#SHAREorg

SHARE
Technology · Connections · Results

Security - What's New in V2R1!

Paul R. Robichaux
NewEra Software, Inc.

Thursday, March13, 2014 - 8:00AM
Platinum Ballroom Salon 3
Anaheim Marriott Hotel

Session Number - 14798

SHARE in Anaheim

Abstract and Speaker

• Upgrading to the latest release of an Operating System is the single most important action that can be taken to assure the integrity of related information systems; their applications and data. In September, 2013 IBM made Version 2 Release 1 of the z/OS Operating System generally available.

• In the presentation the focus will be on certain (not all) changes and enhancements to System z Security and the Security of z/OS its Subsystem and System Management Tools. Including:

- System z Security Portal
- Operator Commands
- RACF
- Communication Server
- CICS
- HCD/HCM
- HMC
- TCP/IP
- ParmLib
- z/OSMF
- z/AWARE

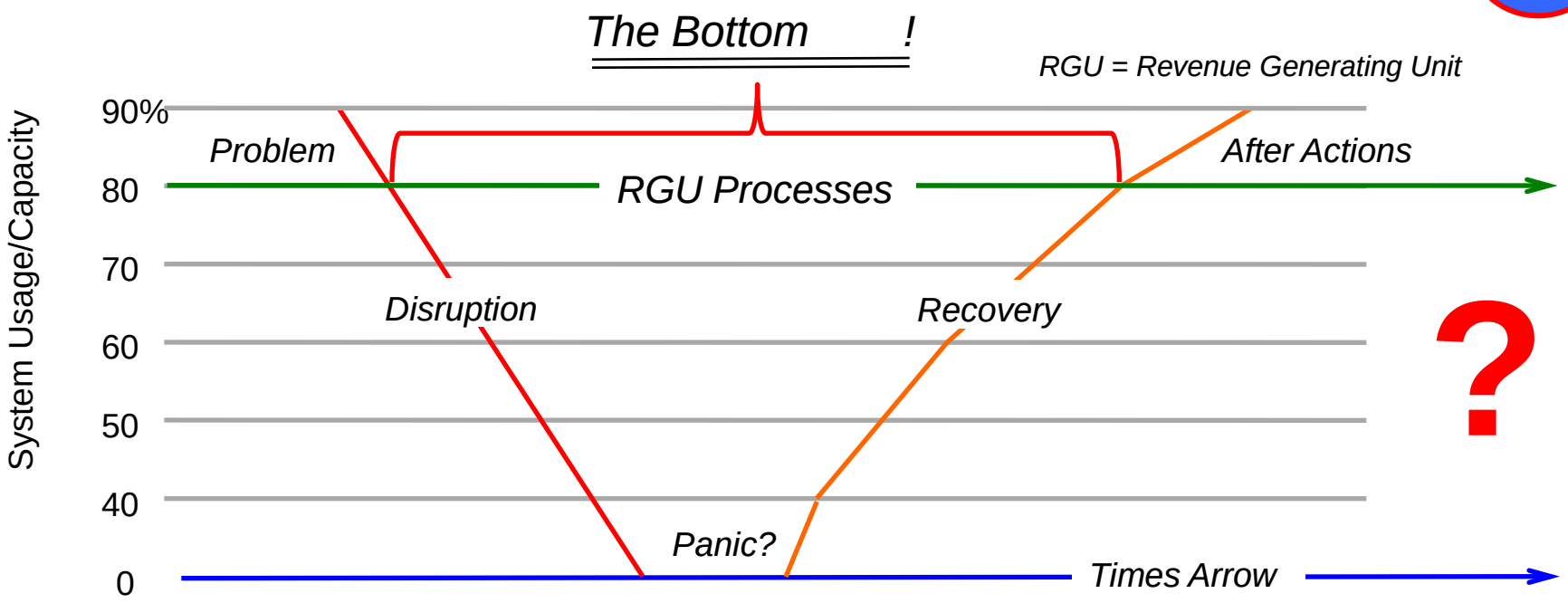
• Paul R. Robichaux is CEO of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a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

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

Security - What's New in V2R1!

