define LOGCD(...)
#define LOGCE(...)
#define LOGCF(...)
#define LOGCG(...)
#define LOGCH(...)
#define LOGCI(...)
#define LOGCJ(...)
#define LOGCK(...)
#define LOGCL(...)
#define LOGCM(...)
#define LOGCN(...)
#define LOGCO(...)
#define LOGCP(...)
#define LOGCQ(...)
#define LOGCR(...)
#define LOGCS(...)
#define LOGCT(...)
#define LOGCU(...)
#define LOGCV(...)
#define LOGCW(...)
#define LOGCX(...)
#define LOGCY(...)
#define LOGCZ(...)
#define LOGDA(...)
#define LOGDB(...)
#define LOGDC(...)
#define LOGDD(...)
#define LOGDE(...)
#define LOGDF(...)
#define LOGDG(...)
#define LOGDH(...)
#define LOGDI(...)
#define LOGDJ(...)
#define LOGDK(...)
#define LOGDL(...)
#define LOGDM(...)
#define LOGDN(...)
#define LOGDO(...)
#define LOGDP(...)
#define LOGDQ(...)
#define LOGDR(...)
#define LOGDS(...)
#define LOGDT(...)
#define LOGDU(...)
#define LOGDV(...)
#define LOGDW(...)
#define LOGDX(...)
#define LOGDY(...)
#define LOGDZ(...)
#define LOGEA(...)
#define LOGEB(...)
#define LOGEC(...)
#define LOGED(...)
#define LOGEE(...)
#define LOGEF(...)
#define LOGEG...)

```

# Outstanding challenges

- Finding a trustworthy platform to run trusted systems on
  - COTS CPU's are very complex
    - Security mechanisms such as TPMs, IOMMU's, secure enclaves, etc, are important, but *add complexity*
