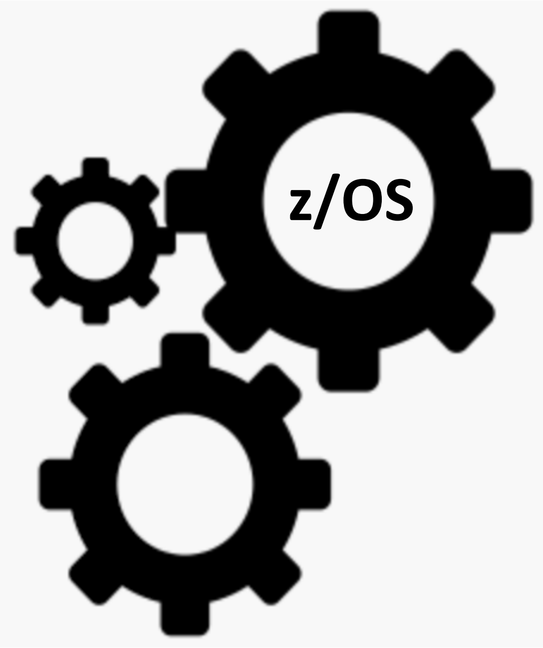


Let’s Build a z Environment - 102

Session 23331

Tuesday, August 14 at 11:15-12:15 AM

STL CC, Room 242

Presented by Paul R. Robichaux

NewEra Software, Inc.

Abstract – Let’s Build a z Environment!

The two presentations in this series focus on the building of a z Environment – Hardware, Software, Security – with the goal of establishing a ‘Trusted Computing Base’. A z/OS System that can provide the reliability needed to meet demanding service levels, integrity and security objectives. All are necessary to execute mission critical applications. This is Intended for those new to z Systems or just beginning their careers with organizations that capitalize on systems anchored to the power and reliability of the IBM Mainframe.

In – 101 – the focus will be on the platform, in this case a z14, hardware divisions of the Central Processing Complex (CEC), its various channel pathways and related devices that define a UCW (Unit Control Work), the front half of the z System Device Chain. This segment continues with the definition of an associated Operating System configuration, its various I/O devices and related features that define a UCB (Unit Control Block), the back half of the z System Device. Detailing both the Power-On and IPL process will join UCWs and UCBs to form a fully addressable device across which data (encrypted or not) may flow to and from the CEC.

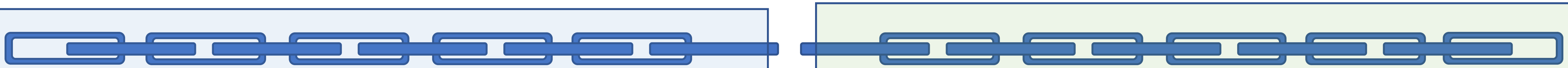
In – 102 – the focus will shift to a discussion of Multiple Virtual Storage (MVS), what is z/OS, how to get it, install it, support it and upgrade/migrate from release to release. The elements of the IPL Path – IPLPARM, IRIMS, IODF, SYSRES – to name just a few will be examined in detail as will the Post-IPL environment – APFLST, LNKLST, LPALST, SVCs, EXITs, PPT. The integrity of the environment will be described within the context of the IBM Integrity Statement and the Authorized Program Facility (APF). The session ends with a discussion concerning system vulnerabilities, their potential impact and sources of possible remediation.

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

The corporate mission of NewEra Software is to provide software solutions that help users avoid z/OS non-compliance, make corrections when needed and in doing so, continuously improve z/OS integrity and Security.

Let’s Build a System z Environment - 102

Sysplex with two z14s and a z14 (CF). A total of 30 LPARs - An average size z/OS shop.



Null Z14 Hardware

Defining the z/14 Hardware

Load the z/OS Program

A Running z/OS LPAR

When the System is at Rest - 101

1. Why are we here?
2. Alphabet, Words, Pictures & Rules
3. The Mainframe Today
4. Virtualization
5. Physicalization
6. Crafting a Partition
7. Goals and Control Points
8. Unpacking the Configuration
9. Power-on-Reset

A. Defining a z/OS Image

When the System is in Flight – 102

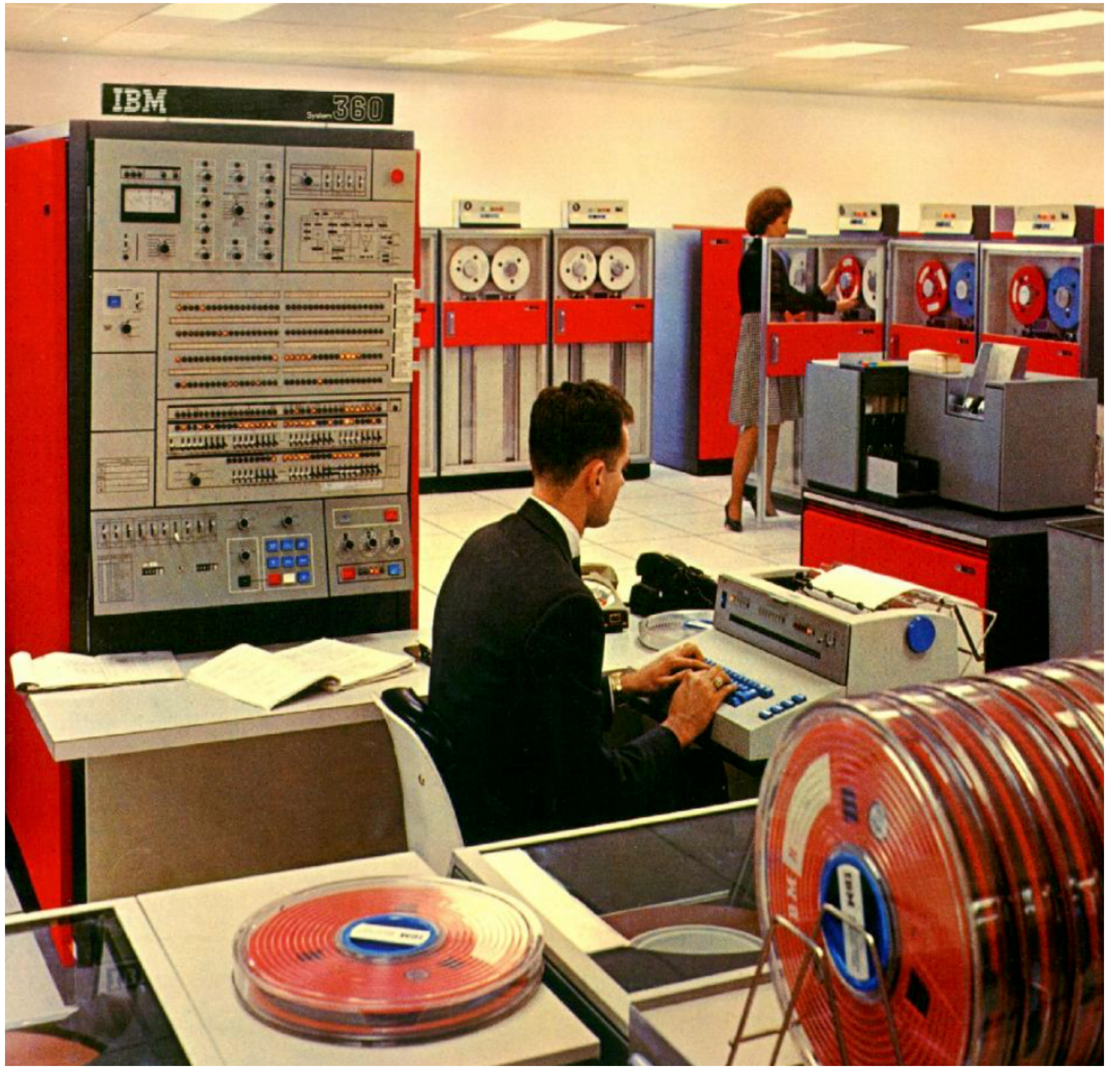
1. What is MVS?
2. Delivery
3. Migration
4. On the IPL Path
5. Post-IPL State
6. z System Integrity
7. Program Authorization
8. System Vulnerabilities
9. Language Index

A. Recommended Reading/Viewing

Why are we here?

"The world is in the midst of a transformation that is having a profound effect on us as individuals, in business, and in society at large. As we adapt to capitalize on these trends, we must come to understand that trust will be the valued currency that will drive our economies."

1 - What is MVS?



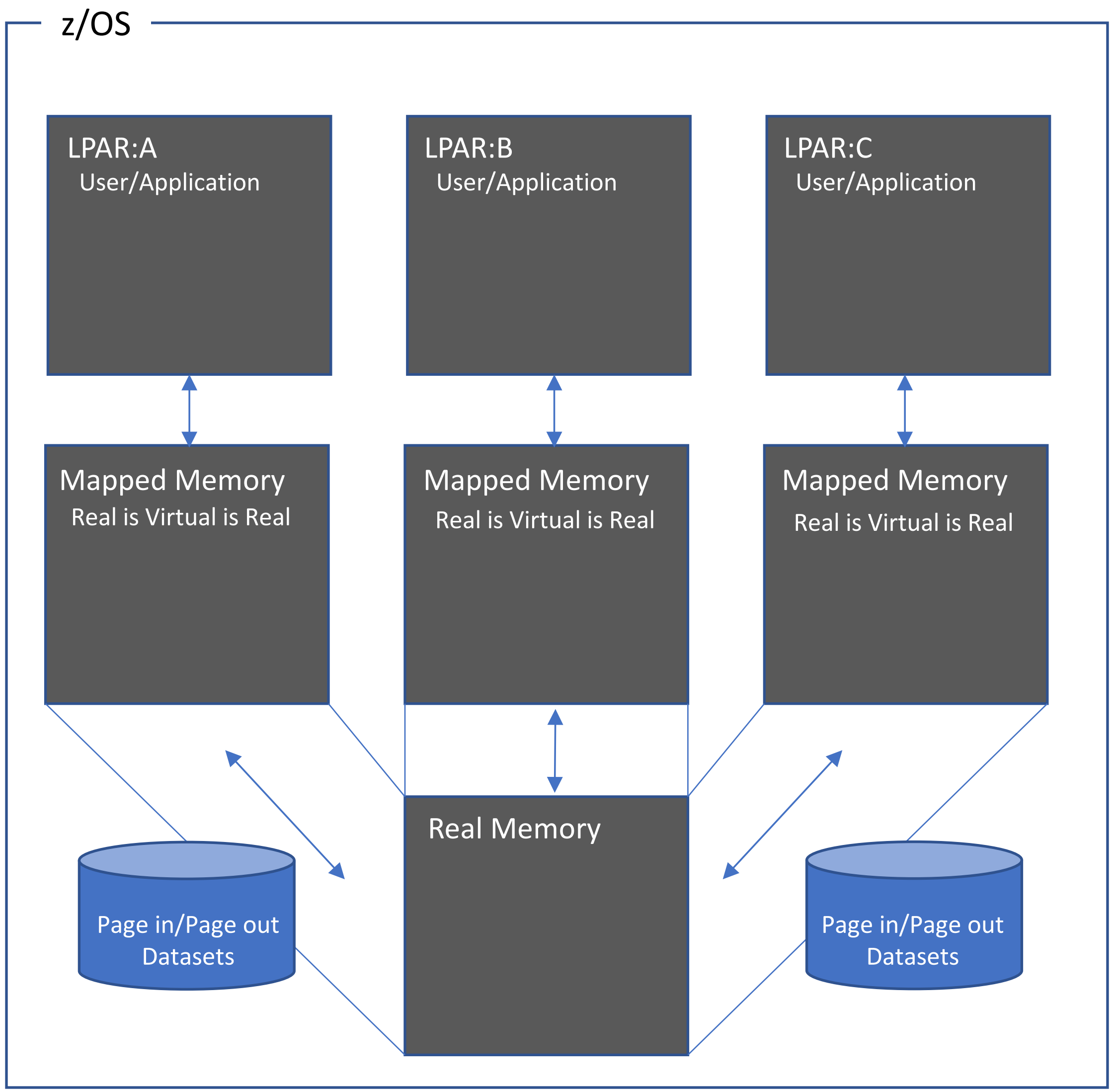
Some History:

MVS (Multiple Virtual Storage) is an operating system from IBM that continues to run on many of IBM's mainframe and large server computers. MVS has been said to be the operating system that keeps the world going and the same could be said of its successor systems, OS/390 and z/OS. The payroll, accounts receivable, transaction processing, database management, and other programs critical to the world's largest businesses are usually run on an MVS or successor system. Although MVS has often been seen as a monolithic, centrally-controlled information system, IBM has in recent years repositioned it (and successor systems) as a "large server" in a network-oriented distributed environment.

The follow-on versions of MVS (z/OS, for example) no longer includes the "MVS" in its names.

https://searchdatacenter.techtarget.com/definition/MVS

2 - What is MVS?



Virtual Storage:

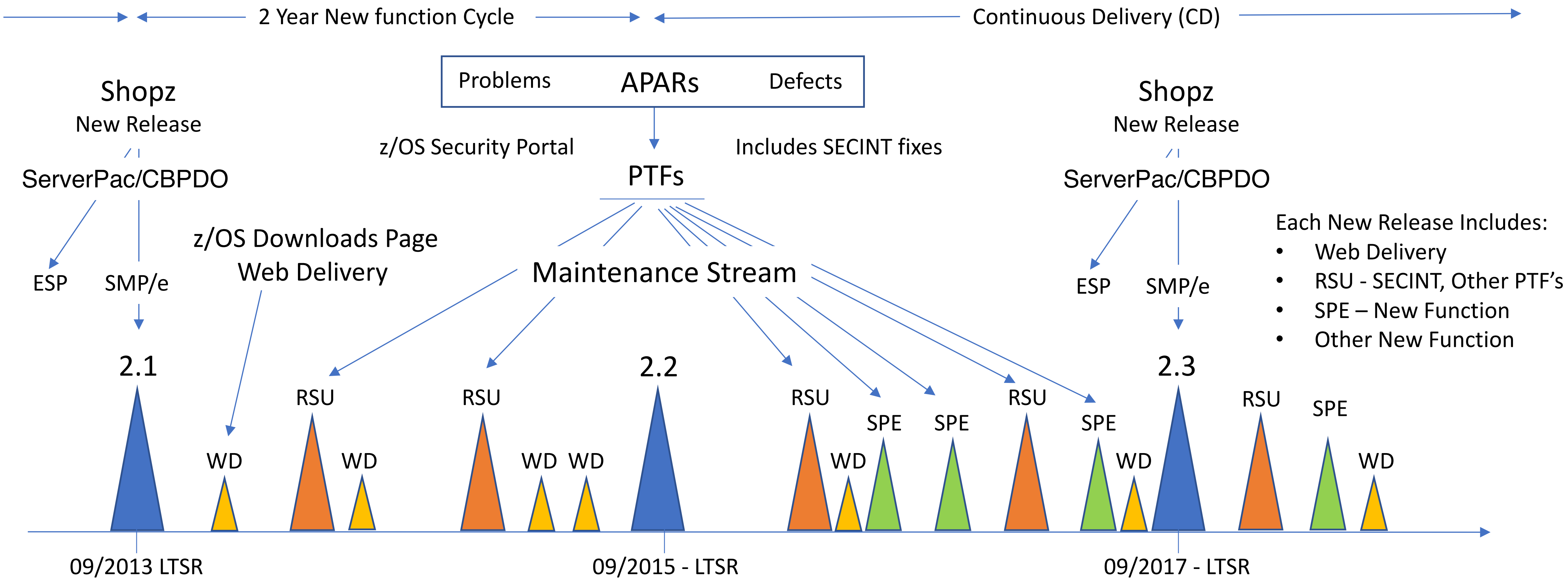
The Virtual Storage in MVS refers to the use of virtual memory in the operating system.

Virtual storage or memory allows a program to have access to the maximum amount of memory in a system even though this memory is actually being shared among more than one application program.

The operating system (z/OS) translates the program's virtual address into the real physical memory address where the data is actually located.

The Multiple in MVS indicates that a separate virtual memory is maintained in the mapped form within a Paged Dataset for each multiple task partition. These Pages are, in turn, called (Paged) in and out of Real Memory as needed.

2 - Delivery - How you get it



Each New Release Includes:

- Web Delivery
- RSU - SECINT, Other PTF's
- SPE – New Function
- Other New Function

```
APAR    - Authorized Program Analysis Report describes problem and  is formally tracked until resolved
RSU     - Recommended Service Update
SPE     - Describes a New Function APAR
PTF     - Program Temporary Fix – When applied, resolves a related APAR – FIX Package FIXPCK
EOS     - End of Service
LTSR    - Long-Term Support Release – 2yrs Minimum, 1yr extension is optional at End of Service - CD has a shorter support cycle
ESP     - Early Support Program
SECINT  - System Security and Integrity APARs/PTFs
CBPDO   - Custom-Built Product Delivery Option
```

2 - Delivery - How you install it

About ServerPac

ServerPac - An entitled software delivery package consisting of products and services for which IBM® has performed the SMP/E installation steps and some post-SMP/E steps.

- A full system replacement installs a complete z/OS system. A full system replacement helps assure a successful first IPL.
- A software upgrade installs only system software and does not create the set of new operational data sets required to IPL.

About CBPDO

CBPDO - An entitled software delivery package consisting of uninstalled products and unintegrated service. There is no dialog program to help you install, as there is with ServerPac.