This is all about RAS - Reliability, Availability and Securability

RAS

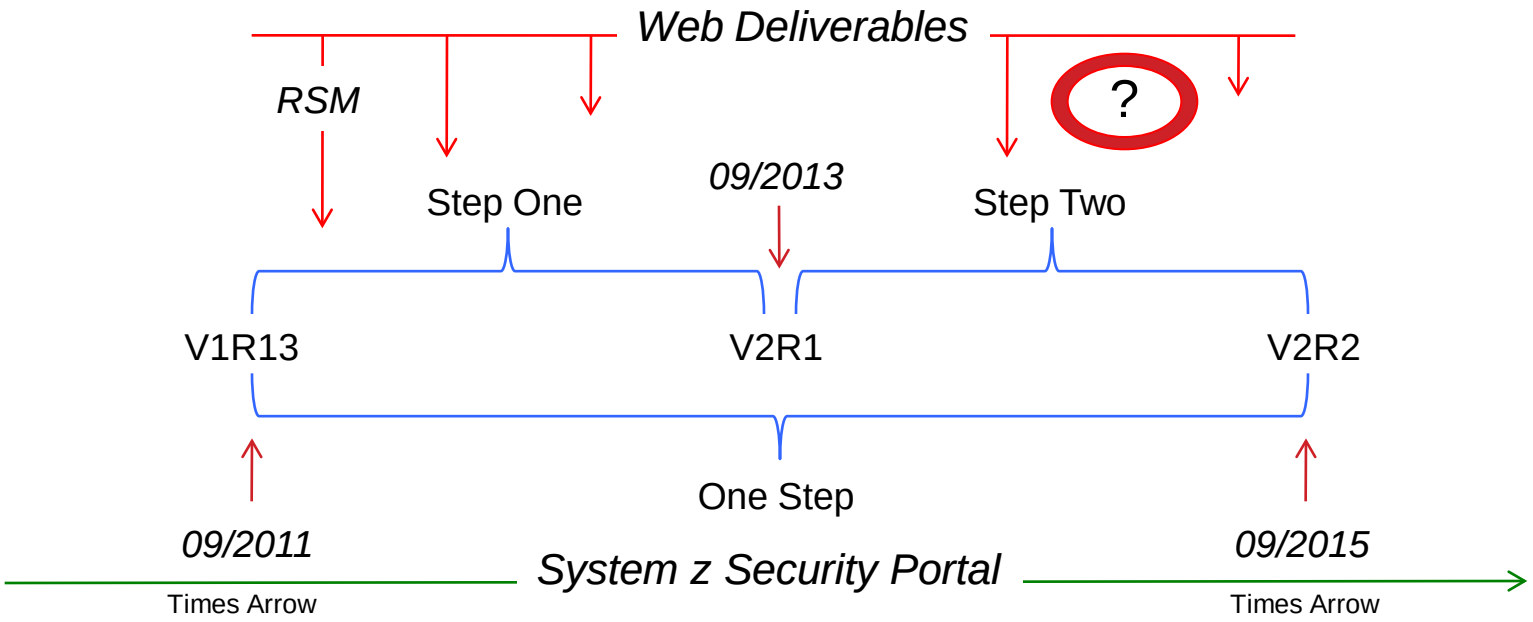


"…tracking and installing security and system integrity fixes will help to mitigate risk in the System z Environment. Recommended Service Upgrades (RSUs) help to minimize your exposure to security threats and system integrity issues." What level are you at?

Security - What's New in V2R1!

z/OS MVS Initialization and Tuning Reference, SA22-7592-25

Get to V2R1 ASAP, and Stay Up-to-date, Please!



