#SHAREorg

SHARE
Technology · Connections · Results

The HMC Is a Fantastic Tool But Are You Making it Secure?

Barry Schrager
Xbridge Systems, Inc.

&

Paul R. Robichaux
NewEra Software, Inc.

Monday, February 5 at 12:15 pm
Session Number 12255
Plaza B

SHARE in San Francisco 2013

Abstract and Speakers

• The Hardware Management Console (HMC) is a fantastic facility that allows an installation to configure and dynamically reconfigure the LPARs in one or more zEnterprise Systems. But the HMC can also issue operator commands, bypassing Best Practice External Security Manager (ESM) procedures.

• It used to be that this kind of physical access was severely restricted because you had to be in the "Computer Room" to get to the console. But, now, this old kind of access plus the ability to change configurations, and even do it remotely, is available to many.

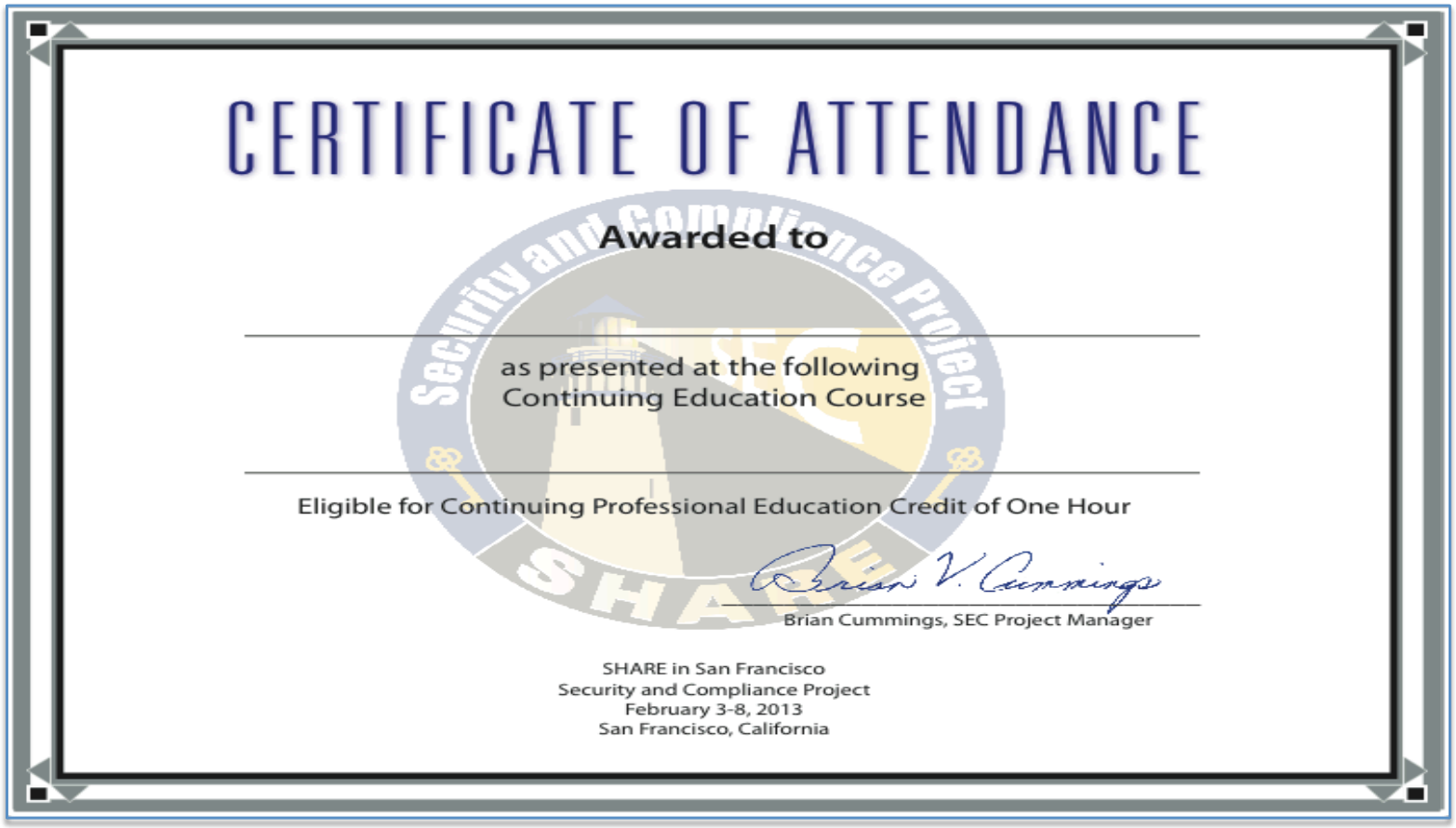
• This presentation will provide insight into HMC Control Issues, for example:

- ✓ Can you vary a storage volume online from the HMC? – sure!
- ✓ Can you add an APF authorized library? – sure!
- ✓ How many people have authorized access to the HMC? 25, 50, 150?
- ✓ Can they access it remotely? Do they need a Digital Certificate to do that?

• Barry Schrager was the first Project Manager of the SHARE Security Project. He is creator of ACF2, a member of the Mainframe Hall of Fame and currently President of Xbridge Systems. He holds a BS Degree in Physics from the University of Illinois and a Masters in Applied Mathematics from Northwestern University.

• Paul R. Robichaux, CEO, is co-founder of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a Certified Public Accountant.

Continuing Education Credit



CERTIFICATE OF ATTENDANCE

Awarded to

as presented at the following
Continuing Education Course

Eligible for Continuing Professional Education Credit of One Hour

Brian V. Cummings

Brian Cummings, SEC Project Manager

SHARE in San Francisco
Security and Compliance Project
February 3-8, 2013
San Francisco, California

The Hardware Management Console

The HMC is a great Tool but…

- It can lead to an opening of system vulnerabilities
- These can be exploited to bypass Security Best Practices
- You need to know both how to use it and secure it.

Complementary Sessions…

- Session 12255 - will cover why you need to secure your HMC
- Session 12807 - will cover how you secure your HMC

Brian Valentine, IBM
HMC Security Basics and Best Practices
Tuesday, February 5 - 3:00 PM
Franciscan D

A Statement of the Problem

HMC Security Vs. zEnterprise Integrity and Security

- It is a common z/OS Security best practice to seek full accountability; user, terminal and action identification of events that are intended to modify the functional configuration - the hardware and software of the IBM zEnterprise.
- Functional control over resource access and resource use is provided by the External Security Managers (RACF, CA ACF2, CA Top Secret) and is dependent on this vital information in maintaining the integrity of the IBM zEnterprise environment.
- When the HMC is used as a tool for the dynamic management of the zEnterprise, the control information it packages and passes to the system is not sufficiently rich with user and terminal information for the ESM to appropriately determine access rights and/or assign event accountability.
- This information deficit results in a loss of zEnterprise system integrity and security from the perspective of the External Security Manager and the Security Professionals that depend on its oversight and reporting.