- Other than z/OS itself, CBPDO is useful to upgrade an existing product, or add a new product to an existing SMP/E environment.
- By contrast, the Product ServerPac is useful when creating a new SMP/E environment.

About SMP/E

SMP/E is the basic tool for installing and maintaining z/OS® systems and subsystems. It controls changes at the element level by:

- Selecting the proper levels of elements to be installed (from a large number of possible changes),
- Calling required system utility programs to install the changes and
- Keeping records of the installed changes.

SMP/E is an integral part of the installation, service, and maintenance processes for CBPDOs, ProductPacs, RefreshPacs, and selective follow-on service for CustomPacs.

SMP/E can be used to install and service any software, including vendor software, that is packaged in SMP/E system modification (SYSMOD) format.

What are the basic SMP/E commands I need to know?

SMP/E – System Modification Program/Extended

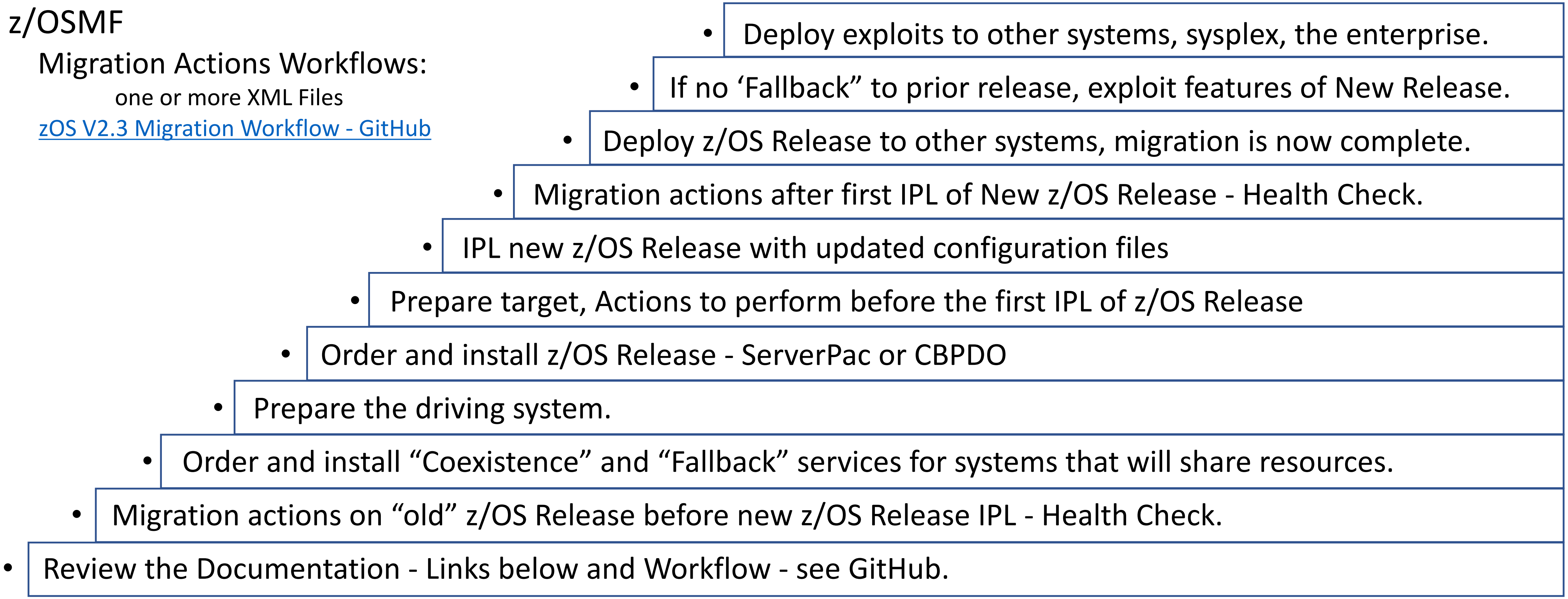
3 - Migration - Workflow

z/OSMF

Migration Actions Workflows:

one or more XML Files

zOS V2.3 Migration Workflow - GitHub

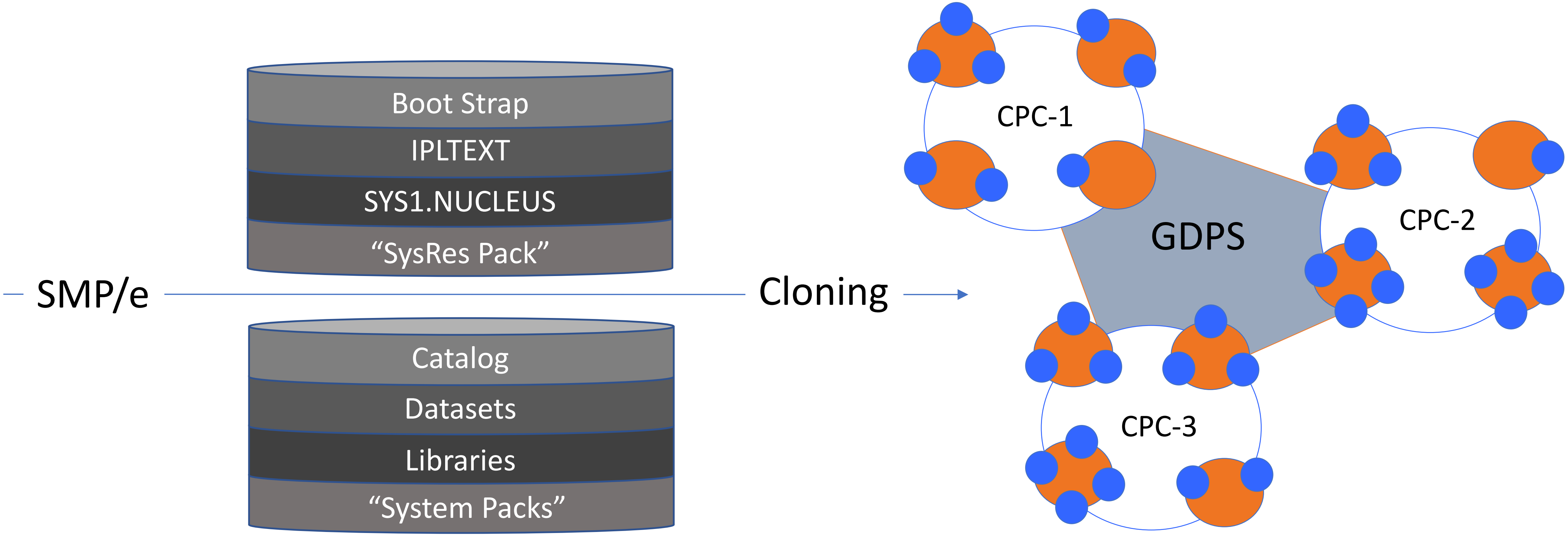


- Deploy exploits to other systems, sysplex, the enterprise.
- If no ‘Fallback” to prior release, exploit features of New Release.
- Deploy z/OS Release to other systems, migration is now complete.
- Migration actions after first IPL of New z/OS Release - Health Check.
- IPL new z/OS Release with updated configuration files
- Prepare target, Actions to perform before the first IPL of z/OS Release
- Order and install z/OS Release - ServerPac or CBPDO
- Prepare the driving system.
- Order and install “Coexistence” and “Fallback” services for systems that will share resources.
- Migration actions on “old” z/OS Release before new z/OS Release IPL - Health Check.
- Review the Documentation - Links below and Workflow - see GitHub.

IBM z/OS Migration (GA32-0889-30)
IBM z/OS Introduction and Release Guide (GA32-0887-30)

IBM z/OS Planning for Installation (GA32-0890-30)
IBM z/OS Management Facility V2R3 - IBM Redbooks

3 - Migration - Sysplex



Boot Strap

IPLTEXT

SYS1.NUCLEUS

“SysRes Pack”

SMP/e

Cloning

Catalog

Datasets

Libraries

“System Packs”

Cloning an already-installed z/OS system is faster and easier than installing z/OS with an IBM installation package such as ServerPac. Cloning system libraries (logical SYSRES volume) may also save DASD and support costs because you only need to install service once.

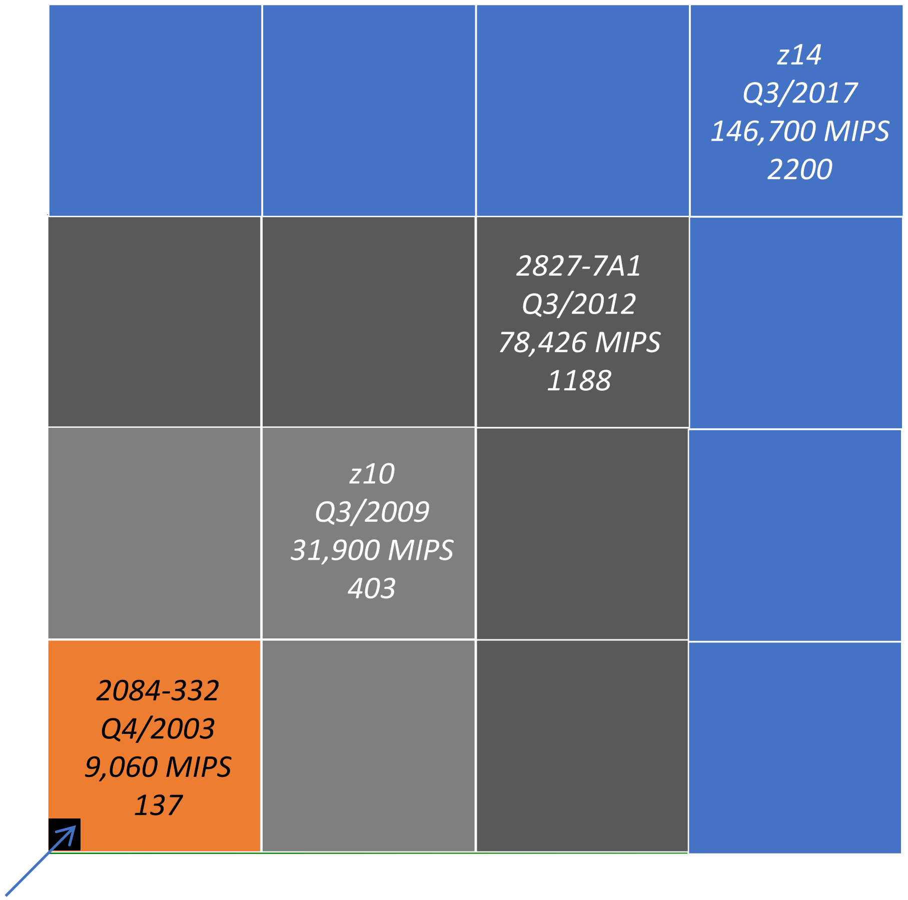
However, before cloning z/OS, you must have a license for each z/OS operating system that you run. If you do not have the appropriate license or licenses, any cloning is an unauthorized use of z/OS.

IBM z/OS Planning for Installation (GA32-0890-30)

GDPS – Geographically Disbursed Sysplex

3 - Migration - Hardware

You'll have to run pretty hard just to keep up with it all!



z14
Q3/2017
146,700 MIPS
2200

2827-7A1
Q3/2012
78,426 MIPS
1188

z10
Q3/2009
31,900 MIPS
403

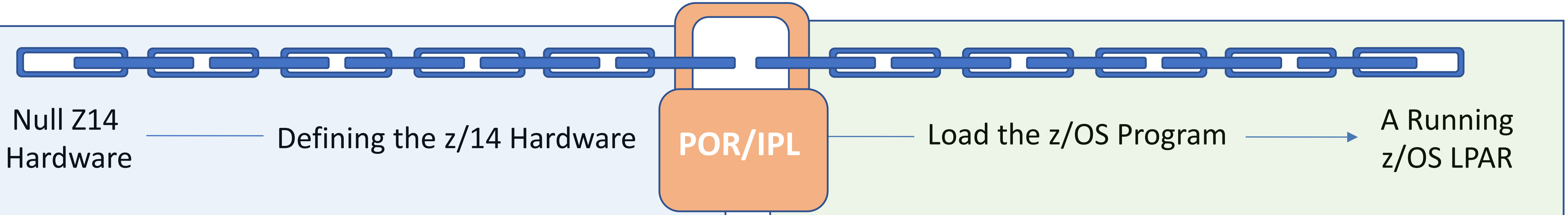
2084-332
Q4/2003
9,060 MIPS
137

9672-R61
Q3/1994
66 MIPS

Source:http://www.tech-news.com/publib

4 - On the IPL Path:

Sysplex with two z14s and a z14 (CF). A total of 30 LPARs - An average size z/OS shop.



Null Z14 Hardware → Defining the z/14 Hardware → POR/IPL → Load the z/OS Program → A Running z/OS LPAR

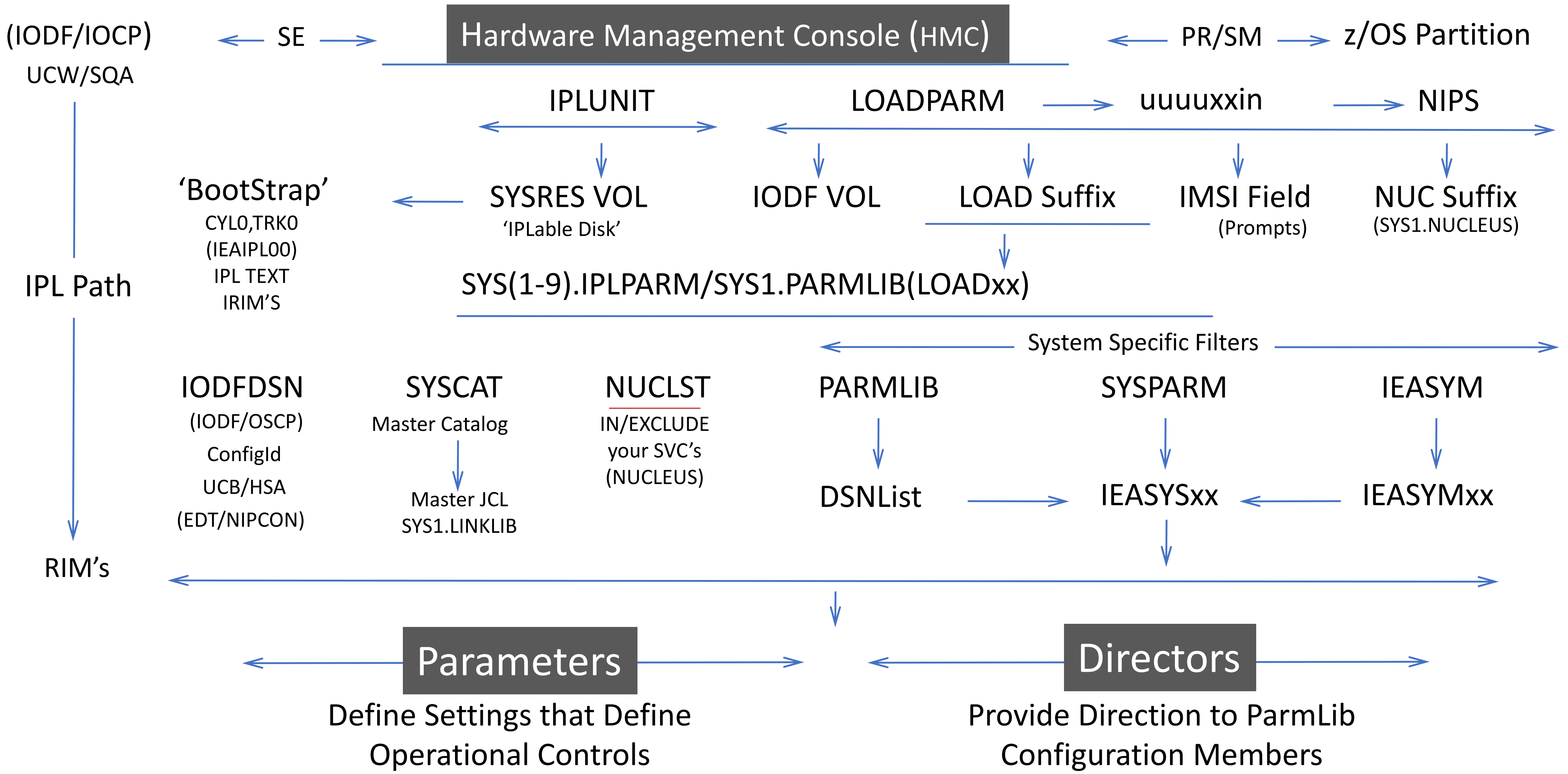
Power on Reset (POR) - IOCP loaded - Hardware Storage Area (HSA), OSCP loaded - System Query Area (SQA), Resource Initialization Modules (I/RIM) and System NUCLEUS Loaded, Parmlib dataset discovered, expanded, APFList, LNKList, LPAList and LPA Modules Loaded, Master Address available.

Cold Start (CLPA) - Reloads Pageable Link Pack Area (PLPA), clears virtual input/output (VIO) Dataset Pages. JOBs require restart

Quick Start - Does not reload the PLPA, but does clears the VIO dataset pages. JOBs require restart.

Warm Start - No reload of PLPA, VIO datasets are preserved, JOBs continue.