The System z Security Portal is intended to help you stay current with security and system integrity fixes by providing current SMP/E HOLDDATA you can use to identify security and system integrity fixes that you might not have installed on your z/OS systems before they are marked RSU. The System z Security Portal now also provides Associated Common Vulnerability Scoring System (CVSS) V2 ratings.[1]

[1] *Source: IBM United States Software Announcement 213-292 - (V2R1 Announcement)*

Security - What's New in V2R1!

z/OS MVS Initialization and Tuning Reference, SA22-7592-25
Originally Documented as: z/OS V1R13 RSM Enablement Offering - December, 2012

Web Delivery:

☑ Why?

- *"Stated simply, because we want you to be able to select new non-priced functions for your z/OS or OS/390 releases (releases for which Web deliverables are offered may or may not be currently orderable). Since we can't offer new features to products that aren't currently marketed, we're using the Internet to provide you with these functions."*

☑ What was it?

- *"The RSM Enablement Offering web deliverable is designed to help improve system availability and responsiveness by using Flash Express across transitional workload events such as market openings and diagnostic data collection."*

RSM = Real Storage Manager, a component of z/OS
ICSF - Delivers its updates this way - expect at least two per z/OS Release Cycle.

Security - What's New in V2R1!

z/OS MVS Initialization and Tuning Reference, SA22-7592-25

Web Delivery:

- ☑ What did it turn out to be?
  - *Parmlib Members:*

    COUPLExx, DIAGxx, IEASYSxx, IECIOxx,
    IGGCATxx, IXGCNFxx,NPFLSTxx
  - *Parmlib Comments:*

    COMMNDxx, GTFPARM, IEAABD00, IEACMD00, IEADMP00
    IEADMR00, IEAPAKxx, IEA SYSxx, LPALSTxx, VATLSTxx
  - *Corrections to Init and Tuning:*

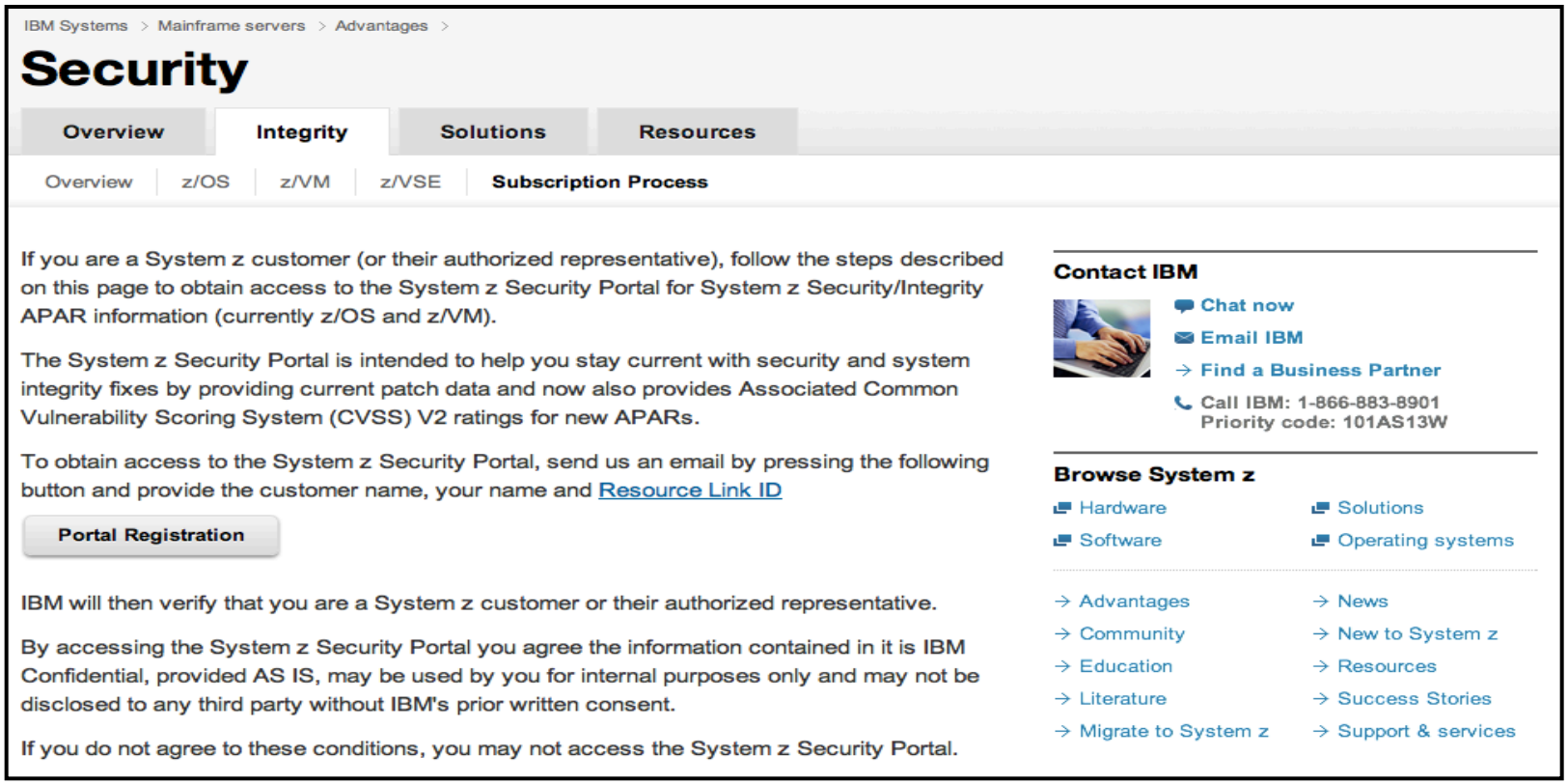
    IEAFIXxx VOLUME PARM NOT DOCUMENTED SHOULD BE SAME AS
    IEALPAxx MASTER CATALOGING NOT REQUIRED WHEN USED.
  - *Operator Command Updates:*