HMC - Security Concerns

How would your organization score on this Compliance Test?

- ❑ Where is your HMC located?
- ❑ Who can walk up to it?
- ❑ Which users are defined to it?
- ❑ Do they all have the same high level authority?
- ❑ Can it be accessed remotely?
- ❑ Which users can access it remotely?
- ❑ Are they defined to require a digital certificate?
- ❑ Does anyone, even occasionally, review the logs?

HMC - Fantastic Tool

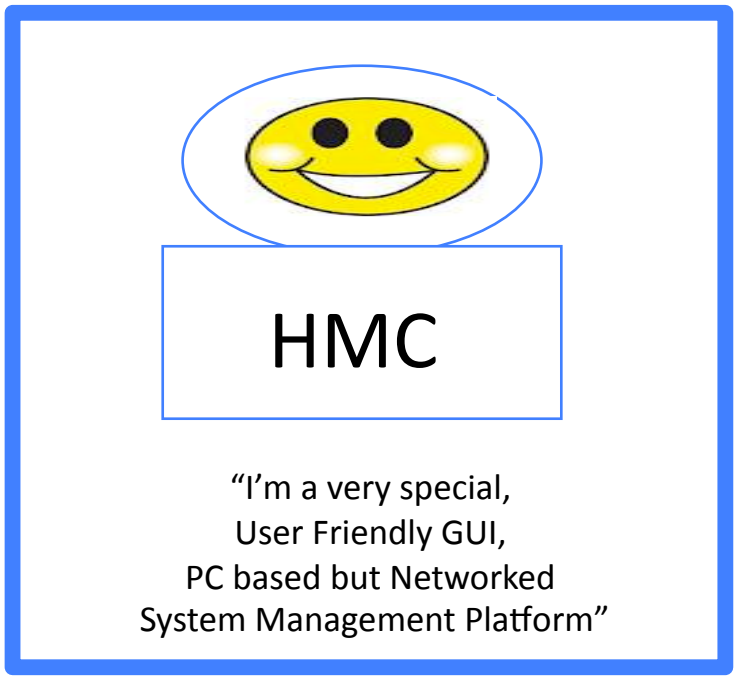
The HMC as The zEnterprise Manager

- *What is it?*
- *How does it work?*
- *Where is it going?*
- *Vulnerability?*
- *Beyond the HMC?*

HMC - Fantastic Tool

Hardware Management Console (HMC) – What is it?

- HMC is an acronym that describes the IBM technology that is used to manage and monitor IBM Mainframe and/or IBM UNIX servers.
- HMC is required before all the capabilities of a System zServer can be fully operational.
- HMC provides a GUI through which authorized operators manage configurations and partitions of zServer in a multi-system complex
- HMC monitors an individual system for hardware and other operational problems.
- HMC should be considered an appliance, meaning it's a *"Closed Platform"*.

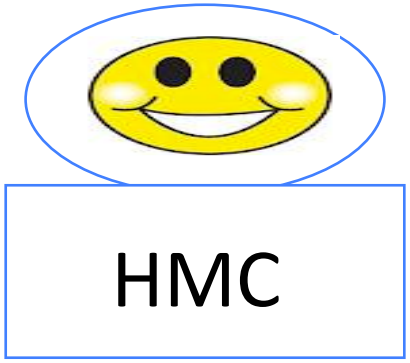


Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – What is it?

- ❑ HMC hardware is not serviced by the user, only IBM personnel perform this task.
- ❑ HMC is not an operating platform, not usable by an end user for other application execution.
- ❑ HMC uses a *"Private Network"* connection(s) to one or more zServer(s) Frames in order to perform management functions.
- ❑ HMC must be tested for network security using procedures that include periodic network scans to detect intrusion attempts.
- ❑ HMC monitors and logs the activity of its users based on their pre-assigned roles.



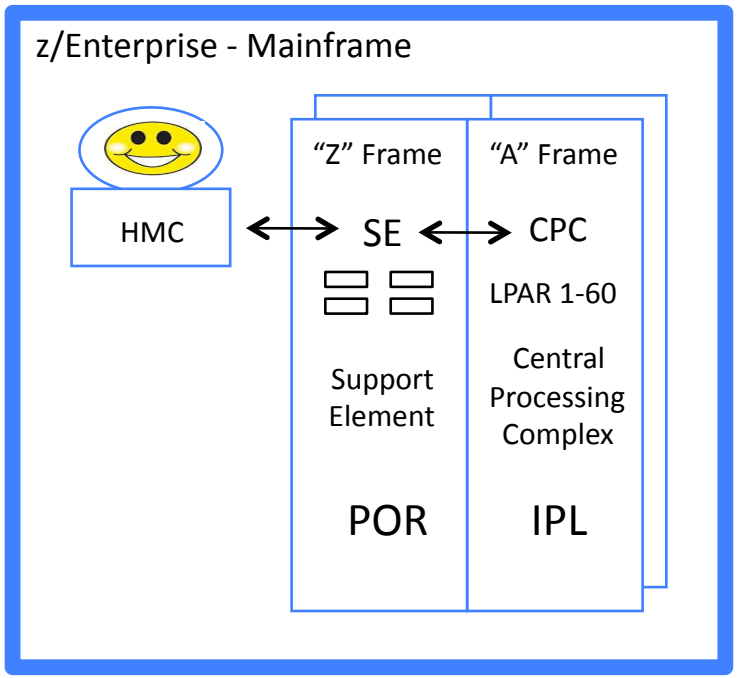
"I'm a very special,
User Friendly GUI,
PC based but Networked
System Management Platform"

Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – What is it?

- The CPC may have up to ~~96~~ 101 processors, ~~80~~ 90 of which are devoted to production work and may be subdivided into up to 60 z/OS LPARs.
- HMC commands are sent to the SE; the SE sends these commands to a targeted CPC/LPAR.
- CPCs can be grouped at the HMC so that a single command can be passed along to all of a defined set of CPCs.
- HMC hardware commands, used in a Power-On-Reset (POR), are processed by the SE. MVS operator commands, used in an Initial Program Load (IPL), are processed by the individual Logical Partitions (LPAR) defined to the CPC.



Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – How Secure!

Physical Security?

It's not that the HMC is either:

- ❑ Insecure or
- ❑ Offers no Security Controls.

It's just not the kind of Security that you're:

- ❑ Thinking of or
- ❑ The type of ESM Security you[1] are used to.

[1] *Resource and/or Access Security of the type provided by CA ACF2, RACF, CA Top Secret*

HMC - Fantastic Tool

z/OS Supports Console Logon and Provides the Ability to:

- Force a user to logon to consoles although it could be set to automatically log them on with a defined Userid
- Authorize commands entered via ACF2, RACF or Top Secret based upon the Userid of the Operator who logged on to the console

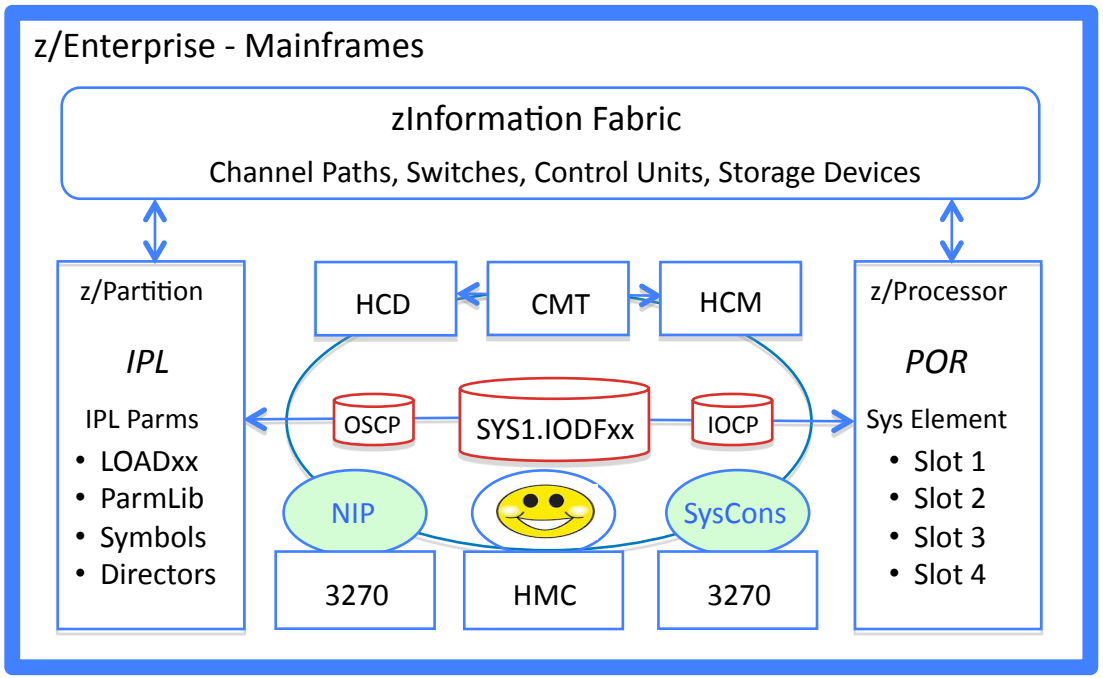
But the HMC Does not Support these z/OS Control Features:

- Commands entered from the HMC pass to ACF2, RACF and Top Secret with the same Userid for ALL HMC's
- All commands have the same Userid – that of the Console name as specified in the Console member of PARMLIB
- There is no way for the ESM to distinguish one user from another or one HMC to another

HMC - Fantastic Tool

Hardware Management Console (HMC) – It's Simple, Don't get Confused!

- You can operate a z/OS system or an entire Sysplex using the *Operating System Message Facility* of the HMC. This facility is also known as the SYSCONS console and is considered an Extended MCS type of Operator Console.
- You would generally only use this facility if there were problems with the CONSOLES defined with *Master Console Authority* in the CONSOLxx parmlib member.



Source: System z:Hardware Management Console Operations Guide, SC28-6857-01

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 1

❑ To use the SYSCONS console on the HMC, select the Operating System Messages (OSM) task and the target system on the HMC. The HMC will open the SYSCONS console for the system.

To use the SYSCONS console for command processing first enter

```
VARY CN(*),ACTIVATE
```

This allow the SYSCONS to send commands in Problem Determination (PD) mode.

- *Almost any z/OS command can now be entered, with a few restrictions.*
- *Active system SYSCONS console may be accessed by multiple HMCs and*
- *It is not necessary to issue the VARY CONSOLE command for each HMC.*

The Active system SYSCONS remains active for the duration of the IPL, or until the

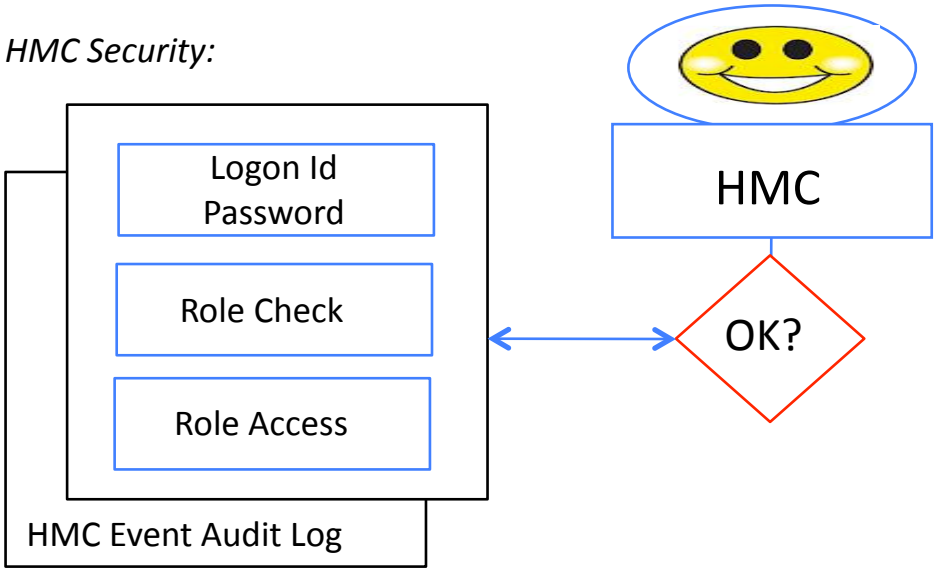
```
VARY CN(*),DEACT
```

command (to deactivate the system console) is entered.