4 - On the IPL Path:



(IODF/IOCP)
UCW/SQA

SE

Hardware Management Console (HMC)

PR/SM

z/OS Partition

IPLUNIT

LOADPARM

uuuuxxin

NIPS

'BootStrap'
CYL0,TRK0
(IEAIPL00)
IPL TEXT
IRIM'S

SYSRES VOL
'IPLable Disk'

IODF VOL

LOAD Suffix

IMSI Field
(Prompts)

NUC Suffix
(SYS1.NUCLEUS)

IPL Path

SYS(1-9).IPLPARM/SYS1.PARMLIB(LOADxx)

System Specific Filters

IODFDSN
(IODF/OSCP)
ConfigId
UCB/HSA
(EDT/NIPCON)

SYSCAT
Master Catalog
Master JCL
SYS1.LINKLIB

NUCLST
IN/EXCLUDE
your SVC's
(NUCLEUS)

PARMLIB
DSNList

SYSPARM
IEASYSxx

IEASYM
IEASYMxx

RIM's

Parameters

Define Settings that Define
Operational Controls

Directors

Provide Direction to ParmLib
Configuration Members

4 - On the IPL Path:

Parameters

CLPA
CMB
CSA
CSCBLOC
CVIO
~~DRMODE~~
DUMP
GRS
HVCOMMON
HVSHARE
HZSPROC
LFAREA
LICENSE
LNKAUTH – APF
LOGCLS
LOGLMT
LOGREC
MAXCAD
MAXUSER
NONVIO

NSYSLX
OPI – See Below*
PAGE – Datasets
PAGESCM
PAGTOTL
PLEXCFG
PRESCPU
RDE
REAL
RER
RSU
RSVNONR
RSVSTRT
SQA
SYSNAME – Name
SYSP
VIODSN
VRREGN
WARNUND
ZAAPZIIP

Directors

ALLOC=xx,xx
APF=xx
AUTOR=xx,xx
AXR=xx,xx
CATALOG=xx,xx
CEA=xx,xx
CEE=xx,xx
CLOCK=xx,xx
CMD=xx,xx
CON=xx
COUPLE=xx
DEVSUP=xx,xx
DIAG=xx,xx
EXIT=xx – Site
FIX=xx,xx
FXE=xx – Registry
GRSCNF=xx
GRSRNL=xx,xx
GTZ=xx,xx
HZS=xx,xx
IEFOPZ=xx,xx

IKJTSO=xx — Auth Cmds/Progs
IOS=xx
IQP=xx,xx
IZU=xx – z/OSMF
IXGCNF=xx,xx
LNK=xx,xx – LNKLST
LPA=xx,xx – LPALST
MLPA=xx,xx
MSTRJCL=xx
OMVS=xx,xx
OPT=xx
PAK=xx
PROD=xx,xx
PROG=xx,xx – APF/LNKLST/LPAMOD
RACF=xx,xx – Db Configuration
SCH=xx,xx – PPTable
SMF=xx,xx
SMS=xx,xx
SSI=xx,xx
SVC=xx,xx – Site SVC Table
SYSP=OPR,xx,xx
UNI=xx & VAL=xx,xx

*Directors and Parameters that can be placed in an IEASYSxx member or specified by the operator.

Overview of IEASYSxx parameters

4 - On the IPL Path:

Unit Address

LOADPARM

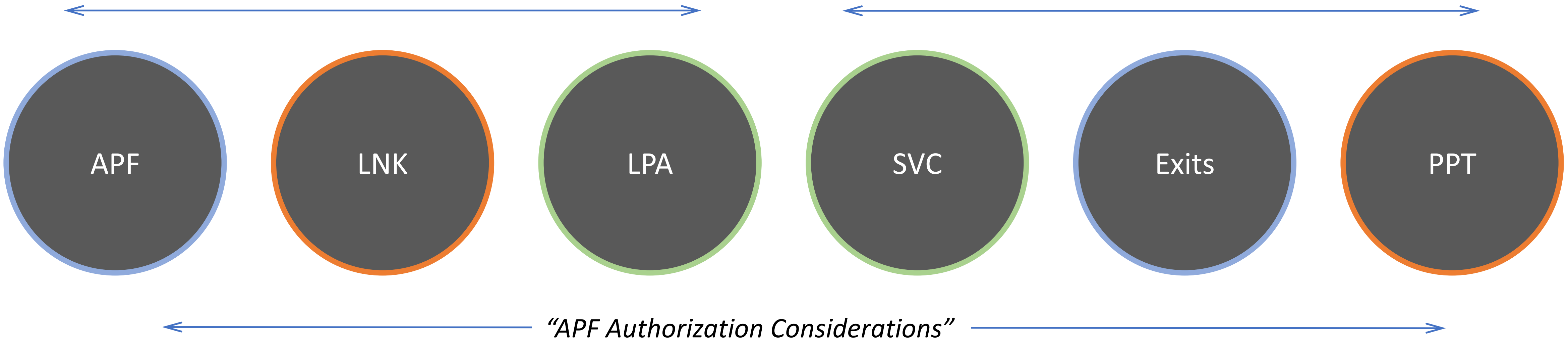
```
*---+----1----+----2----+----3----+----4----+----5----+----6----+----7
HWNAME h1
LPARNAME l1
VMUSERID v1
ARCHLVL a
DYNCPADD { nnnn | ENABLE | DISABLE}
IEASYM [xx]
          [(xx,yy,zz,...,L)]
INITSQA xxxxK  yyyyK
           xxxxM  yyyyM
IODF xx  hiqualif  configid  id  y  s
MACHMIG x1,x2,...,xn
MTLSHARE {Y | N}
NUCLEUS n
NUCLST nn  y
PARMLIB dsn                                   [volid]
                                               [******]
                                               [*MCAT*]

PROCVIEW {CORE | CPU | CORE,CPU_OK}
SYSCAT volserxycsdsname  hlqtvc
SYSPARM [xx]
           [(xx,yy,zz,...,L)]
SYSPLEX plexname
```

01-04 - IODF Keyword
10-11 - IODF DS Suffix, if “01” then Dataset name would be IODF01
13-21 - IODF DS High Level Qualifier, if “SYS1” then fully qualified = SYS1.IODF01
22-29 - OS configuration identifier used to select named OSCP from the IODF DS
31-32 - The Eligible Device Table associated with a named OSCP configuration
34-34 - “Y” to load all IODF defined devices & any other dynamically available devices
36-36 - “S” the subchannel set to be used during an IPL – Specify 0,1,2,3 or *

When PROCVIEW CPU is in effect, DYNCPADD applies to CPUs. When PROCVIEW CORE is in effect, DYNCPADD applies to cores. Remains unchanged for the duration of the IPL.

5 - Post IPL - The z System Environment

These are loaded before the system is operational. Therefore, during the IPL their referential integrity cannot be fully validated.



APF

LNK

LPA

SVC

Exits

PPT

“APF Authorization Considerations”

APF Datasets are defined to the system at a very early stage of the IPL process. As a result the system has no knowledge of their actual existence and loads “as is”. Errors in naming lead to Post-IPL APF vulnerabilities if they are allocated

LINKLST Datasets are APF-authorized when IEASYS value LNKAUTH is set =LNKLST and a fetch is done using that dataset as part of the LNKLST but not when using that dataset as part of JOBLIB/STEPLIB/TASKLIB or any user-opened-DCB.

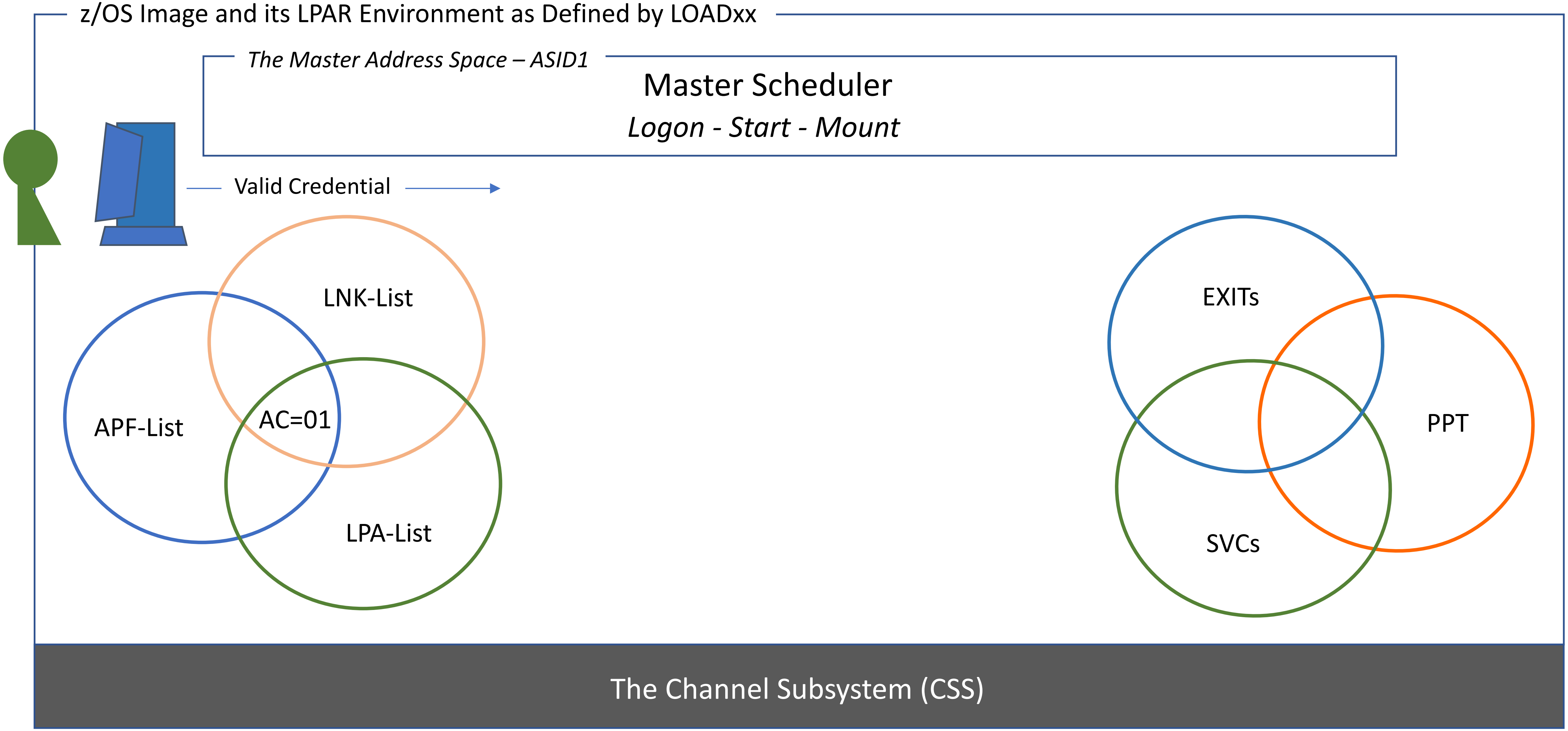
If a library is in the LNKLST concatenation but is not APF-authorized, the system will consider the library to be unauthorized for the duration of the job or step if the library is referred to through a JOBLIB or STEPLIB DD statement.

It is not necessary for the datasets in the LPALST to be APF-authorized. However, any module in the link pack area (pageable, modified, fixed, or dynamic LPA) is treated by the system as though it came from an APF authorized library

PSW keys 0 - 7 are used by the z/OS base control program (BCP) and various subsystems and middleware. Key 0 is the master key. PSW keys 8 through 15 are assigned to users. The Program Properties Table can be used to modify expected PSW key values

Properly protect LNK and LPA data set to avoid system security and integrity exposures, just as you would any APF-authorized library.

5 - Post IPL - The z System Environment


z/OS Image and its LPAR Environment as Defined by LOADxx

The Master Address Space – ASID1

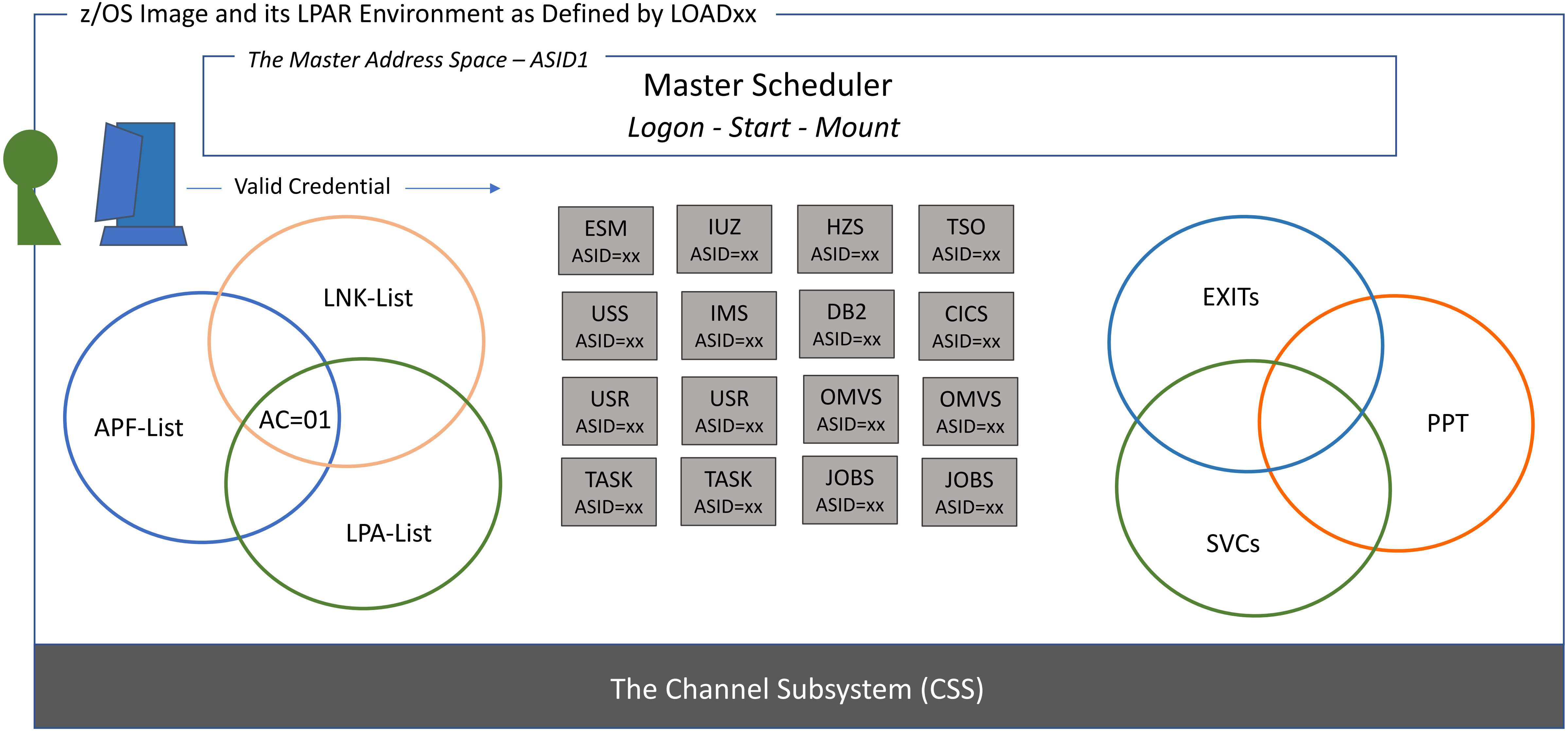
Master Scheduler

Logon - Start - Mount

Valid Credential

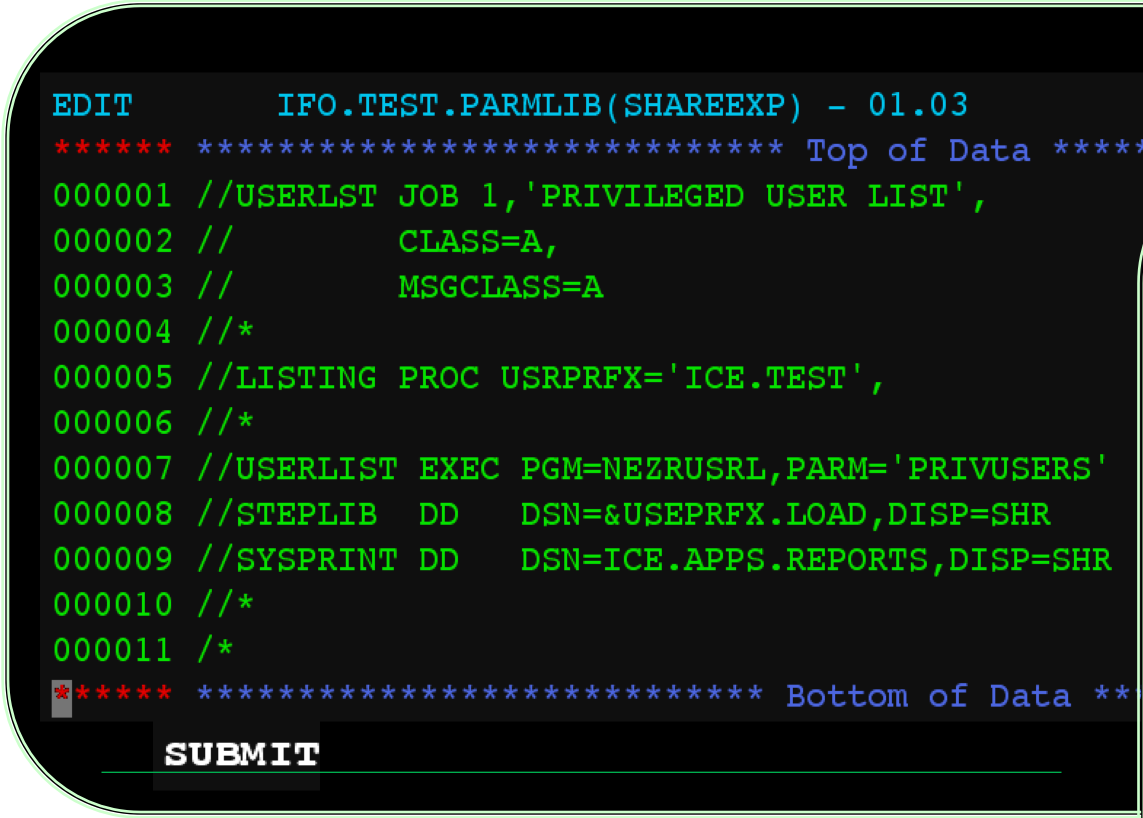
The Channel Subsystem (CSS)