    MODIFY, SETLOGR, SETXCF

Security - What's New in V2R1!

http://www-03.ibm.com/systems/z/advantages/security/integrity_sub.html
http://www.vm.ibm.com/devpages../SPERA/aparint.html

System z Security Portal:



Security - What's New in V2R1!

http://www.first.org/cvss *and* http://en.wikipedia.org/wiki/CVSS

System z Security Portal:

A Common, Standardized, Free Vulnerability Scoring System (CVSS)

☑ Provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of 3 groups:

- *The Base group represents the intrinsic qualities of a vulnerability.*
- *The Temporal group reflects the characteristics of a vulnerability that change over time.*
- *The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment.*

☑ From each Group the following is produced:

- *A numeric score ranging from 0 to 10, and*
- *A Vector, a compressed textual representation that reflects the values used to derive the score.*

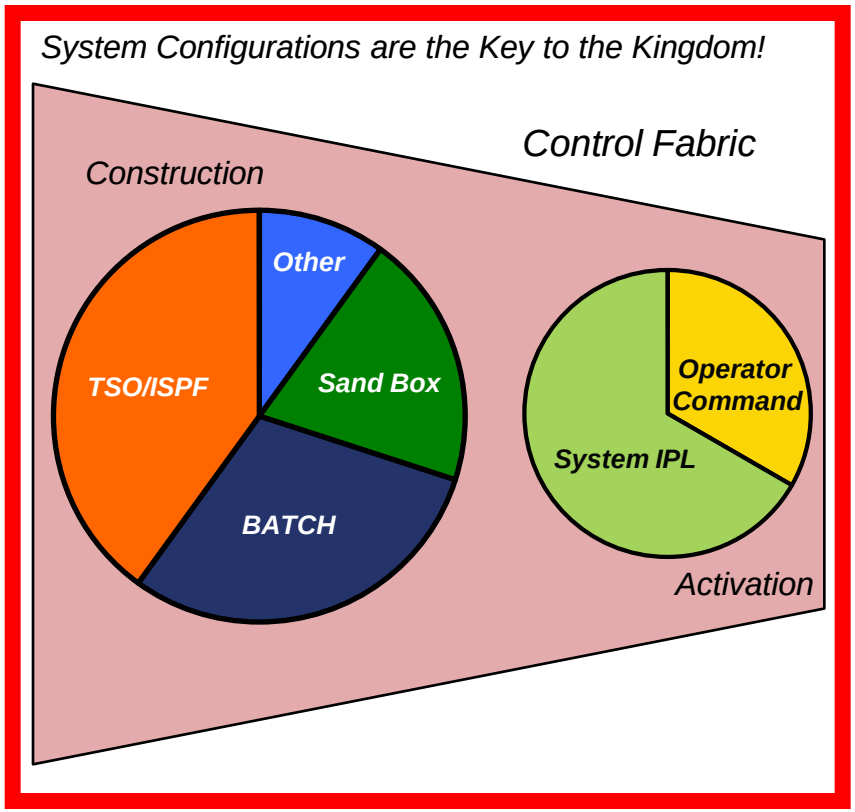
☑ This scoring process enables IT managers to more productively evaluate, recognize, prioritize and resolve System Threats across the entire organization.

FIRST = Forum of Incident Response and Security Teams

Security - What's New in V2R1!

Dynamic Updates - Make us More Agile but Compliance Difficult!

- *A Control and Productivity gap exists between conventional Change Management Systems and your External Security Manager (IBM-RACF, CA-ACF2, CA-Top Secret), making it difficult to comply with System Programming and System Security best practices.*
- *These practices, are intended to shield the z/OS System Configuration from unauthorized and/or undocumented changes but more often than not result in findings of non-compliance with industry and regulatory requirements.*
- *Without Adequate Operating System Controls all Other System z Controls become Questionable!*



Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Operator SET Commands:

Command	Authority	Resource-Name
SET CON	UPDATE	MVS.SET.CON
SET GTZ	UPDATE	MVS.SETGTZ.GTZ
SETALLOC	UPDATE	MVS.SETALLOC.ALLOC
SETIOS	UPDATE	MVS.SETIOS.IOS
SETHS	UPDATE	MVS.SETHS
SETLOAD	UPDATE	MVS.SETLOAD.IEASYM/LOAD
SETLOGR	UPDATE	MVS.SETLOGR.LOGR
SETOMVS	UPDATE	MVS.SETOMVS.OMVS
SETPROG	UPDATE	MVS.SETPROG
SETSMS	UPDATE	MVS.SETSMS.SMS
SETUNI	UPDATE	MVS.SETUNI.UNI

*Class M1 and M2 commands attach and run in the *MASTER* address space.*

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Operator SET Commands - Dynamics and Agility in Operations

☑ SET CON - *enables you to add MCS consoles dynamically when they are being used in distributed mode. It processes a CONSOLxx parmlib member and adds new consoles, up to the system and sysplex limits for the maximum number of consoles.*

SET [CON={(xx,[xx]...)}]

Where xx if the suffix of the target CONSOLxx parmlib member.

☑ SETCON - *enables you to specify a console to be removed from the sysplex and/or system. All resources associated with the named console will be freed and/or removed.*

SETCON {DELETE,CN=nnnnnnnn}

Were nnnnnnnn is the Console Name.

Note: The system pins UCBs for console devices defined in CONSOLxx at IPL time. Deleting a console device using HCD requires an IPL unless IEARELCN was used; a version of this program is found in SYS1.SAMPLIB.

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Operator SET Commands - Dynamics and Agility in Operations

☑ SETLOAD - *supports updating the values of system symbols dynamically. A new Keyword enables you to specify that the values of local static system symbols be updated using the values from an IEASYMxx member of parmlib.*

SETLOAD xx,{PARMLIB|IEASYM

Where xx suffix of the target LOADxx iplparm member.