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 1

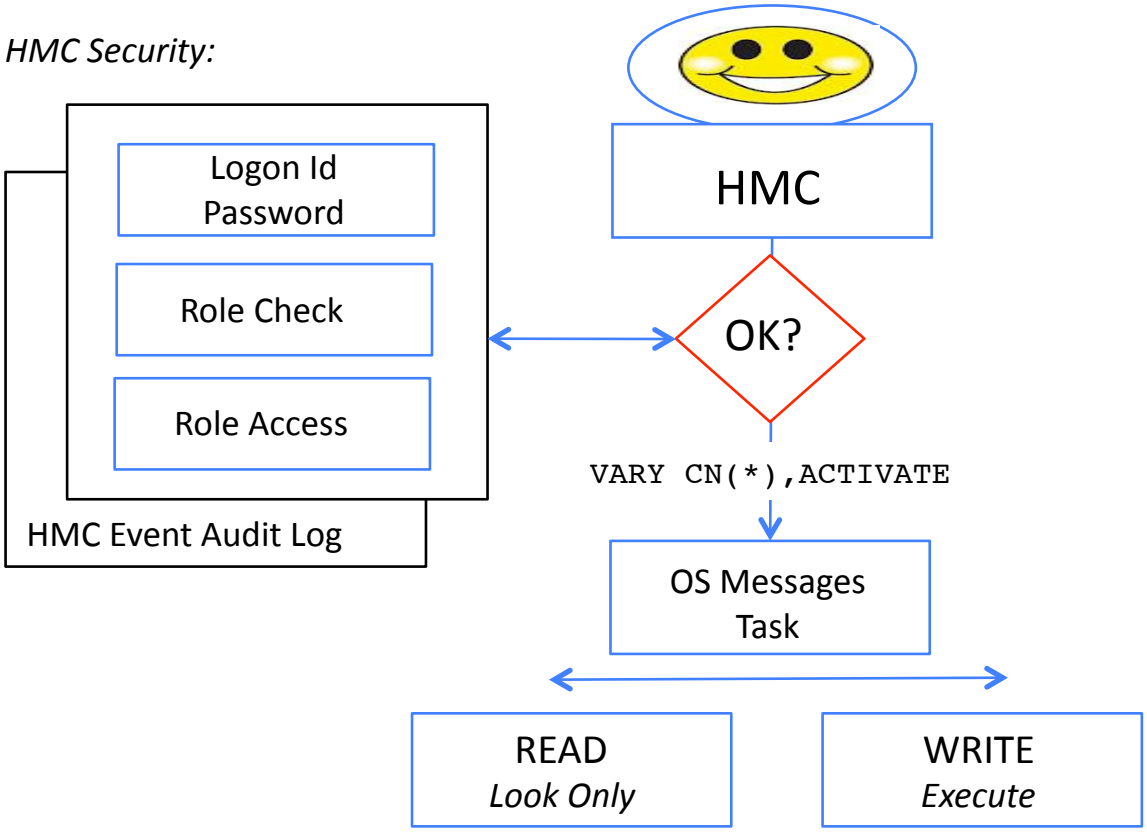
HMC Security:



HMC - Fantastic Tool

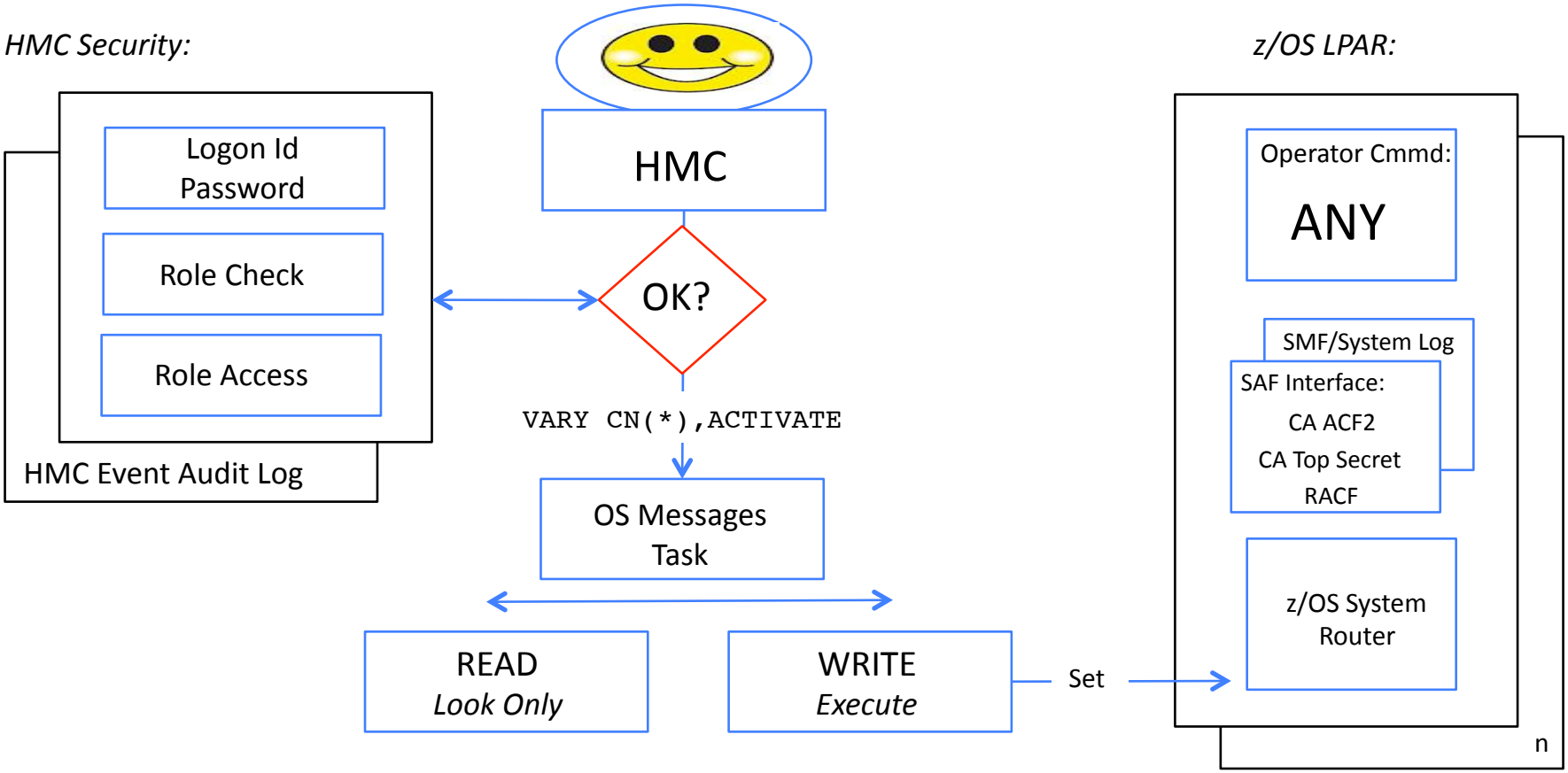
Know Your Environment – The Origin of Vulnerability – Part 1