  - trustworthy CPU's are not COTS
  - assurance in the face of multicore is ongoing research
- The market for trustworthy systems is still emerging - *still a hard sell*
  - though the value proposition is (sadly) growing fast
- Complexity is inevitable
  - how to analyze systems with *emergent behavior*

[dylan@galois.com](mailto:dylan@galois.com)

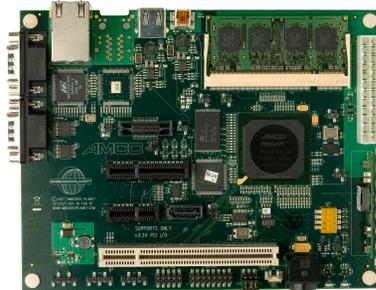


# A shifting hardware landscape

2002



2006



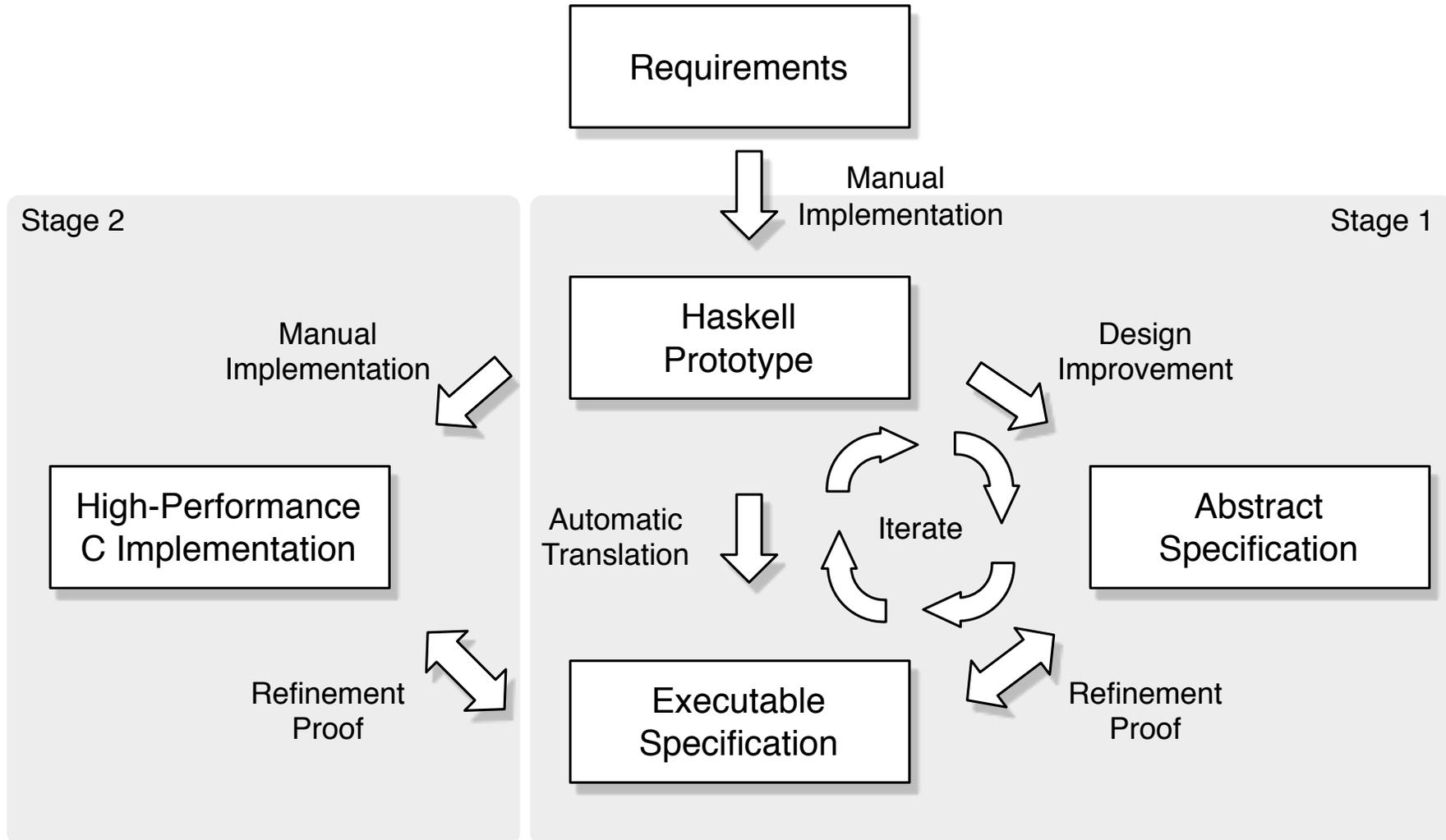
PowerPC

2007



ARM

# NICTA's seL4 design process



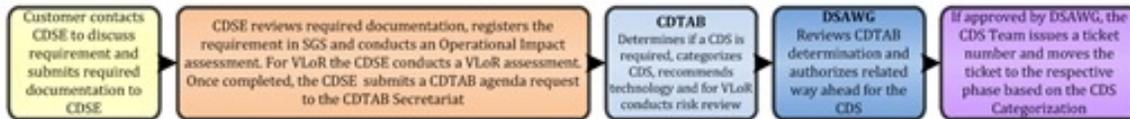
from "Comprehensive Formal Verification of an OS Microkernel" Klein et al, ACM TOCS Feb 2014

# The accreditation process

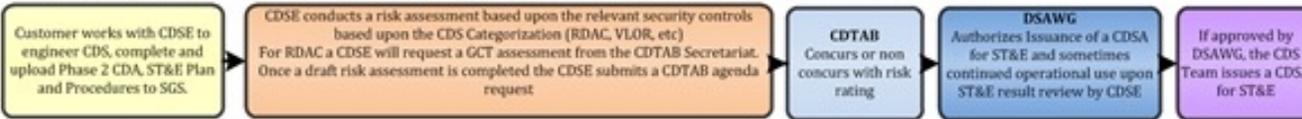
Enterprise Connection Division (NSC)

## DoD Cross Domain Solutions Connection Process Diagram

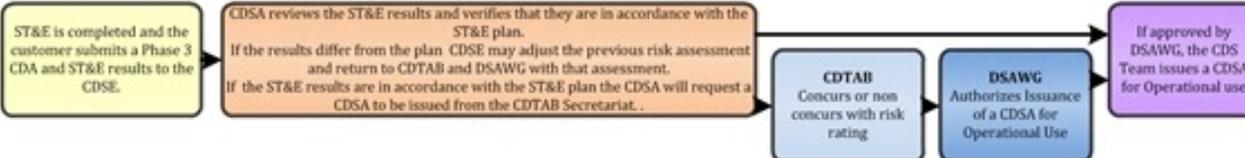
### Phase 1: CDS Categorization and Criticality Determination



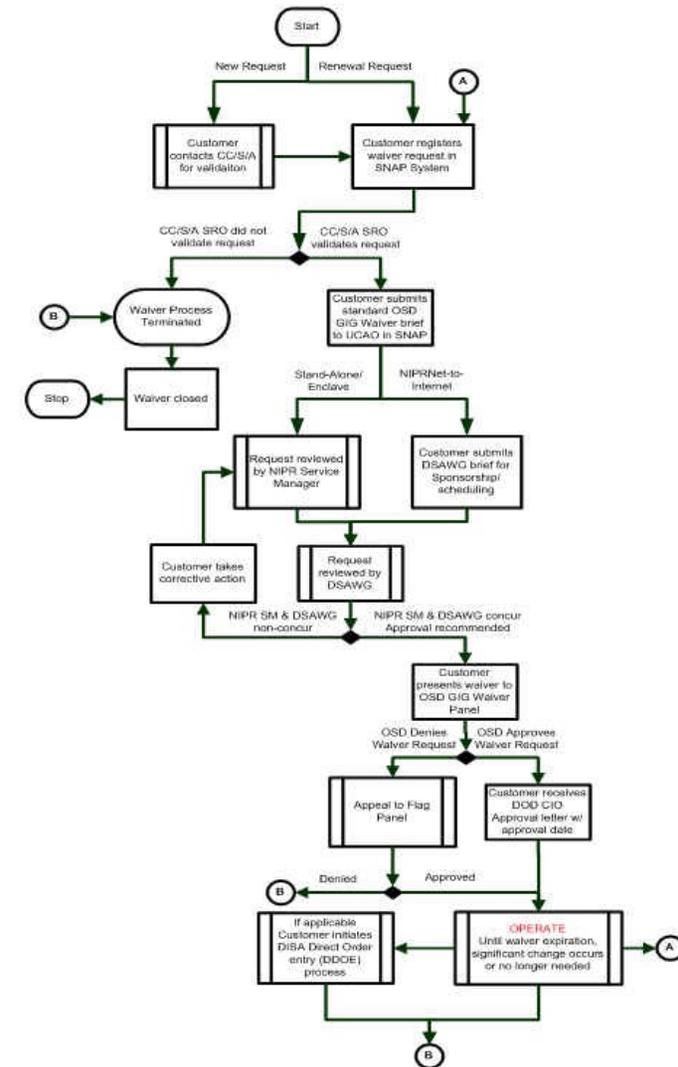
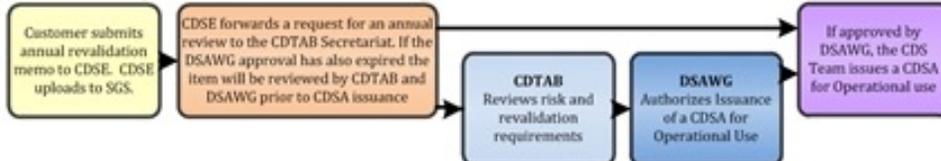
### Phase 2: CDS Engineering, Security Control Selection, and Security Control Implementation



### Phase 3: CDS Security Control Assessment and Authorization



### Phase 4: Operational CDS Monitoring



**Iranian nuclear program - High Wiki - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Address [http://www.galois.com/docserver-demo/high-net/high/index.php/Iranian\\_nuclear\\_program](http://www.galois.com/docserver-demo/high-net/high/index.php/Iranian_nuclear_program)

Google  Go   346 blocked

article discussion edit history

Use this page: [Iranian nuclear program](#)

## Iranian nuclear program hide LOW

The Iranian nuclear program was originally started in the 1950s with the help of the United States. After the **Islamic Revolution** in 1979, the government temporarily disbanded the programme. Iran soon resumed the programme, albeit with less Western assistance than the pre-revolution era. Iran's current nuclear programme consists of several research sites, a uranium mine, a nuclear reactor, and uranium processing facilities that include a uranium enrichment plant. The Iranian government asserts that the programme's only goal is to develop the capacity for peaceful nuclear power generation, and plans to generate 6000 MW of electricity with nuclear power plants by 2010 but some nations believe it covers an attempt to acquire nuclear weapons. As of 2006 nuclear power does not contribute to the Iranian energy grid.