☑ SETPROG - *Hardware Instrumentation Services (HIS), collects hardware event data in SMF records type 113, subtypes 1 and 2, and/or some z/OS UNIX files. Use the sub-command TRACKDIRLOAD to enable system-wide tracking of directed load modules.*

SETPROG TRACKDIRLOAD|NOTRACKDIRLOAD

Note: A directed load module is one loaded to a specified storage address. When enabled, mapping information about directed load modules is included in the maps produced by HIS. Tracking ENABLED by default.

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Other Operator Commands:

Command	Authority	Resource-Name
MODIFY	UPDATE	MVS.MODIFY.JOB/STC
SLIP	UPDATE	MVS.SLIP
START	UPDATE	MVS.START.STC.xxxxxxxx
VARY CN	UPDATE	MVS.VARY.CN
CONTROL V	READ [1]	MVS.CONTROL

[1] *The access authority for all CONTROL commands is normally READ, but the L=name (console name) operand can change the access level. When L=name specifies a console that is not full-capability and is not the issuing console, the access authority is UPDATE. When L=name specifies a console that is full-capability and is not the issuing console, the access authority is CONTROL.*

CONTROL V has sysplex scope only when *L=console_name* is specified.

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00
z/OS V2R1.0 MVS Initialization and Tuning Reference

Control Commands - Dynamics and Agility in Operations

☑ CONTROL V,LOGON|LOGOFF - *supports updating of system control functions that require an System Operator to log on and/or log off of MCS, SMCS, and HMCS Consoles, overriding settings defined in the CONSOLxx member of parmlib.*

☑ The CONSOLE statement in the CONSOLxx parmlib member establishes a device as an MCS, HMCS or SMCS console and defines its attributes.

CONSOLE LOGON {(REQUIRED)} Logon before issuing commands
{(OPTIONAL)} Always optional for the System Console
{(AUTO) } Logged on using Console Name as UserId

DEFAULT LOGON {(REQUIRED)} These are System-Wide Defaults that
{(OPTIONAL)} apply to all Consoles without specific
{(AUTO) } Log on/Log off specifications.

☑ Best Practice - Configure such that SMCS consoles are LOGON(REQUIRED), either by the system-wide DEFAULT or by the individual CONSOLE statement.

The system console is always treated as LOGON(OPTIONAL).

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Operator Display Commands:

Command	Authority	Command Description
D CONSOLE	READ	Console status information
D GRS	READ	Global resource serialization information
D GTZ	READ	Generic Tracker Information
D HIS	READ	Hardware event data collection status
D HS	READ	Basic HyperSwap Information
D LIST|ALL	READ	System activity
D OMVS	READ	z/OS UNIX System Services Status
D PCIE	READ	PCIe information
D PPT	READ	PPT information
D PROG	READ	Status of PROG, TRACKDIRLOAD option
D SLIP	READ	SLIP Trap information
D VIRTSTOR	xxxx	Virtual Storage Information
D XCF	READ	XCF information

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Display PPT - The IBM Program Properties Table:

```
PgmName  NC NS PR ST ND BP Key 2P 1P NP NH CP
AHLGTF    Y  Y  .  Y  .  .  0  .  .  Y  .  .
AKPCSIEP  .  Y  .  Y  Y  .  1  .  .  Y  .  .
ANFFIEP   .  Y  .  Y  Y  .  1  .  .  .  .  .
APSHPOSE  .  Y  .  Y  Y  .  1  .  .  Y  .  .
APSKAFPD  .  Y  .  Y  Y  .  1  .  .  Y  .  .
```

Synonym	Meaning	SCHEDxx keyword
NC	Non-cancelable	NOCANCEL
NS	Non-swappable	NOSWAP
PR	Privileged	PRIV
ST	System task	SYST
ND	No dataset integrity	NODSI
BP	Bypass password protection	NOPASS
Key	PSW key for this program	KEY(x)
2P	Second level preferred storage	SPREF
1P	First level preferred storage	LPREF
NP	No preferred storage	NOPREF
NH	No honor IEFUSI region settings	NOHONORIEFUSIREGION
CP	Critical paging	CRITICALPAGING