HMC Security:



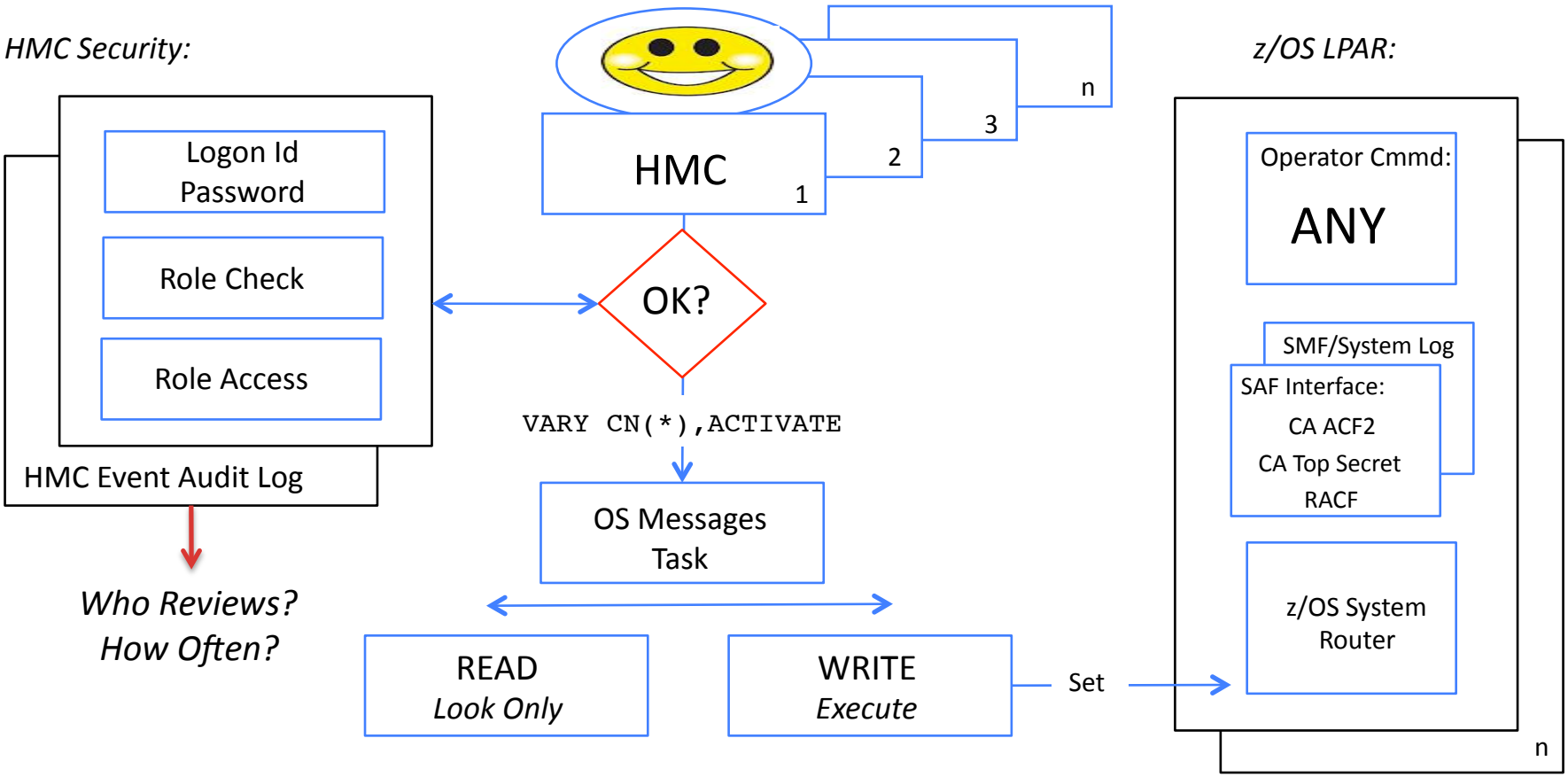
HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 1



HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 1



HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 1

- Try this at Home – Display the Active Consoles ACTIVE using this command:

```
/DISPLAY CONSOLE,ACTIVE,CA
```

- The name of HCM Console(s) returned is the System Name/Id and NOT the Console Name. The HMC per se will not show up as an active console. It appears that System Name/Id is used for logging command issued from the HMC.