5 - Post IPL - The z System Environment

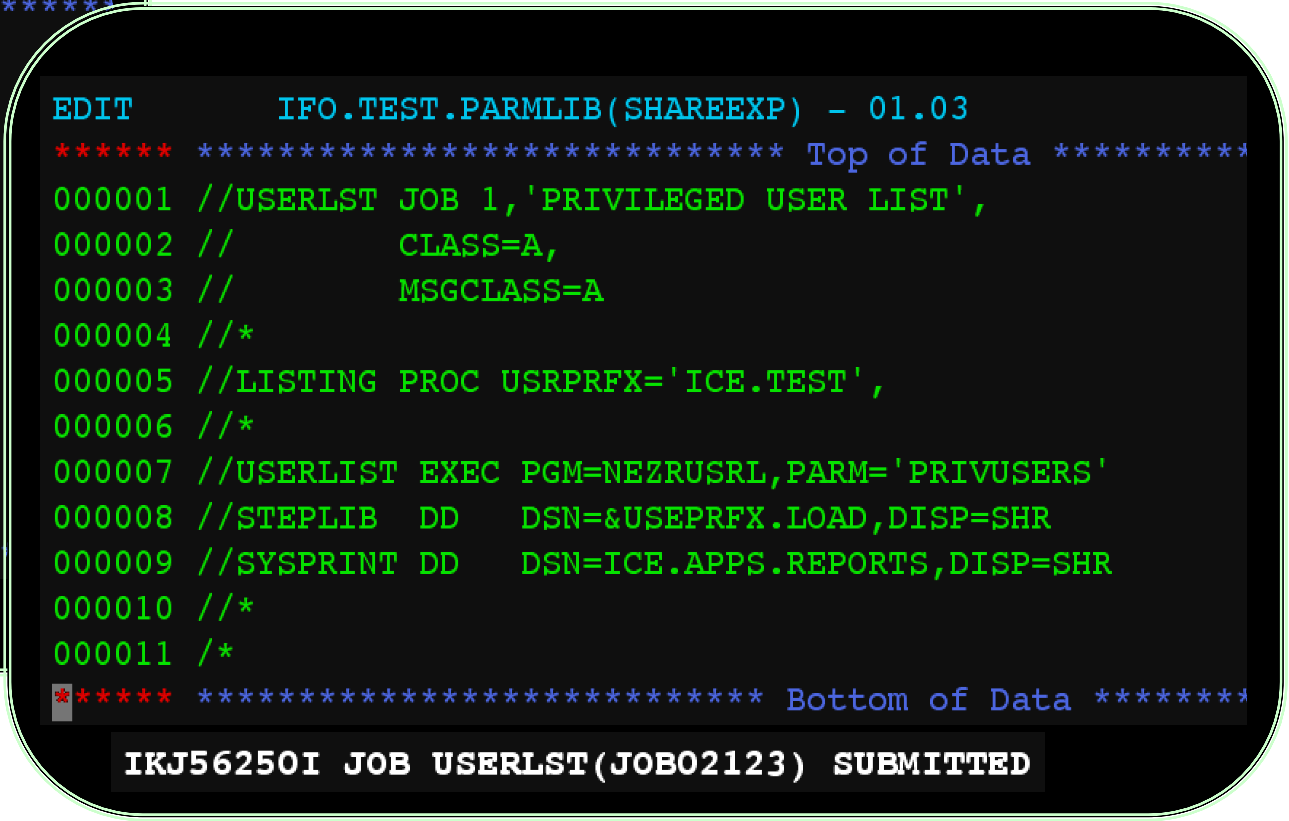

z/OS Image and its LPAR Environment as Defined by LOADxx
The Master Address Space – ASID1
Master Scheduler
Logon - Start - Mount
Valid Credential
LNK-List
APF-List
AC=01
LPA-List
EXITs
PPT
SVCs
The Channel Subsystem (CSS)

ESM ASID=xx	IUZ ASID=xx	HZS ASID=xx	TSO ASID=xx
USS ASID=xx	IMS ASID=xx	DB2 ASID=xx	CICS ASID=xx
USR ASID=xx	USR ASID=xx	OMVS ASID=xx	OMVS ASID=xx
TASK ASID=xx	TASK ASID=xx	JOBS ASID=xx	JOBS ASID=xx

5 - Post IPL - The z System Environment



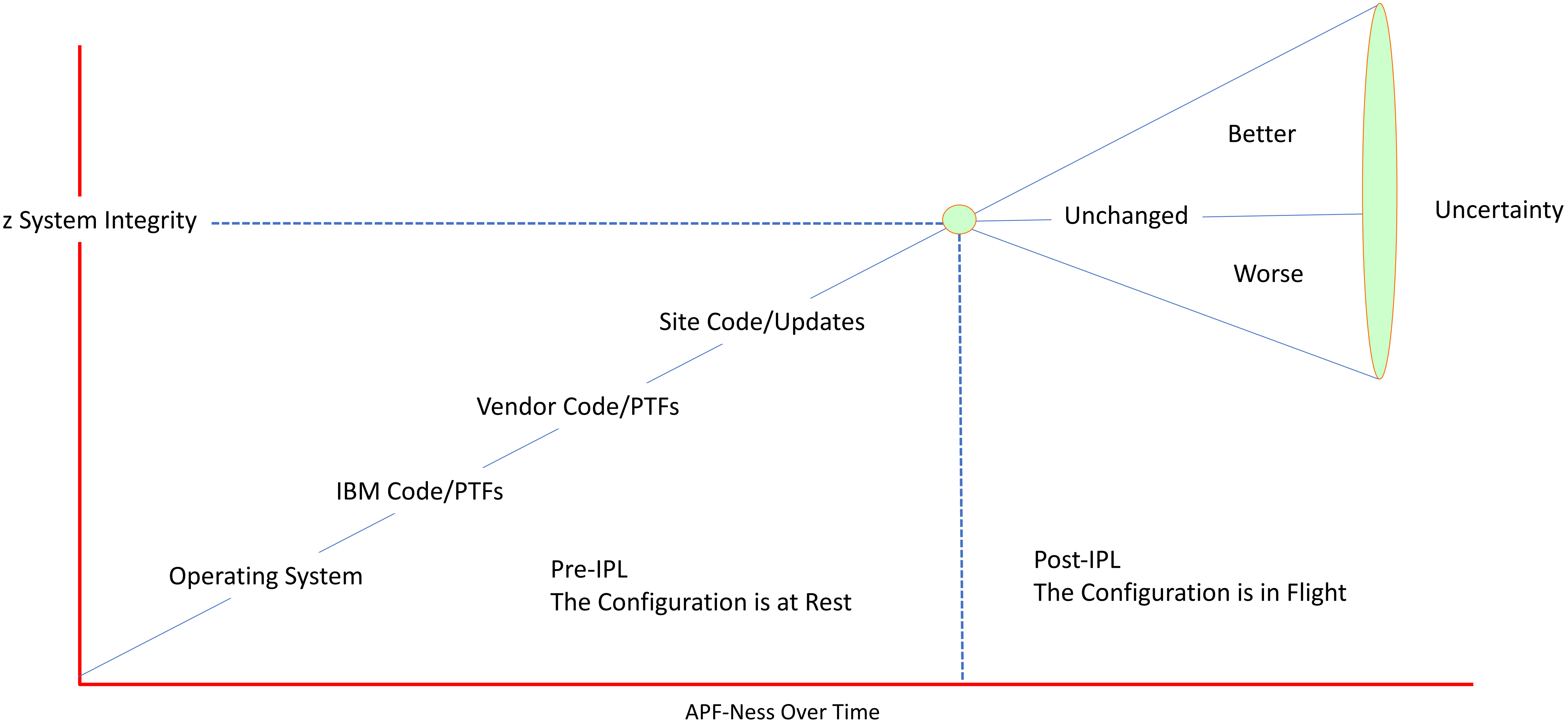
```
EDIT       IFO.TEST.PARMLIB(SHAREEXP) - 01.03
****** ***************************** Top of Data **********
//USERLST JOB 1,'PRIVILEGED USER LIST',
//        CLASS=A,
//        MSGCLASS=A
//*
//LISTING PROC USRPRFX='ICE.TEST',
//*
//USERLIST EXEC PGM=NEZRUSRL,PARM='PRIVUSERS'
//STEPLIB  DD   DSN=&USEPRFX.LOAD,DISP=SHR
//SYSPRINT DD   DSN=ICE.APPS.REPORTS,DISP=SHR
//*
/*
****** **************************** Bottom of Data **
   SUBMIT
```



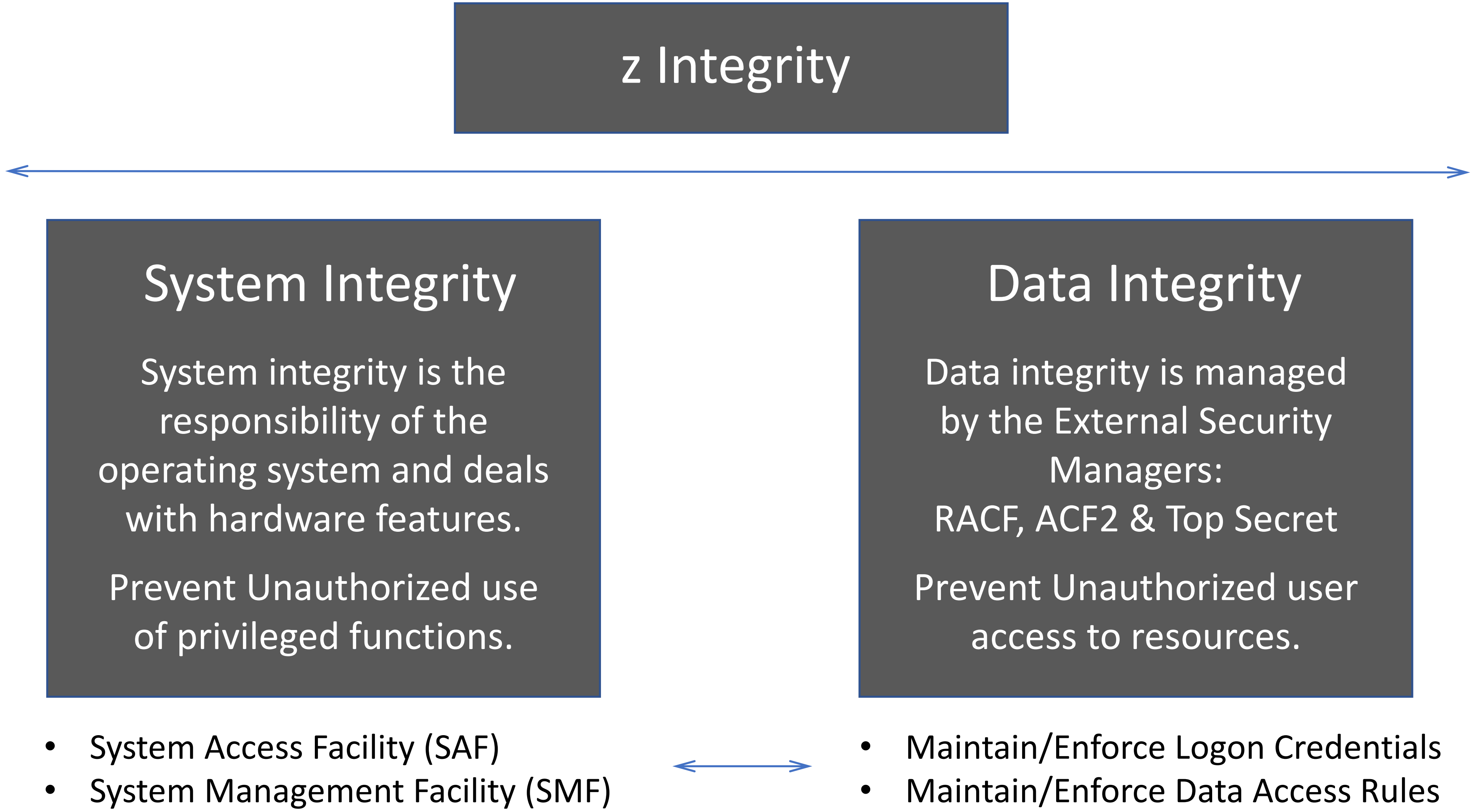
```
EDIT       IFO.TEST.PARMLIB(SHAREEXP) - 01.03
****** ***************************** Top of Data **********
//USERLST JOB 1,'PRIVILEGED USER LIST',
//        CLASS=A,
//        MSGCLASS=A
//*
//LISTING PROC USRPRFX='ICE.TEST',
//*
//USERLIST EXEC PGM=NEZRUSRL,PARM='PRIVUSERS'
//STEPLIB  DD   DSN=&USEPRFX.LOAD,DISP=SHR
//SYSPRINT DD   DSN=ICE.APPS.REPORTS,DISP=SHR
//*
/*
****** **************************** Bottom of Data ********
   IKJ56250I JOB USERLST(JOB02123) SUBMITTED
```

On IBM mainframe systems *Job Entry Control Language* or *JECL* is the set of command language control statements that provide information for the spooling subsystem – JES2/JES3 - Wikipedia

5 - Post IPL - The z System Environment



6 - z System Integrity



z Integrity

System Integrity

System integrity is the responsibility of the operating system and deals with hardware features.

Prevent Unauthorized use of privileged functions.

- System Access Facility (SAF)
- System Management Facility (SMF)

Data Integrity

Data integrity is managed by the External Security Managers:
RACF, ACF2 & Top Secret

Prevent Unauthorized user access to resources.

- Maintain/Enforce Logon Credentials
- Maintain/Enforce Data Access Rules

IBM System Integrity

6 - z System Integrity

System Integrity is IBM's commitment, design, and development practices intended to prevent unauthorized application programs, subsystems and users from bypassing system security–that is, to prevent them from gaining access, circumventing, disabling, altering or obtaining control of key system processes and resources unless allowed by the installation.

Authorized Program Facility (APF)

Allows the authorization of system-level programs to access/use privileged Instructions in order to modify or extend the basic z/OS functions.

For a Module to become APF Authorized:

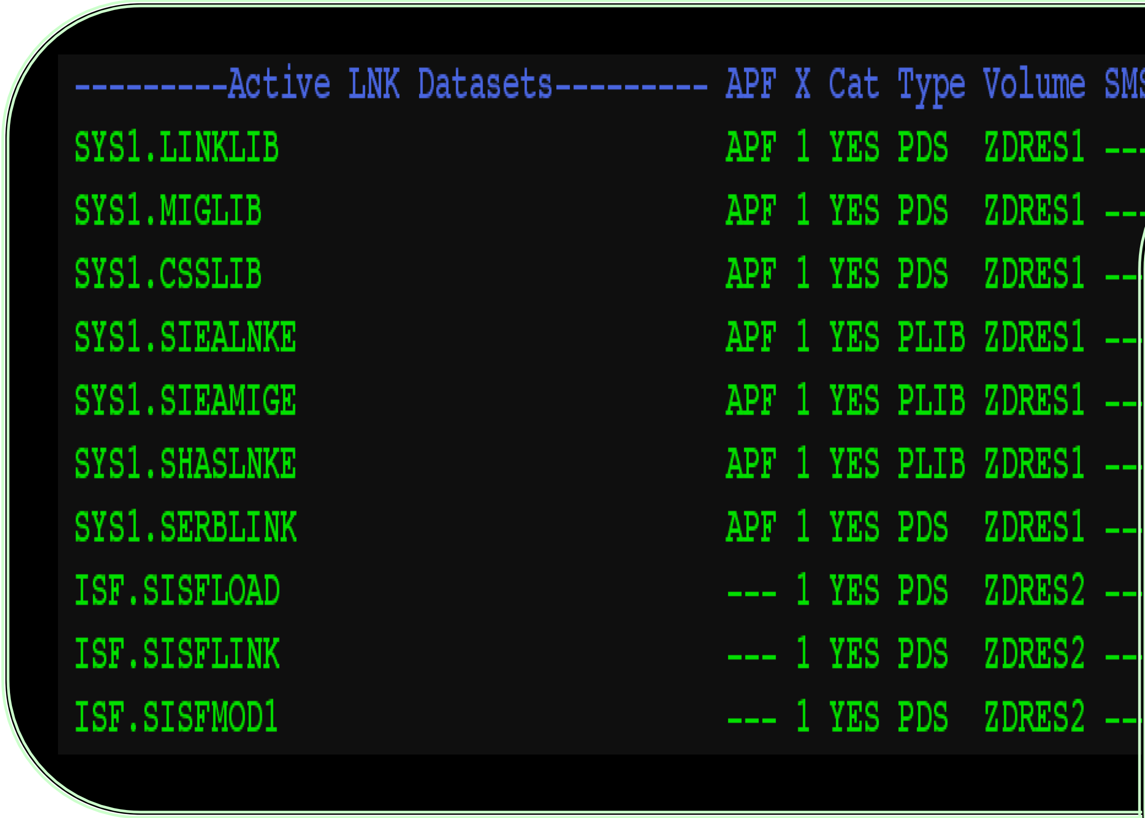
1. It must Reside in a APF Dataset
2. Be Link Edited AC Code of (01) or
3. Reside in the Link Pack Area (LPA)

Abuse of APF Authorization will result in a loss of System Integrity and Security!