Use this page: [Iranian nuclear program](#)

## Iranian nuclear program show MEDIUM

## Iranian nuclear program hide HIGH

### Nuclear facilities (high) [edit]

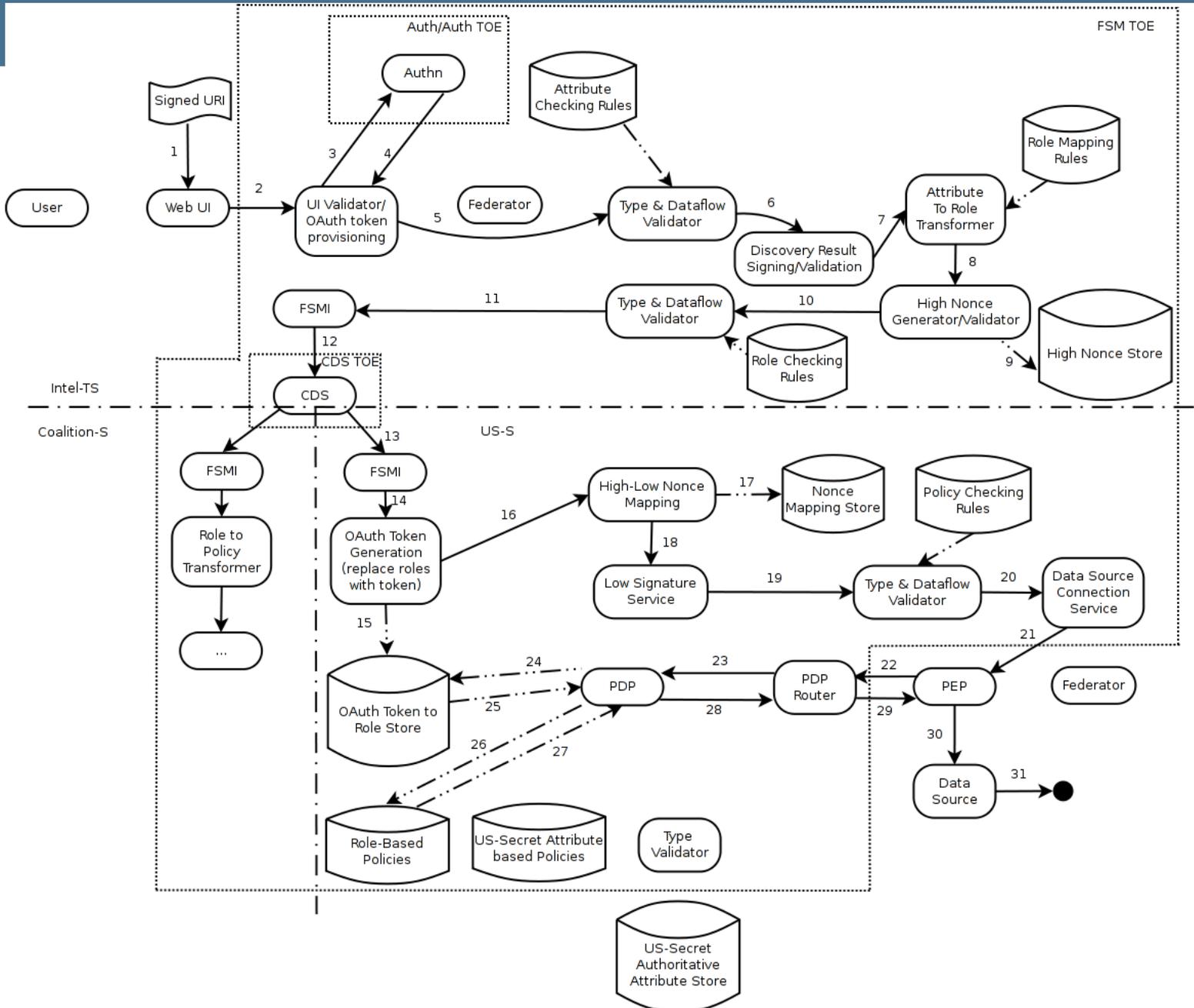
#### Isfahan [edit]

The Uranium Conversion Facility at Isfahan converts yellowcake into uranium hexafluoride. As of late October 2004, the site is 70% operational with 21 of 24 workshops completed. There is also a Zirconium Production Plant (ZPP) located nearby that produces the necessary ingredients and alloys for nuclear reactors.

#### Lavizan [edit]

According to Reuters, claims by the US that topsoil has been removed and the site had been sanitized could not be verified by IAEA investigators who visited Lavizan: Washington accused Iran of removing a substantial amount of topsoil and rubble from the site and replacing it with a new layer of soil, in what U.S. officials said might have been an attempt to cover clandestine nuclear activity at Lavizan. Former U.S. ambassador to the IAEA, Kenneth Brill, accused Iran in June of using "the wrecking ball and bulldozer" to sanitize Lavizan prior to the arrival of U.N. inspectors. But another diplomat close to the IAEA told Reuters that on-site inspections of Lavizan produced no proof

Done Internet



# Trusted handheld project