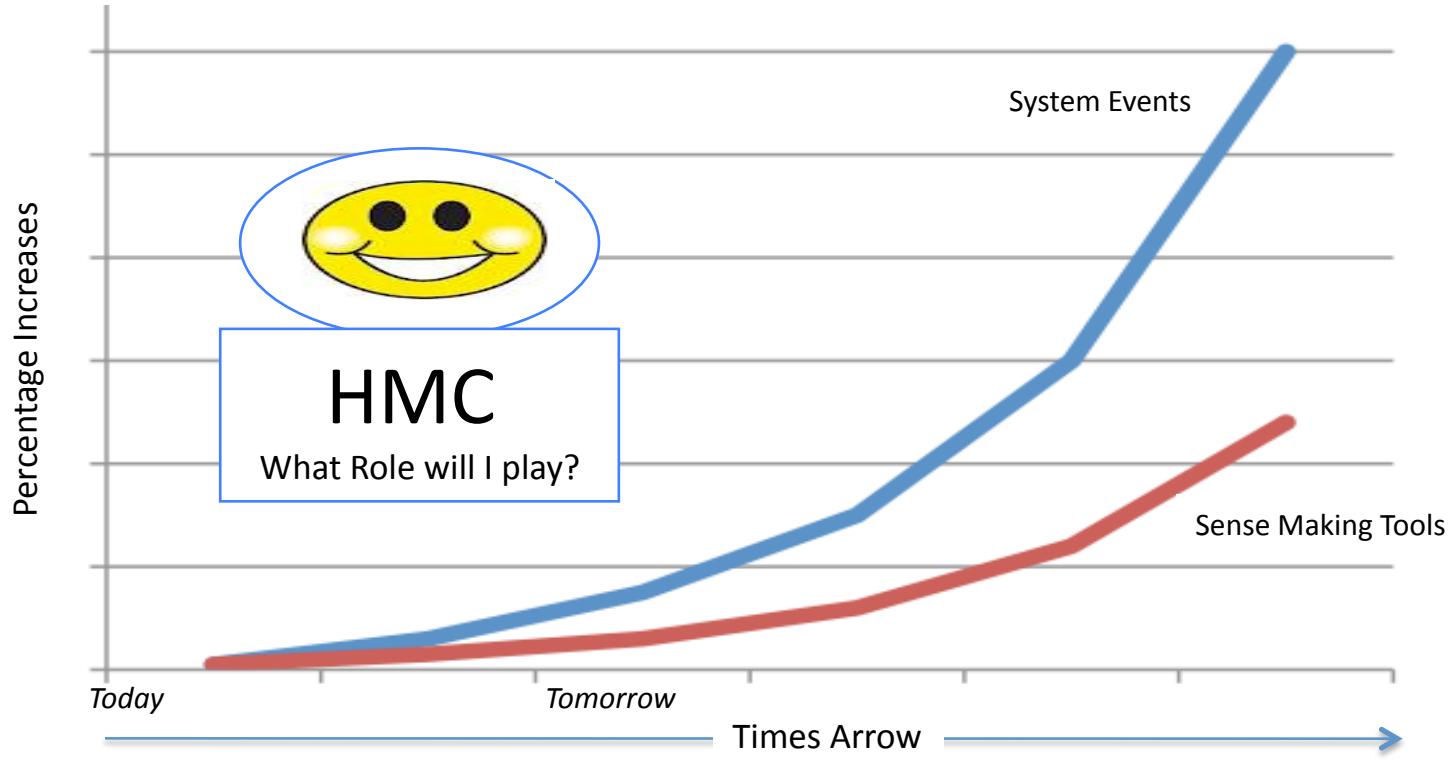
```
NC0000000 MAI2     2012123 13:34:56.98 MAI2     00000290  D C,A,CA

  LR                 291 00000090  CONSOLES MATCHING COMMAND: D C,A,CA
  LR                 291 00000090  NAME      TYPE  SYSTEM    ADDRESS   STATUS
  DR                 291 00000090  MAANXOCC  MCS   MAI2      10A2      ACTIVE
  DR                 291 00000090  MACN10A0  MCS   MAI2      10A0      ACTIVE
  DR                 291 00000090  MACR2080  MCS   MAI2      1080      ACTIVE
  DR                 291 00000090  MFANXOCC  MCS   MFI3      10A2      ACTIVE
  DR                 291 00000090  MFCN10A0  MCS   MFI3      10A0      ACTIVE
  ER                 291 00000090  MFCR2180  MCS   MFI3      1180      ACTIVE
```

Source: A Gracious project participant!

HMC - Fantastic Tool

Hardware Management Console (HMC) - The Future - Manage it All!



[1] *More than 40,000 unique message IDs are defined for z/OS and the IBM software that runs on z/OS systems.*

A Statement of the Problem

Hardware Management Console (HMC) – The Future – z/OS V2R1

- z/OS Console support for HMC 3270 console planned
  - For z/OS console, during and after IPL
  - Intended to add another backup console
  - Designed to allow small z/OS LPARs to run without OSA-ICC
- HMC complex-wide IODF Activate
  - For all z/OS and z/VM LPARs managed in the same HMC complex
    - Same CEC, different CEC
    - Same Sysplex, different Sysplex
    - On IBM System z9® and later servers
    - For z/OS V1.12 (5694-A01), z/VM V5.4 (5741-A05), and later when initiated from a system running z/OS V2.1
  - Initiate from HCD or HCM
  - Eliminate the need to activate I/O configuration changes one LPAR at a time

A Statement of the Problem

Hardware Management Console (HMC) – The Future – z/OS V2R1

Link to zEC12 and V2R1 Update

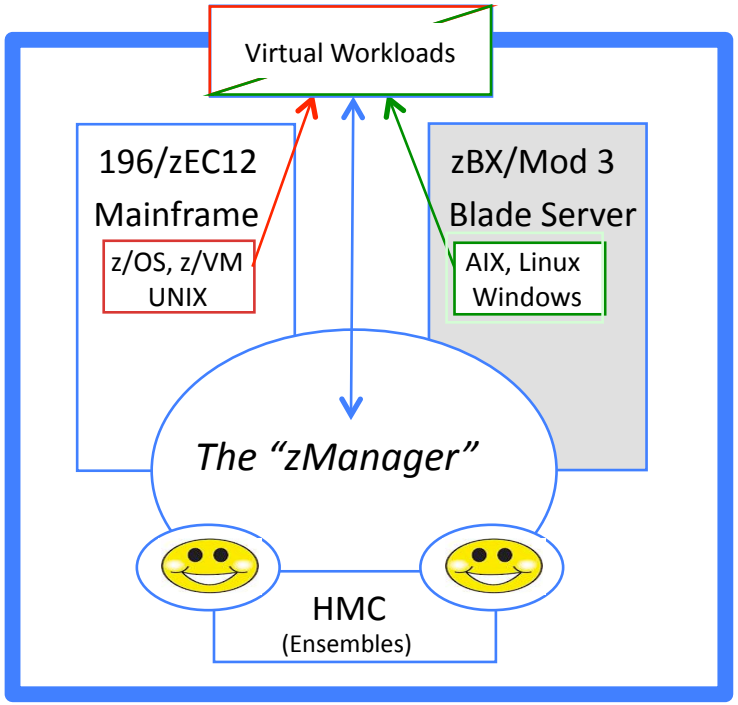
https://share.confex.com/share/120/webprogram/Handout/Session12728/SHARE%20120%20Session%2012728.pdf