IBM z/OS® System Integrity Statement

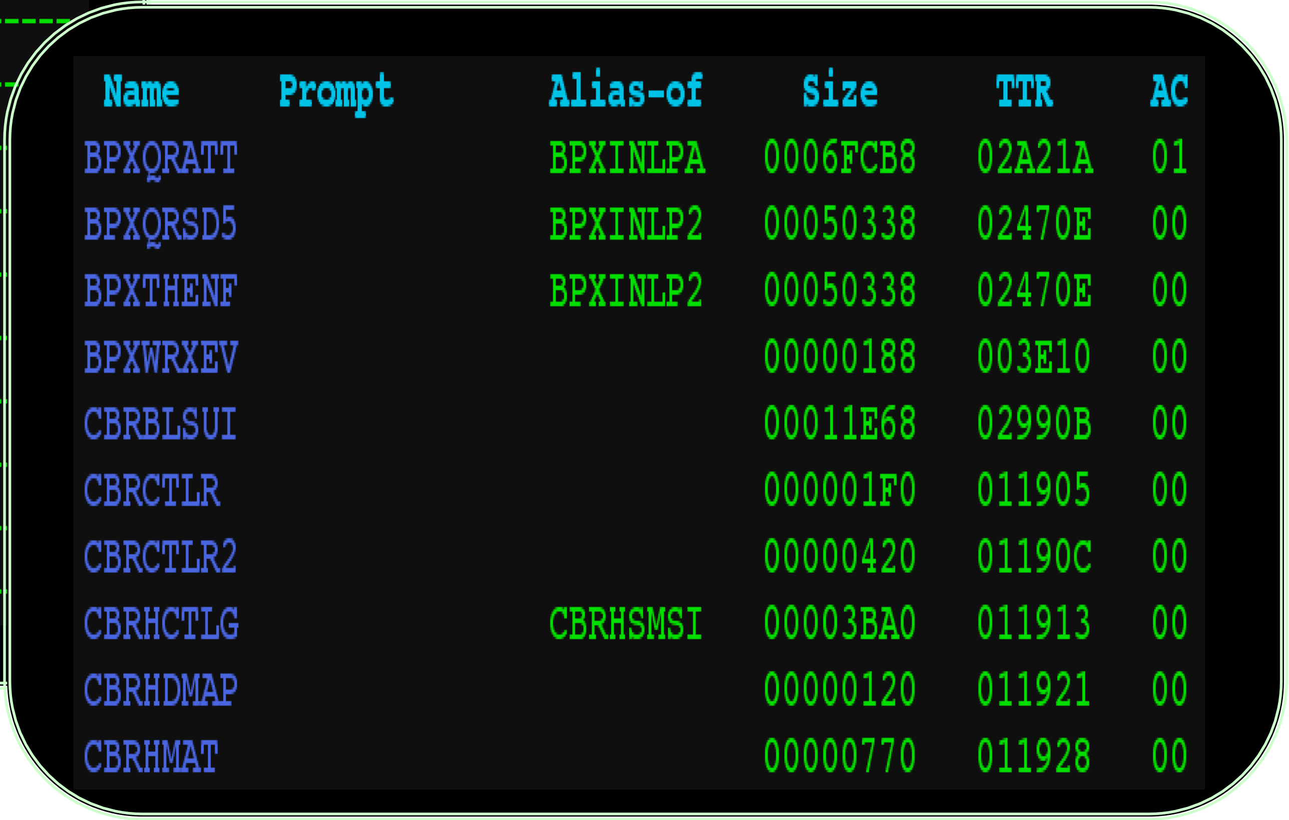
6 - z System Integrity

APF Authorized Libraries



```
---------Active LNK Datasets--------- APF X Cat Type Volume SMSVol
SYS1.LINKLIB                          APF 1 YES PDS  ZDRES1 ------
SYS1.MIGLIB                           APF 1 YES PDS  ZDRES1 ---
SYS1.CSSLIB                           APF 1 YES PDS  ZDRES1 --
SYS1.SIEALNKE                         APF 1 YES PLIB ZDRES1 --
SYS1.SIEAMIGE                         APF 1 YES PLIB ZDRES1 --
SYS1.SHASLNKE                         APF 1 YES PLIB ZDRES1 --
SYS1.SERBLINK                         APF 1 YES PDS  ZDRES1 --
ISF.SISFLOAD                          --- 1 YES PDS  ZDRES2 --
ISF.SISFLINK                          --- 1 YES PDS  ZDRES2 --
ISF.SISFMOD1                          --- 1 YES PDS  ZDRES2 --
```

Any AC(01) Module in APF Libraries



```
 Name      Prompt        Alias-of   Size      TTR     AC
BPXQRATT                 BPXINLPA   0006FCB8  02A21A  01
BPXQRSD5                 BPXINLP2   00050338  02470E  00
BPXTHENF                 BPXINLP2   00050338  02470E  00
BPXWRXEV                            00000188  003E10  00
CBRBLSUI                            00011E68  02990B  00
CBRCTLR                             000001F0  011905  00
CBRCTLR2                            00000420  01190C  00
CBRHCTLG                 CBRHSMSI   00003BA0  011913  00
CBRHDMAP                            00000120  011921  00
CBRHMAT                             00000770  011928  00
```

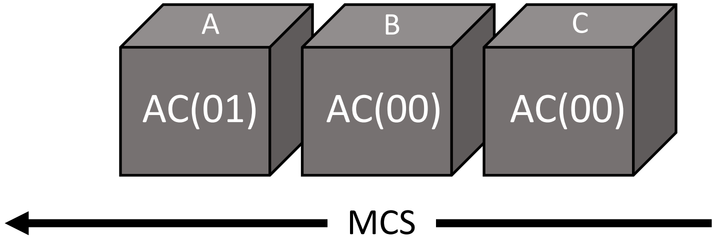
Just take a Look-See using TSO/ISPF 3.4!

6 - z System Integrity

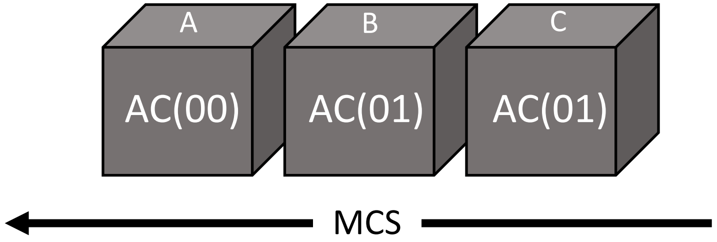
A Program’s “Module Calling Sequence” will determine if it’s APF Authorized!

- The “Module Calling Sequence” (MCS) represents the order in which modules are concatenated together in order to build “Complete” Program Functions.
- The ”Lead Off” Module in the MCS must be Link Edited AC(01) for the Program to achieve Authorized Program Status.
- Except for the “Lead Off” Module all other modules in the ‘”Module Calling Sequence” all others need NOT be Link Edited AC(01) but they must all come from APF Authorized Datasets for the Program to gain Authorized Program Status or APF Authorized sources, i.e. System Link Pack Area (LPA).
- Upon execution of an Authorized Program all modules are treated “as if’ they are AC(01).

Good to go!



Not so much!

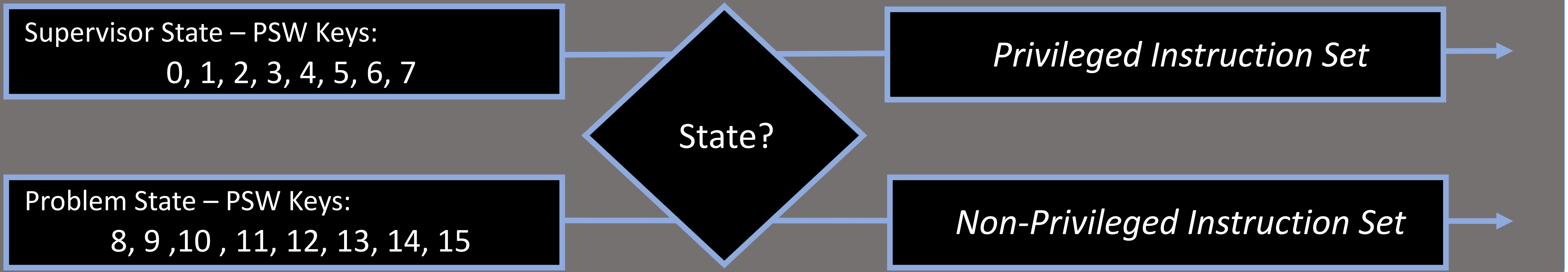


7 - Program Authorization

As a general statement, Privileged instructions are intended for OS supervisory functions. If by intent or not they may be used to compromise other users or the entire z Environment.

z/OS operates in either of two states: *Problem or Supervisor/System State. Which is determined by the value of their Program Status Word (PSW).*

- *Programs with a PSW in the range of 0-7 operate in Supervisor State - execute privileged instructions.*
- *Programs with a PSW in the range of 8-15 operate in Problem State - execute non-privileged instructions.*



Supervisor State – PSW Keys:
0, 1, 2, 3, 4, 5, 6, 7

Problem State – PSW Keys:
8, 9 ,10 , 11, 12, 13, 14, 15

State?

Privileged Instruction Set

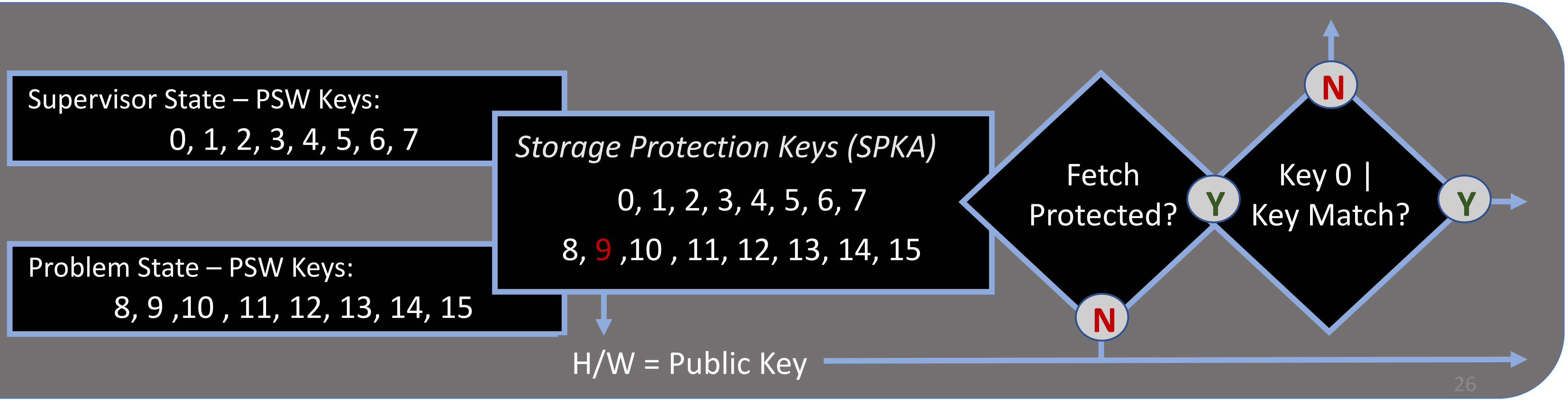
Non-Privileged Instruction Set

7 - Program Authorization

Storage KEYs (SPKA) range from 0 to 15. 0-7 are "system keys”. 8-15 are considered "user keys”. Key 9 is a "public key" to which normal KEY checking does not apply. KEY 9 is a hardware implementation.

- *A program with any PSW KEY can READ storage that is not fetch-protected. Only a program with PSW KEY 0 or with PSW KEY exactly matching the storage KEY can READ fetch-protected storage, unless KEY 9.*
- *A program with PSW KEY 0 can WRITE into storage of any key. A program with PSW KEY 1-15 can WRITE into storage only of that exact KEY or KEY=9.*

Therefore, when in PSW KEY 0, a program can do whatever!

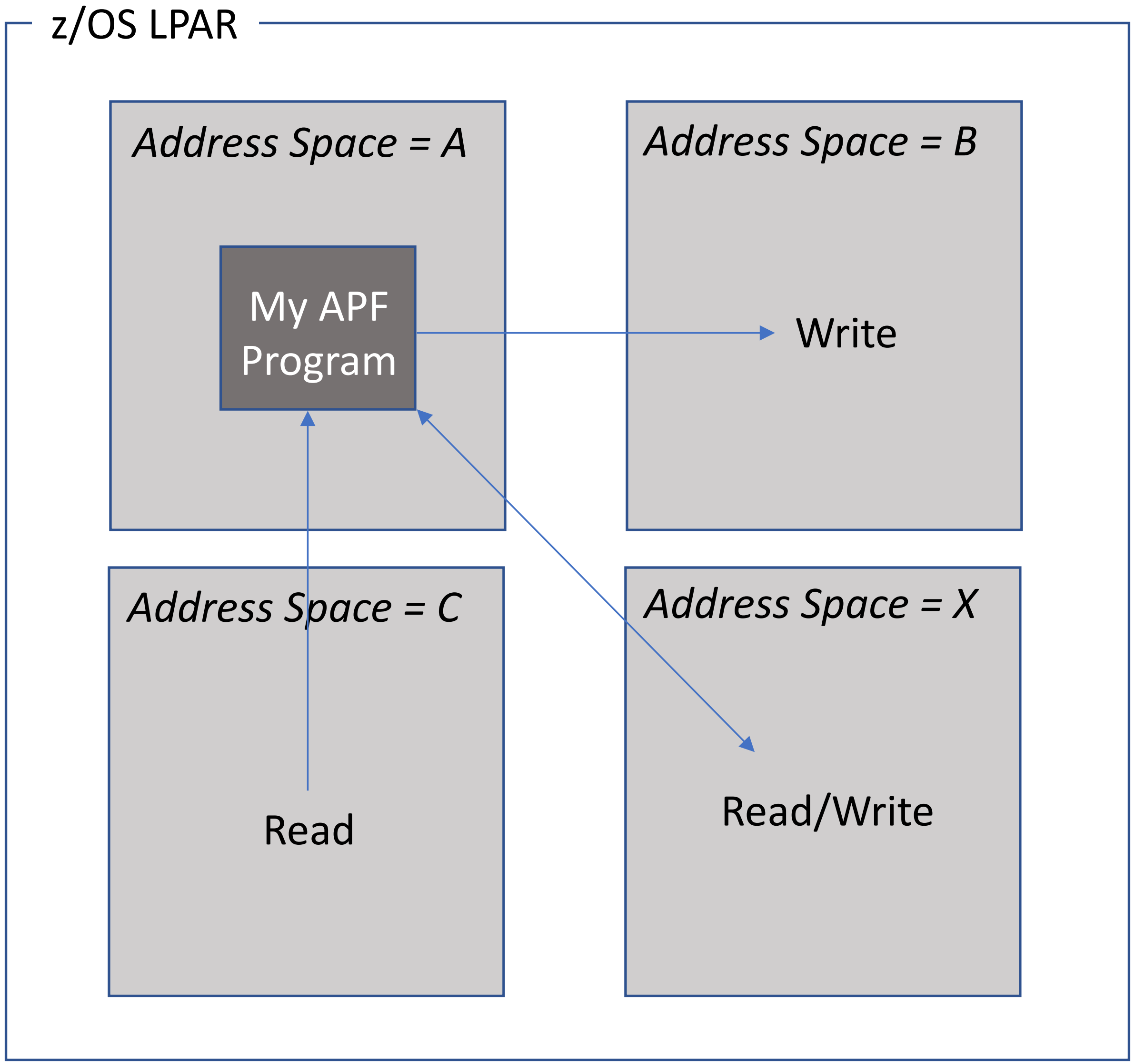


Supervisor State – PSW Keys:
0, 1, 2, 3, 4, 5, 6, 7

Problem State – PSW Keys:
8, 9 ,10 , 11, 12, 13, 14, 15

Storage Protection Keys (SPKA)
0, 1, 2, 3, 4, 5, 6, 7
8, 9 ,10 , 11, 12, 13, 14, 15

7 - Program Authorization



Question:

Can My APF Authorized program (from a valid APF Authorized Dataset marked AC(01) in one Address Space (A) Read from or Write to the memory of any other Address Space – B, C, X?

Answer:

If the Target Memory is not Fetch Protected, no problem.

If operating in Supervisor State, PSW KEY=0, no problem!