John Eells
IBM Poughkeepsie
eells@us.ibm.com
4 February 2013

HMC - Fantastic Tool

Hardware Management Console (HMC) – The Future – zManager

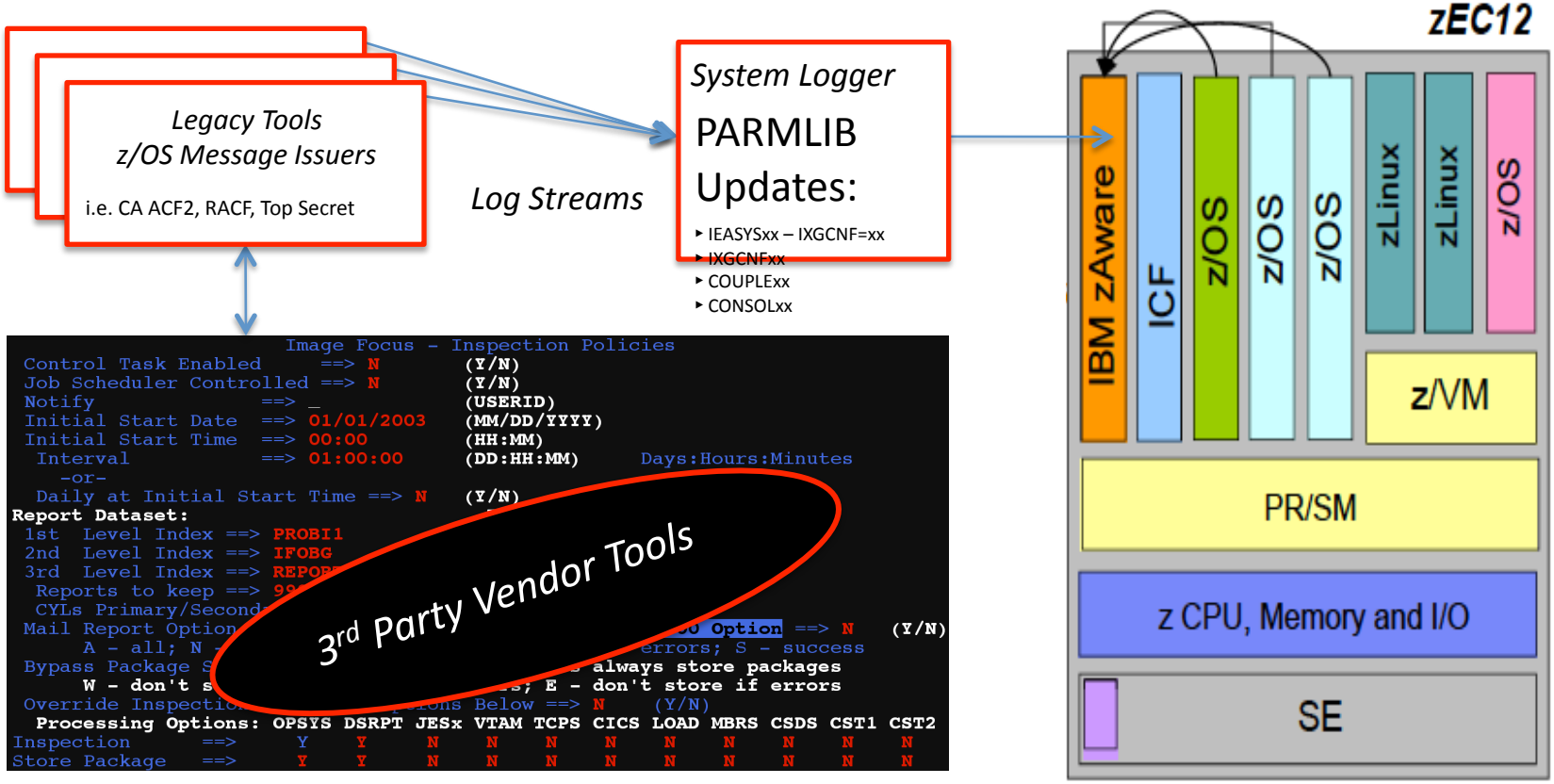
- The integration of the hardware platform that brings mainframe and distributed technologies together will, over time, replace individual islands of computing. These integrated resources are called *Ensembles*.
- Each Ensemble will be managed as a single logical, "Virtualized" system by the URM, through the HCM. The HMC will create and manage ensemble resources.
- Some of the benefits of the ensemble:
  - ✓ Reduction of complexity
  - ✓ Improve security
  - ✓ Applications closer to needed data.



Source: zEnterprise Unified Resource Manager: Building an Ensemble, SG24-7921-00

HMC - Fantastic Tool

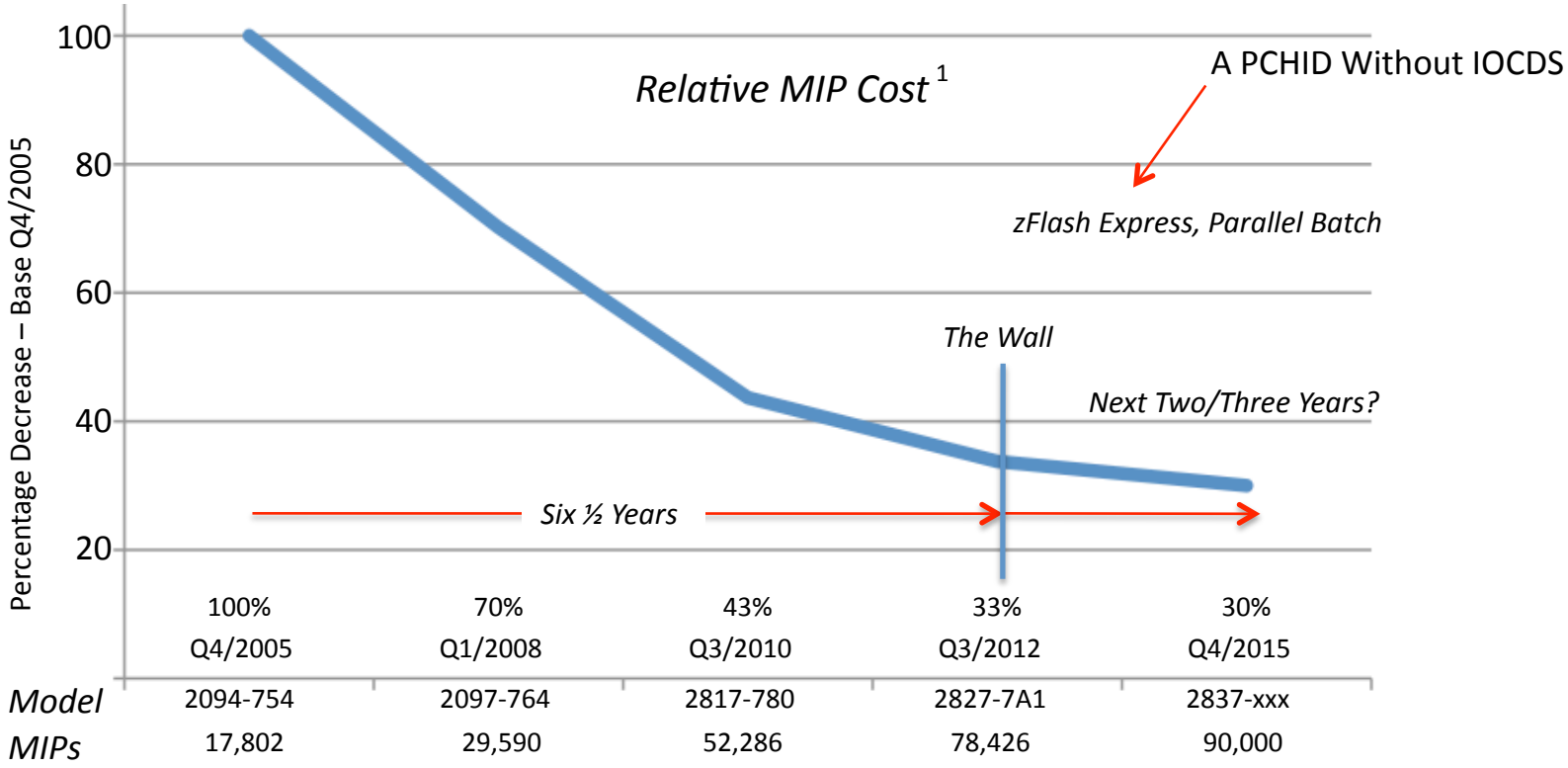
Hardware Management Console (HMC) – The Future - zAware