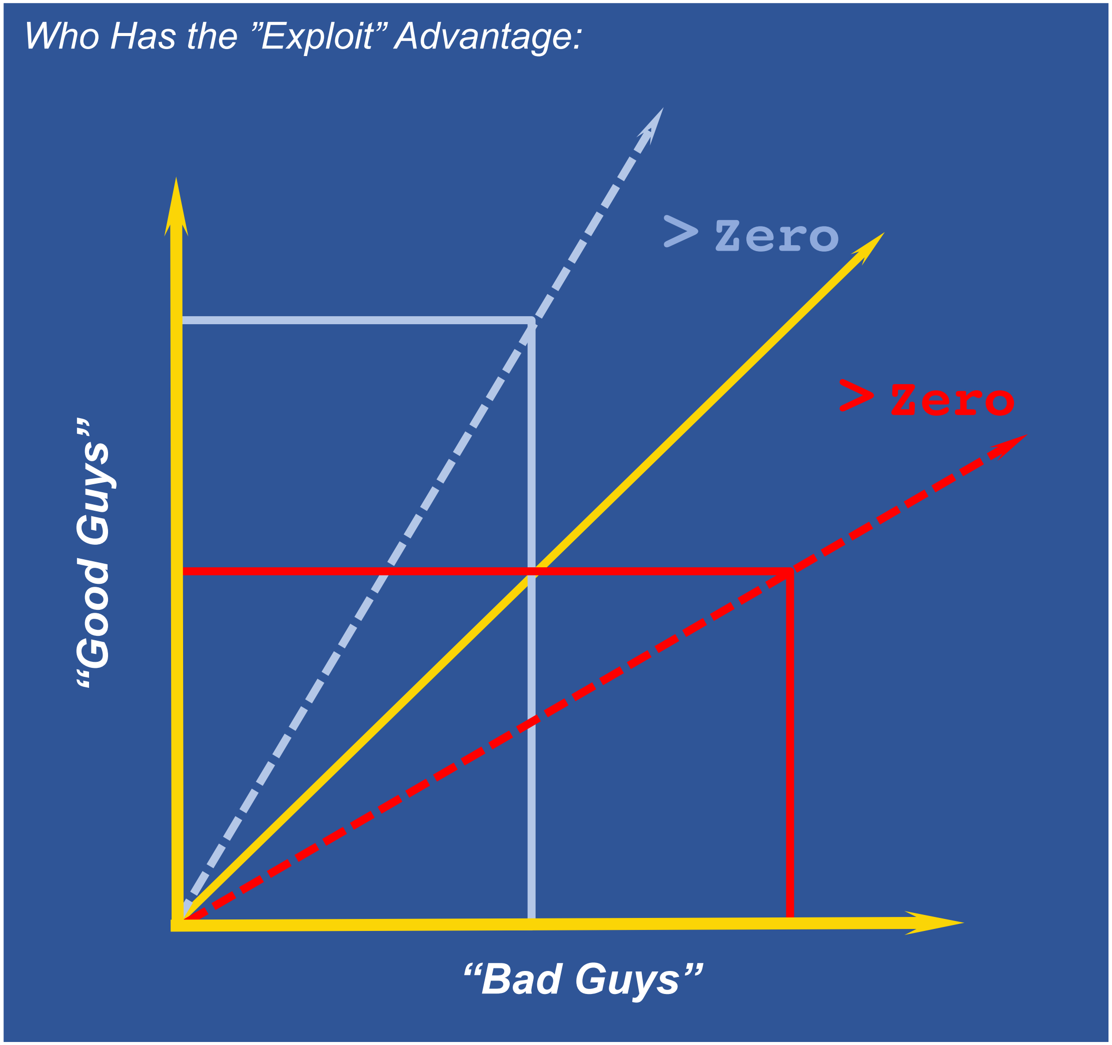
If Target Memory is Fetch Protected and the PSW Key of My APF matches the SPKA or the Target Memory, no problem.

If operating in PSW Key ”ZERO”, no problem. You have the Key to the “Kingdom”!

7 - Program Authorization

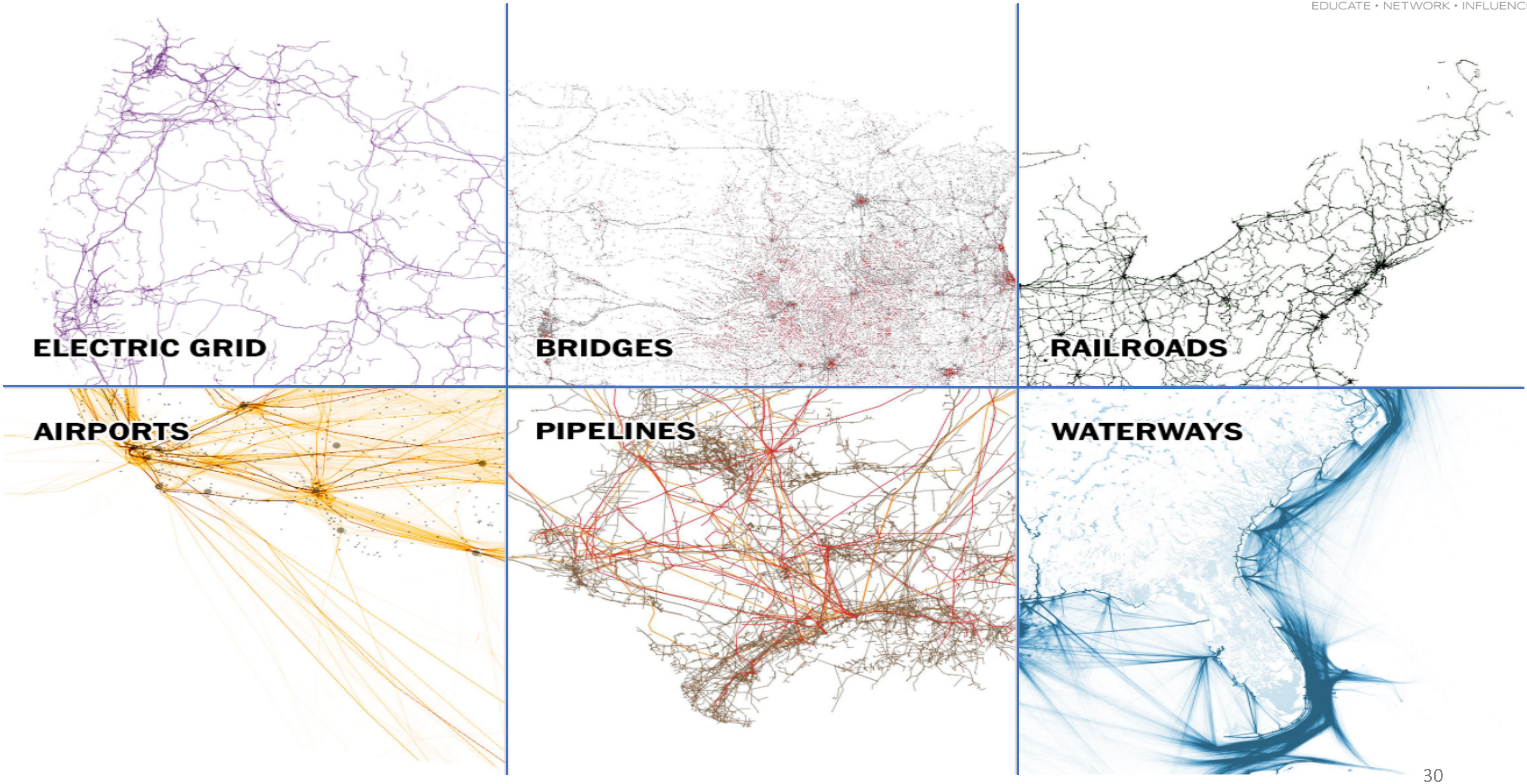
- Note that giving WRITE or higher access to an APF authorized library is analogous to giving a Linux user root authority. Users with WRITE or higher access to an APF authorized library can do anything they want to the system:
- As an APF authorized program I can issue SAF calls (RACROUTE) to create and delete security credentials with NO extraordinary RACF privileges
- Read/update the RACF database as an APF authorized program with NO extraordinary RACF privileges
- By giving someone update access to an APF authorized library you are saying "they can invoke ANY API that is available on this system that would normally be restricted. ANY of the restricted APIs
- MODESET can get you into and out of supervisor state and into key 0 or 8. To get into other keys, you would issue an SPKA instruction.
- The thing about supervisor state, key 0 is that you can access any storage in any key in any address space. When you are in supervisor state, non-zero key, you can access all storage in the key you are in and all storage you own, but the operating system protects you from accessing other storage.
- It's the job of the application/program to set the key and to request the key assigned to allocated storage. Some storage subpools have system-defined keys. But for all intents and purposes, it's the program itself that controls those values.
- Is correct when he says AC(1) does not give you either key 0 or supervisor state. It does give you the variations of MODESET that issue an SVC, and that can give you key 0 and supervisor state.
- It can change to supervisor state; it can to whatever key it wants to be running in - that is why the access to APF libraries is of such high concern to auditors.

8 - System Vulnerabilities

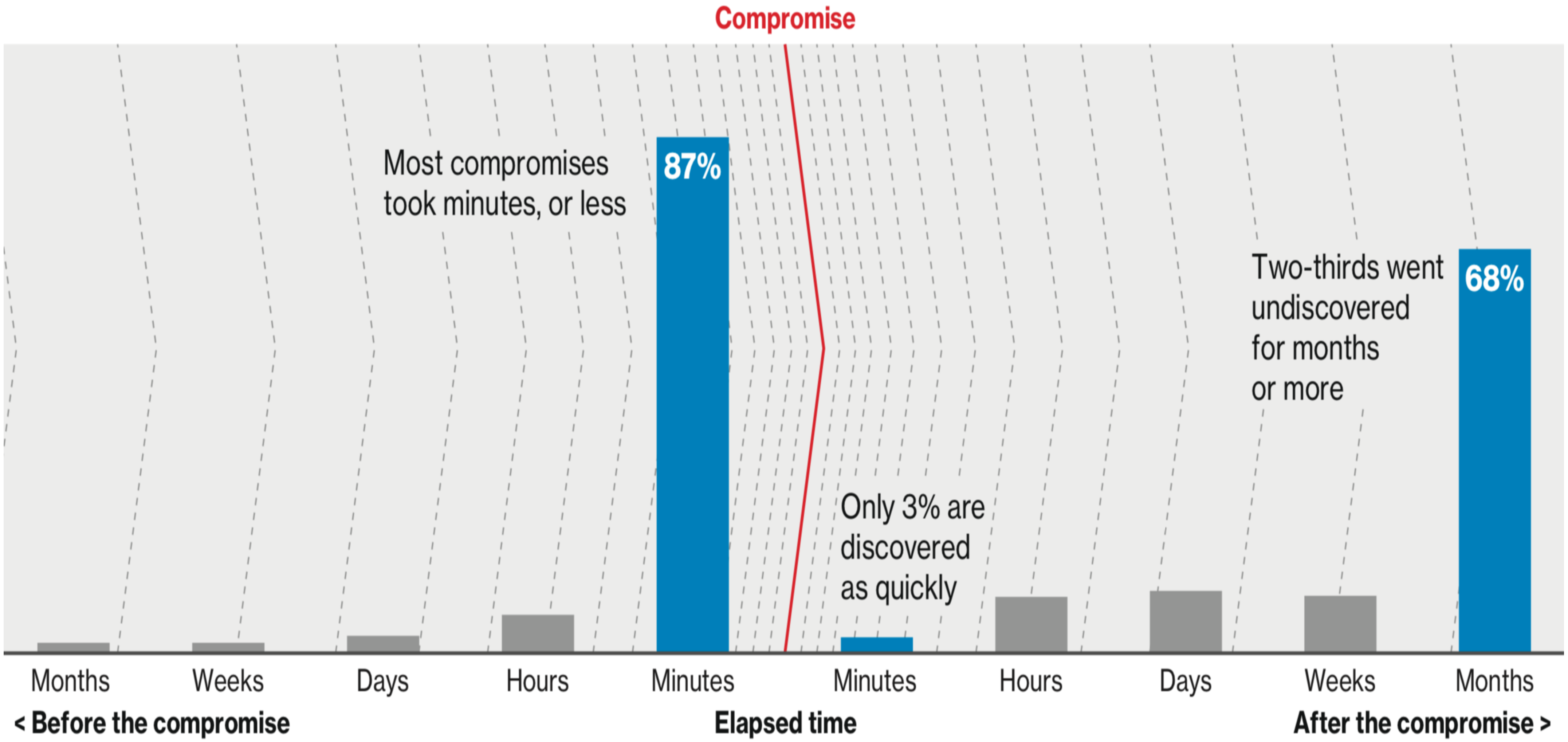


A System is Considered Secure when "Bad Guys" have a Negligible Advantage over "Good Guys".

8 - System Vulnerabilities



8 - System Vulnerabilities



* Verizon's 2017 Data Breach Investigations Report

Those that result from lax User Credential Control
Those that result from Over Privileging Users

Those that result form Configuration Errors
Those that result from Code Based Errors

8 - System Vulnerabilities

First Response & Health Care

Auto, Home, Life Insurance

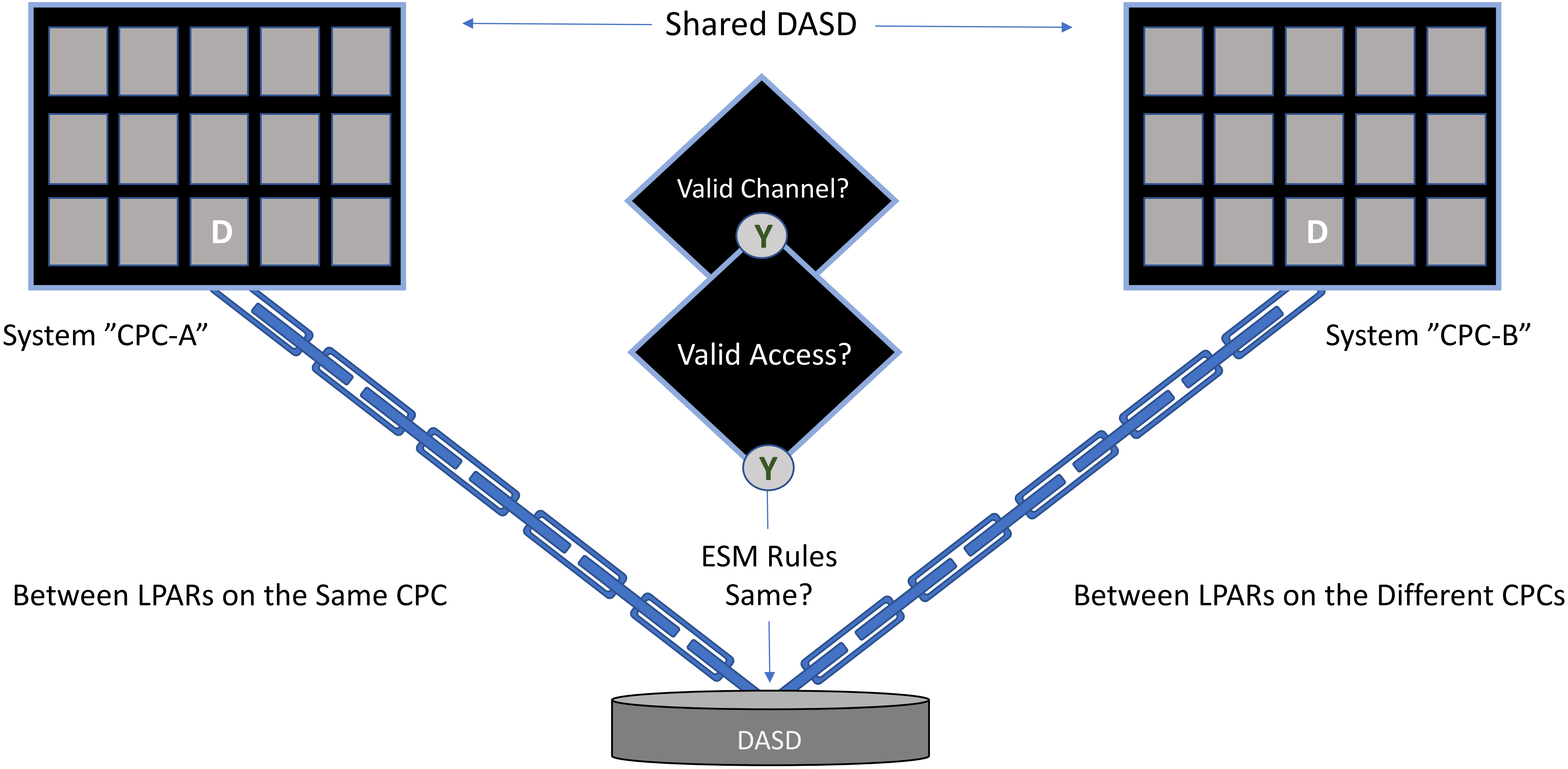
Finance & Banking

Federal & State Governments

Intel & Defense Agencies

Mining & Manufacturing

8 - System Vulnerabilities



Shared DASD

System ”CPC-A”

System ”CPC-B”

Valid Channel?

Y

Valid Access?

Y

ESM Rules Same?

Between LPARs on the Same CPC

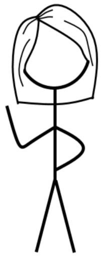
Between LPARs on the Different CPCs

[The RACF remote sharing facility (RRSF)](#)

8 - System Vulnerabilities

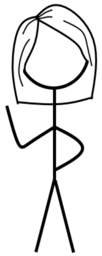
Pervasive DS Encryption - Don't Misplace Your Master Key!

Separation of Duties and Responsibilities



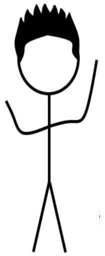
System Programming

- Key Life Cycle
- ICSF



Storage Administration

- Dataset Management
- DFSMF



Security Administration

- Dataset Access
- RACF, ACF2, TSS

Long/Short-term data storage can be securely managed without exposing content to administrators/others.

```
ICSF     - Integrated Cryptographic Services Facility
DSFMF    - Assign attributes to data sets and objects so system can auto manage storage
```

8 - System Vulnerabilities

Code Based Vulnerabilities may exist:

Controlling access to Supervisor/System State and therefore restricting access to privileged instructions is a critical first step in preventing vulnerabilities that expose system memory, control functions, integrity and security.