[1] *z/U 04/2012 - zZS18: Smart Monitoring of z/OS with IBM zAware on zEC12 by Riaz Ahmad*

HMC - Fantastic Tool

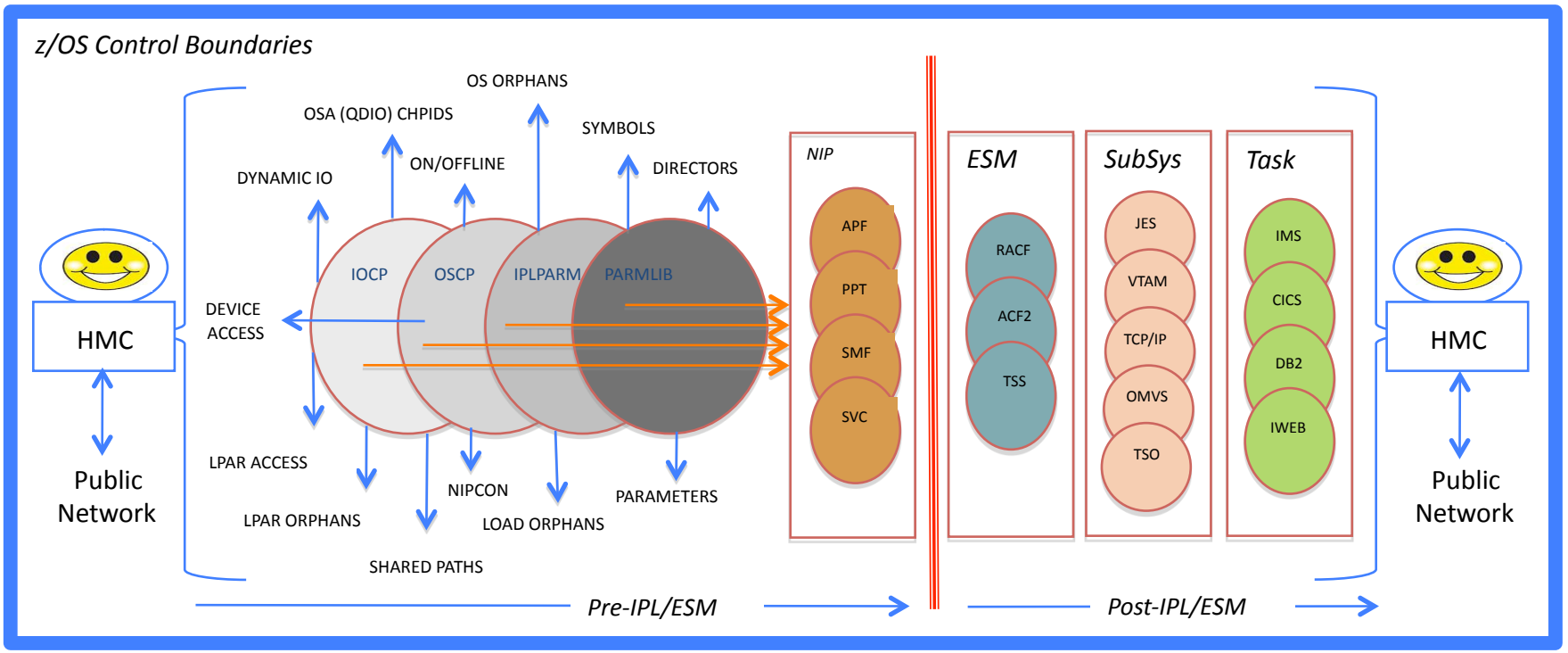
Hardware Management Console (HMC) – The Future - zFlash



Source:http://www.tech-news.com/publib/pl2084, pl2094, pl2097, pl2817 and pl2827 all .html

HMC - Fantastic Tool

Hardware Management Console (HMC) - It's Simple, Don't get Confused!



Source: Share, August, 2011, Session Number 10101 "IODF as the Foundation of z/Enterprise Compliance"

HMC - Fantastic Tool

HMC Security Vs. zEnterprise Integrity and Security - Requirements Statement!

- It is a common z/OS Security best practice to seek full accountability; user, terminal and action identification of events that are intended to modify the functional configuration - the hardware and software of the IBM zEnterprise.
- Functional control over resource access and resource use is provided by the External Security Managers (RACF, CA ACF2, CA Top Secret) and is dependent on this vital information in maintaining the integrity of the IBM zEnterprise environment.
- When the HMC is used as a tool for the dynamic management of the zEnterprise, the control information it packages and passes to the system is not sufficiently rich with user and terminal information for the ESM an appropriately determine access rights and/or assign event accountability.
- This information deficit results in a loss of zEnterprise system integrity and security from the perspective of the External Security Manager and the Security Professionals that depend on it oversight and reporting.

That's it folks, all done!

Session Evaluation – Session Number - 12255

The HMC Is a Fantastic Tool But Are You Making it Secure?

Barry Schrager
Xbridge Systems, Inc.
BSchrager@xbridgesystems.com

Paul R. Robichaux
NewEra Software, Inc.
prr@newera.com

SHARE.org/SanFrancisoEval

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Insert Custom Session QR if Desired.