By intent or not, a program, like the sample shown, operating authorized can, as in this case, use the MODESET instruction to move into and out of Supervisor/System State.

Such “State Switching” could give the program unintended powers to READ Memory, as in this case, to extract the PSW Key using other privileged instruction. Change the Key Value as needed and then replace the old value with the new, thus changing the PSW/SPKA key association.

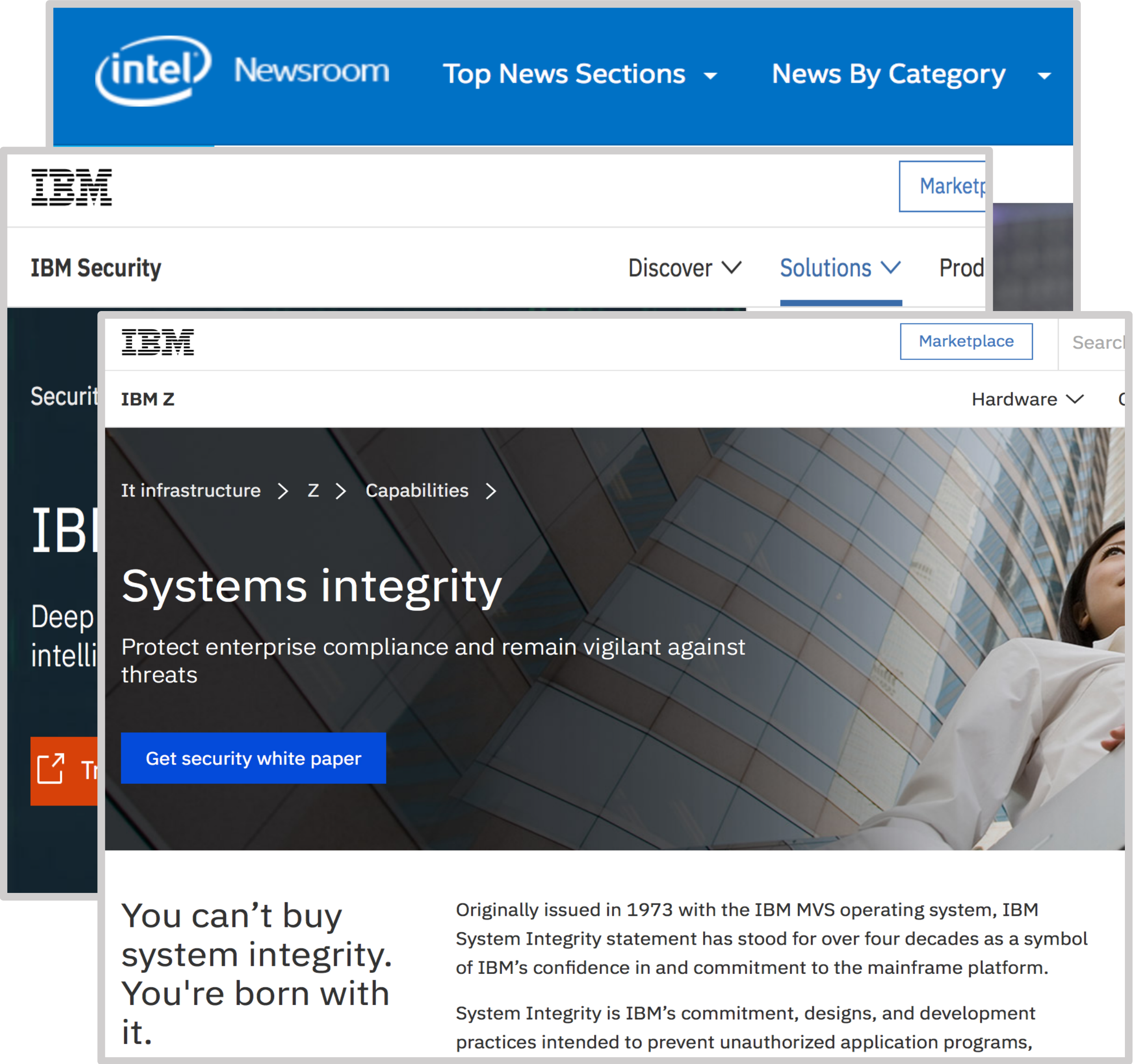
```
TESTAUTH STATE=YES,RBLEVEL=1  TEST STATE
STC    R15,STATE              SAVE IT
LA     R2,0
MODESET MODE=SUP              CAPTURE KEY
IPK                           GET KEY R2
MODESET MODE=PROB,KEY=NZERO   SET KEY
ST     R2,KEY                 SAVE KEY
.
.
.
.
MODESET MODE=SUP
L      R2,KEY
SPKA   0(R2)                  REVERT KEY
CLI    STATE,0                SUP. STATE
BE     RETURN2                YES
MODESET MODE=PROB
```

Never forget PSW Key 0 is the Key to the “Kingdom”!

Ray Overby, CEO Key Resources

8 - System Vulnerabilities

IBM utilizes several internal and external sources as input to the security and system integrity process to assist IBM as it investigates and works on vulnerabilities that might potentially affect IBM Z. So should you! [US-CERT | United States Computer Emergency Readiness Team]



Systems integrity

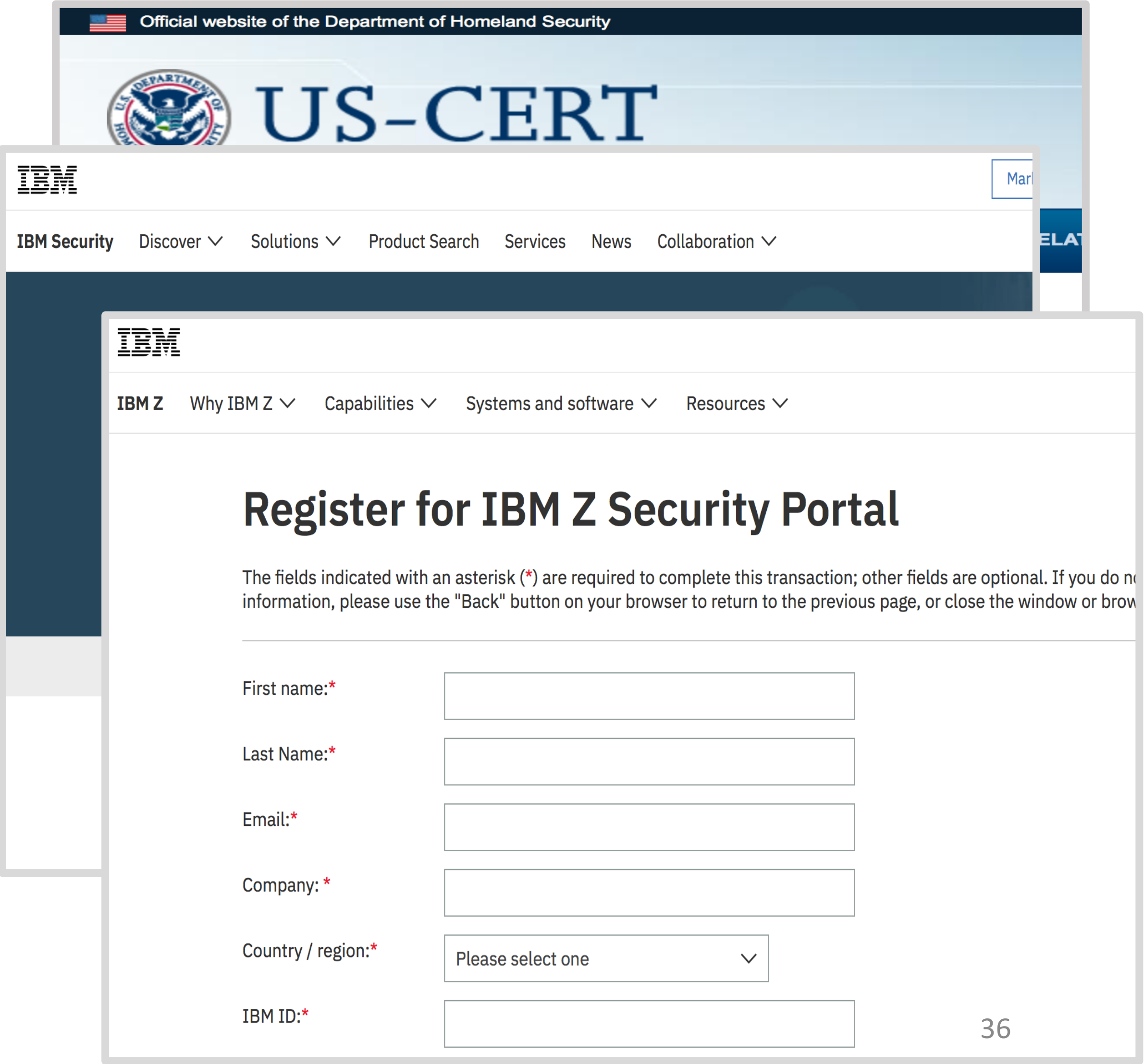
Protect enterprise compliance and remain vigilant against threats

Get security white paper

You can't buy system integrity. You're born with it.

Originally issued in 1973 with the IBM MVS operating system, IBM System Integrity statement has stood for over four decades as a symbol of IBM's confidence in and commitment to the mainframe platform.

System Integrity is IBM's commitment, designs, and development practices intended to prevent unauthorized application programs,



Register for IBM Z Security Portal

The fields indicated with an asterisk (*) are required to complete this transaction; other fields are optional. If you do n information, please use the "Back" button on your browser to return to the previous page, or close the window or brow

First name:*

Last Name:*

Email:*

Company: *

Country / region:* Please select one

IBM ID:*

9 - Language Index

Glossary of Terms:

1. APAR - Authorized Program Analysis Report describes problem, formally tracked until resolved
2. APF - Authorized Program Facility
3. ASID - The Numeric Address Space Identifier
4. BCP - The Base Control Program - Backbone of z/OS Reliability and Integrity
5. CBPDO - Custom-Built Product Delivery Option
6. CF - Channel Facility
7. CPC - The Central Processing Complex
8. CPACF - CP Assist for Cryptographic Functions
9. CLI - Compare Logical Intermediate - In snippet - test for change in State
10. CSS - Channel Sub-System — Controls data flow input/output.
11. CHPID - Channel Path Identifier — a logical disignation
12. CMT - CHPID Mapping Tool — Maps Logical to Physical Channels
13. DASD - Direct Access Storage Device
14. DEB - Data Extent Block build on OPEN of DCB (Data Control Block). Can examine but not change
15. DPM - Dynamic Partition Manager — Linux specific Partition Management
16. DUCT - Dispatchable Unit Control Table - Control over the Authority State
17. DSFMF - Assign attributes to data sets and objects so system can auto manage storage
18. EDT - Eligible Device Table
19. EOS - End of Service — a date
20. ESM - External Security Manager

9 - Language Index

Glossary of Terms:

21. ESP - Early Support Program
22. FICON - Fiber Connection - FICON has replaced ESCON
23. GDPS - Geographically Disbursed Sysplex
24. HCD - Hardware Configuration Definition
25. HMC - Hardware Management Console
26. HSA - Hardware Storage Area
27. ICSF - Integrated Cryptographic Services Facility
28. IFL - Integrated Facility for Linux – A System Assist Processor(SAP)
29. IMSI - Initialization Message Suppression Indicator
30. IOCP - I/O Configuration Program – Hardware Portion of IODF
31. IODF - Input/Output Definition File - HCD - IOCP, OSCP and SWCP
32. IOCDS - Input/Output Configuration Dataset, same as IOCP
33. IPK - Insert PSW Key - A privileged Instruction - See snippet
34. IRIM - IPL Resource Initialization Modules
35. JCL - JOB Control Language – used to submit job to z/OS
36. LCSS - Logical Channel Sub-System – Up to 6 in a z14 each supports up to 15 LPARs
37. LPAR - Logical Partition – Up to 85 in a z14
38. LTSR - Long-Term Support Release – 2yrs Minimum, 1yr extension is optional at EOS
39. MODESET - Change system status - alter PSW/PKM or State Indicator
40. NIPCON - A named Console Device used only during a system IPL

9 - Language Index

Glossary of Terms:

41.NIPS – Nucleus Initialization Processing

42.OSCP – Operating System Control Program — Software portion of IODF

43.PCIe – Peripheral Component Interconnect Express

44.PCHID – Physical Channel Identifier - Up to 256 in a z14, shared by all CHPIDs

45.PDE — Pervasive Dataset Encryption

46.PTF – Program Temporary Fix — When applied resolves a related APAR — FIX Package FIXPCK

47.PU – Processor Unit — Up to 107 in a single z14 CPC

48.RCT – Region Control Task - Highest priority Task in Address Space - Controls Swap in/out

49.RIM – Resource Initialization Modules

50.RRSF – RACF Resource Sharing Facility

51.RSU – Recommended Service Update

52.SAF – System Access Facility

53.SAP – Service Assist Processor — I/O Channel Channel Management, zIIPs, zAAPs, IFL's

54.SPE – Describes a New Function APAR

55.SPKA – Set Storage Protect Key from Address - A Privileged Instruction

56.SMP/E – System Modification Program/Extended

57.SQA – System Query Area - A storage area in main memory

58.SRB – Service Request Block - Supervisor State - SRB Routine, SRB Mode, Scheduling an SRB

59.SVC – Supervisor Call - Named System Modules - System Service Routines - IBM/USER

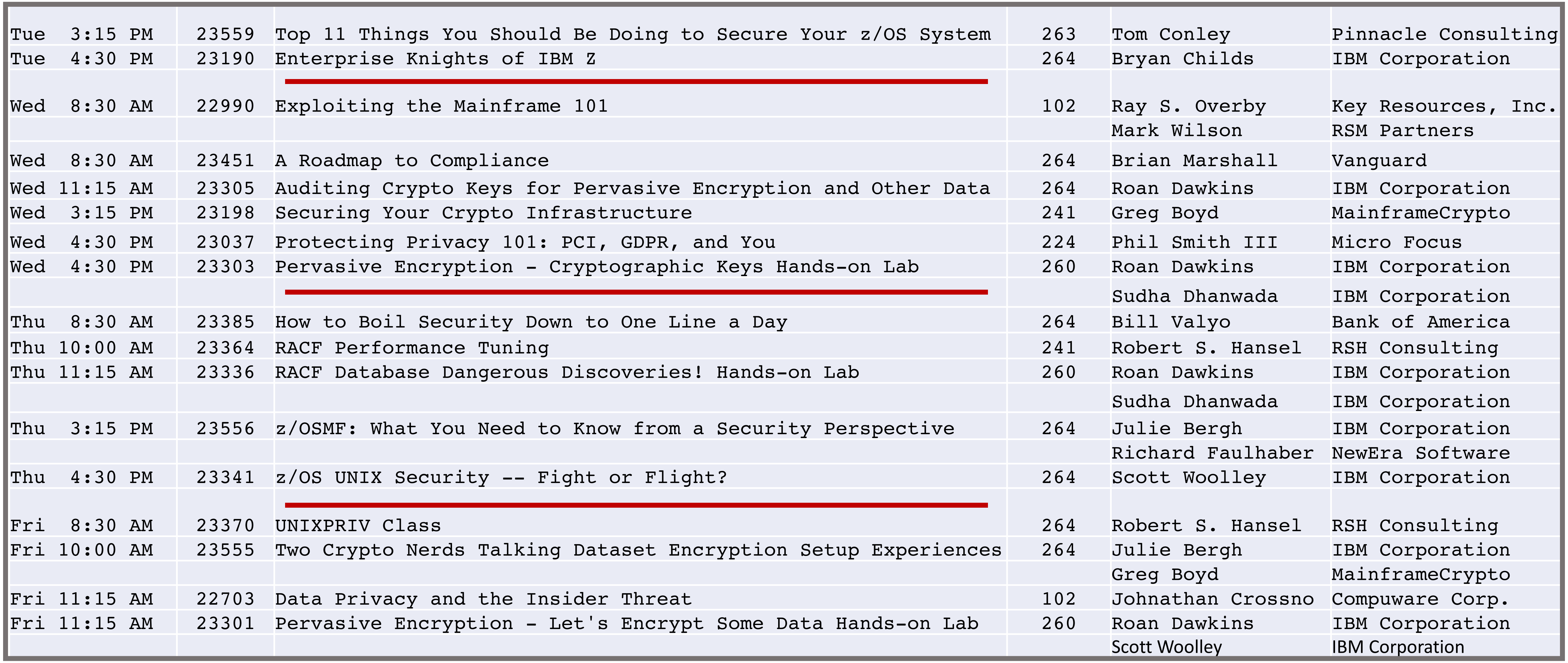
60.SWCP – Switch Configuration Program

9 - Language Index

Glossary of Terms:

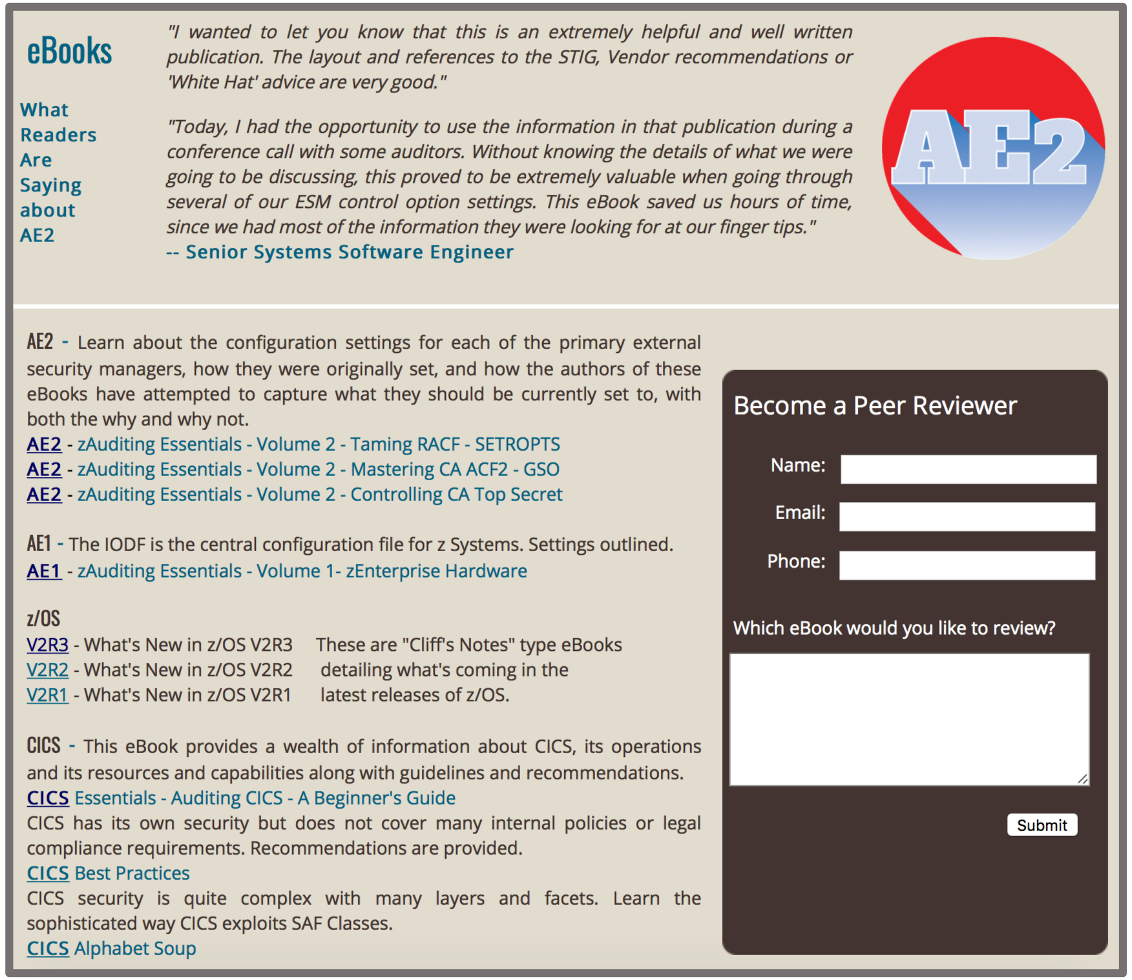
61. TCB - Task Control Block - Problem State - Application Programs
62. UCB - Unit Control Block – Software portion of the Device Chain
63. UCW - Unit Control Work – Hardware portion of the Device Chain
64. USS - Unix System Services
65. SE - System Element - 1 of 2 CPC specific Workstations
66. SECINT - System Security and Integrity APARs/PTFs
67. POR - Power on Reset – A base level initialization of hardware and possible IPL
68. PPT - Program Properties Table
69. PR/SM - Processor Resource/System Manager
70. PKM - Program Status Word MASK - Control PSW Key Changes
71. PSW - Program Status Word - 0/7 protected & 8/15 not protected
72. SMF - System Management Facility – used to control system event logging
73. SAN - Storage Area Network – Sometime SNIA
74. TKE - Trusted Key Entry Workstation
75. US-CERT – United States Computer Emergency Readiness Team
76. z/OS - A z Mainframe Operating System
77. z/OSMF - The z/OS System Management Facility – a web-based workstation interface

A - Recommended Reading/Viewing– Lesson 10



Tue	3:15 PM	23559	Top 11 Things You Should Be Doing to Secure Your z/OS System	263	Tom Conley	Pinnacle Consulting
Tue	4:30 PM	23190	Enterprise Knights of IBM Z	264	Bryan Childs	IBM Corporation
Wed	8:30 AM	22990	Exploiting the Mainframe 101	102	Ray S. Overby	Key Resources, Inc.
					Mark Wilson	RSM Partners
Wed	8:30 AM	23451	A Roadmap to Compliance	264	Brian Marshall	Vanguard
Wed	11:15 AM	23305	Auditing Crypto Keys for Pervasive Encryption and Other Data	264	Roan Dawkins	IBM Corporation
Wed	3:15 PM	23198	Securing Your Crypto Infrastructure	241	Greg Boyd	MainframeCrypto
Wed	4:30 PM	23037	Protecting Privacy 101: PCI, GDPR, and You	224	Phil Smith III	Micro Focus
Wed	4:30 PM	23303	Pervasive Encryption - Cryptographic Keys Hands-on Lab	260	Roan Dawkins	IBM Corporation
					Sudha Dhanwada	IBM Corporation
Thu	8:30 AM	23385	How to Boil Security Down to One Line a Day	264	Bill Valyo	Bank of America
Thu	10:00 AM	23364	RACF Performance Tuning	241	Robert S. Hansel	RSH Consulting
Thu	11:15 AM	23336	RACF Database Dangerous Discoveries! Hands-on Lab	260	Roan Dawkins	IBM Corporation
					Sudha Dhanwada	IBM Corporation
Thu	3:15 PM	23556	z/OSMF: What You Need to Know from a Security Perspective	264	Julie Bergh	IBM Corporation
					Richard Faulhaber	NewEra Software
Thu	4:30 PM	23341	z/OS UNIX Security -- Fight or Flight?	264	Scott Woolley	IBM Corporation
Fri	8:30 AM	23370	UNIXPRIV Class	264	Robert S. Hansel	RSH Consulting
Fri	10:00 AM	23555	Two Crypto Nerds Talking Dataset Encryption Setup Experiences	264	Julie Bergh	IBM Corporation
					Greg Boyd	MainframeCrypto
Fri	11:15 AM	22703	Data Privacy and the Insider Threat	102	Johnathan Crossno	Compuware Corp.
Fri	11:15 AM	23301	Pervasive Encryption - Let's Encrypt Some Data Hands-on Lab	260	Roan Dawkins	IBM Corporation
					Scott Woolley	IBM Corporation

A - Recommended Reading/Viewing– Lesson 10



eBooks

What Readers Are Saying about AE2

"I wanted to let you know that this is an extremely helpful and well written publication. The layout and references to the STIG, Vendor recommendations or 'White Hat' advice are very good."

"Today, I had the opportunity to use the information in that publication during a conference call with some auditors. Without knowing the details of what we were going to be discussing, this proved to be extremely valuable when going through several of our ESM control option settings. This eBook saved us hours of time, since we had most of the information they were looking for at our finger tips."

-- Senior Systems Software Engineer

AE2 - Learn about the configuration settings for each of the primary external security managers, how they were originally set, and how the authors of these eBooks have attempted to capture what they should be currently set to, with both the why and why not.

AE2 - zAuditing Essentials - Volume 2 - Taming RACF - SETROPTS
AE2 - zAuditing Essentials - Volume 2 - Mastering CA ACF2 - GSO
AE2 - zAuditing Essentials - Volume 2 - Controlling CA Top Secret

AE1 - The IODF is the central configuration file for z Systems. Settings outlined.
AE1 - zAuditing Essentials - Volume 1- zEnterprise Hardware

z/OS
V2R3 - What's New in z/OS V2R3
V2R2 - What's New in z/OS V2R2
V2R1 - What's New in z/OS V2R1

These are "Cliff's Notes" type eBooks detailing what's coming in the latest releases of z/OS.

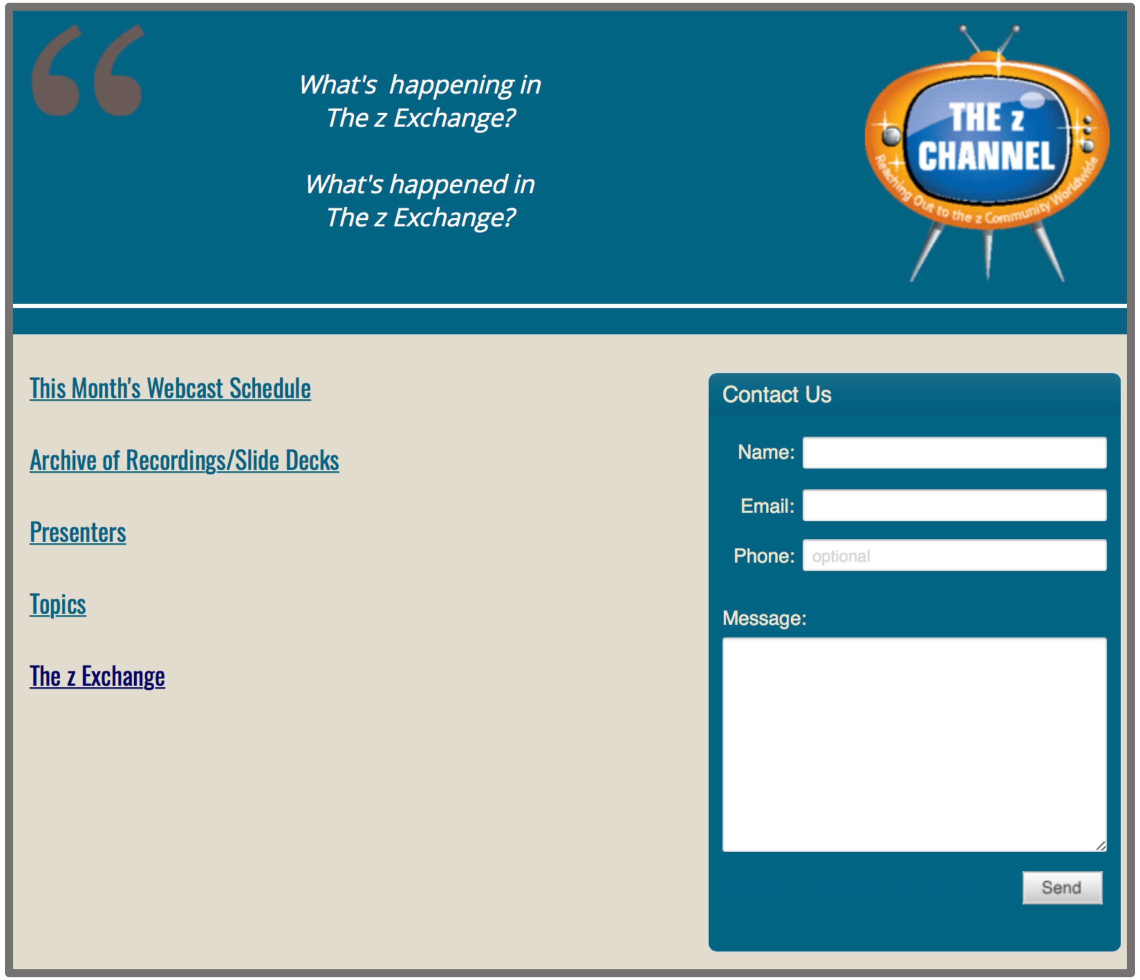
CICS - This eBook provides a wealth of information about CICS, its operations and its resources and capabilities along with guidelines and recommendations.
CICS Essentials - Auditing CICS - A Beginner's Guide
CICS has its own security but does not cover many internal policies or legal compliance requirements. Recommendations are provided.
CICS Best Practices
CICS security is quite complex with many layers and facets. Learn the sophisticated way CICS exploits SAF Classes.
CICS Alphabet Soup

Become a Peer Reviewer

Name:
Email:
Phone:

Which eBook would you like to review?

Submit



What's happening in The z Exchange?

What's happened in The z Exchange?

This Month's Webcast Schedule

Archive of Recordings/Slide Decks

Presenters

Topics

The z Exchange

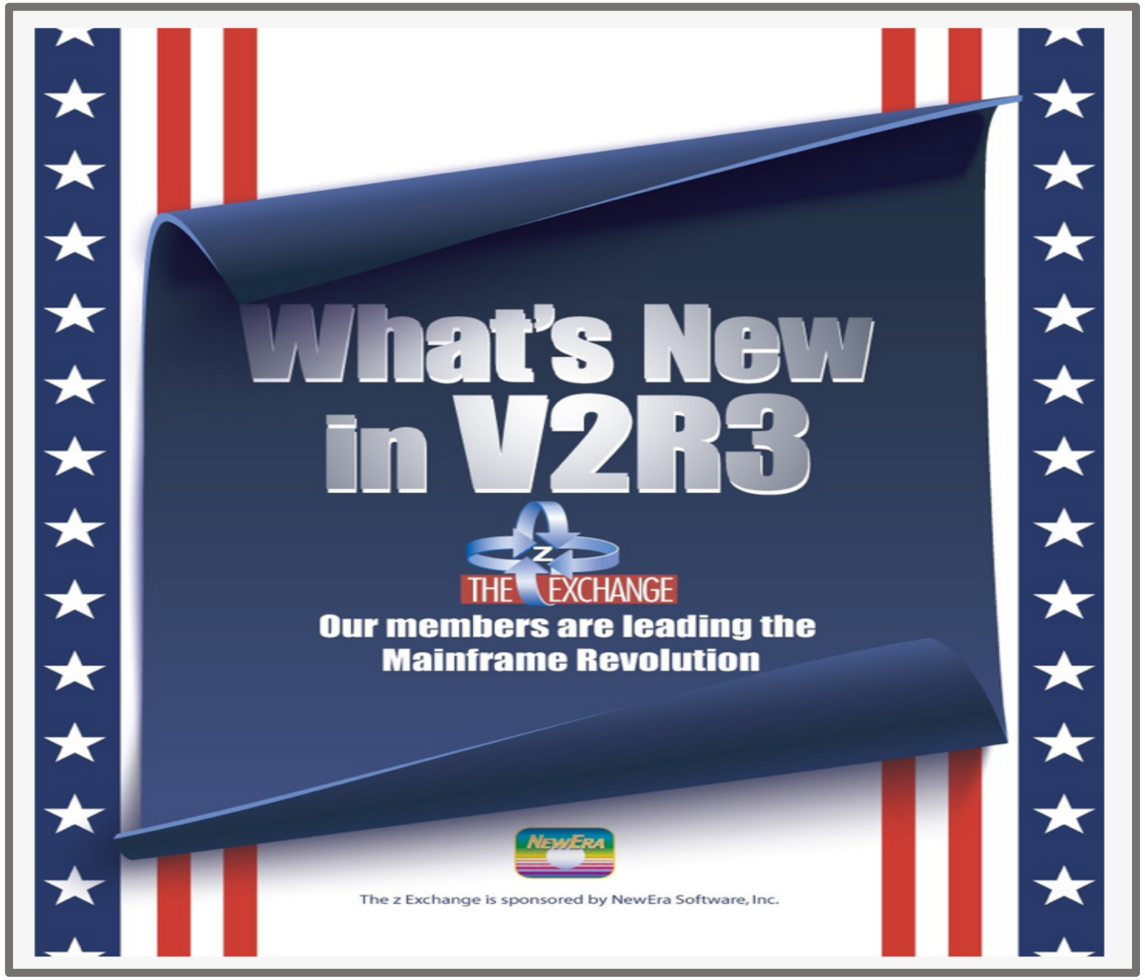
Contact Us

Name:
Email:
Phone: optional
Message:

Send

eBooks White Papers Subject Matter Experts Presentation Slide Decks

A - Recommended Reading/Viewing– Lesson 10


What's New
in V2R3
THE EXCHANGE
z
Our members are leading the
Mainframe Revolution
NewEra
The z Exchange is sponsored by NewEra Software, Inc.

The zExchange

A - Recommended Reading/Viewing– Lesson 10

z Systems customers should subscribe to the Systems Security Portal to receive information about security and system integrity APARs, their associated fixes, and critical IBM Systems security and integrity service updates.

IBM System z Security Portal FAQ

This document is intended to help customers better understand the System z Security and System Integrity process. It answers questions about the System z Security Portal so they can best integrate this critical security information into their individual security processes.

IBM z Systems Security Portal

Frequently Asked Questions

Worldwide

IBM System z Security Portal FAQ

THE LAST CHAPTER

- ✓ What we've been doing – How to Build a Trusted Computer Base, a base that provides both Operational Integrity and Data Security.
- ✓ What we know now is that the trust we seek is a process that will work most of the time. But, it's not an absolute or something we are able to measured.
- ✓ In order to understand how to build trust you need to study these materials and when you're done (it may take a while) be able to communicate your understanding clearly to others.
- ✓ To communicate it you need to explain how it works, why it matters to you and why others should care as well.
- ✓ To maximize the value of what you now know about z/OS as the platform for building a trust with users, business partners and your fellow employees you must be ready and able to SHARE (it).
- ✓ Finally, System Integrity and the Trusted Base will prove to be absolutely useless if not understood. From this point forward, it's up to you.

Thank You – Evaluations Please

Let's Build a z Environment - 102

Session 23331

Tuesday, August 14 at 11:15-12:15 AM

STL CC, Room 242

Presented by Paul R. Robichaux

NewEra Software, Inc.