Security - What's New in V2R1!

z/OS V2R1.0 MVS Initialization and Tuning Reference, Page 728 - 732

The IBM Program Properties Table - SYS1.LINKLIB(IEFSDPPT)

Table 34. IBM-supplied Program Properties Table (PPT) Values

Program Name	Program Description	NC	NS	PR	ST	ND	BP	Key	2P	1P	NP	NH	CP
AHLGTF	GTF	x	x		x			0			x		
AKPCSIEP	ISP		x		x	x		1			x		
ANFFIEP	IP Printway		x		x	x		1					
APSHPOSE	PSF AFP Download Plus		x		x	x		1			x		
APSKAFPD	PSF Download		x		x	x		1			x		
APSPPIEP	PSF		x		x	x		1			x		
ASBSCHIN	APPC/MVS Scheduler Address Space (ASCH)		x		x			1	x	x			
ASBSCHWL	APPC/MVS Message Log Writer			x				1					
ATBINITM	APPC/MVS Address Space		x		x			1	x	x			
ATBSDFMU	APPC/MVS SDFM Utility			x				1					
AVFMNBLD	AVM	x	x		x			3			x		

Security - What's New in V2R1!

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Display PROG TRACKDIRLOAD - Better SMF Records:

☑ DISPLAY PROG,TRACKDIRLOAD displays the status of the TRACKDIRLOAD option: {IN EFFECT | NOT IN EFFECT

- Syntax is:

  D PROG,TRACKDIRLOAD [,L={a|name|name-a}]
  Where L=*a, name, or name-a* Specifies the display area (*a), console name (name), or both (name-a) where the* display is to appear.

- Example:

  CSV567I TRACKDIRLOAD IS {IN EFFECT | NOT IN EFFECT}

Note: When TRACKDIRLOAD is in EFFECT Hardware Instrumentation Services (HIS), collects hardware event data in SMF records type 113, subtypes 1 and 2, and/or some z/OS UNIX files. Use the sub-command TRACKDIRLOAD to enable system-wide tracking of directed load modules.

Security - What's New in V2R1!

The External Security Manager (ESM)

- *What's New in CA-ACF2*
- *What's New in CA-Top Secret*
- *What's New in IBM-RACF*

Security - What's New in V2R1!

z/OS V2.1 RACF - Mark Nelson - IBM

RACF

- *RRSF (RACF Remote Sharing Facility - now using TCP/IP instead of APPC)*
  - *Support for TCP/IP V6 (extending the existing IPV4 Support)*
  - *Comments in the RACF parameter library*
  - *TLS 1.2 cipher suite support*
- *New and improved RACF Health Checks*
  - *RACF_AIM_STAGE*
  - *RACF_UNIX_ID*
  - *RACF_CERTIFICATE_EXPIRATION*
  - *RACF_SENSITIVE_RESOURCES*
- *In IRRDBU00 output*
  - *Certificate issuer distinguished name*
  - *Subject distinguished names*
  - *Signature algorithms*
- *&RACUID in home directory path name*
- *Access controls for JES2/JES3 job classes*

Security - What's New in V2R1!

IBM Health Checker for z/OS: User's GuideSC23-6843-00

Selected RACF Health Checks

☑ RACF_CERTIFICATE_EXPIRATION - *allows RACF to identify all certificates which have expired, identify all certificates which are going to expire within the next few days, and ensures that the user has defined a proper baseline set of protections within the z/OS environment.*

- *Extracts each certificate from the RACF database.*
- *Examines the ending date, lists if the ending date is equal to or less than the warning date.*
- *If the certificate is TRUST or HIGHTRUST then the certificate is marked as an Exception.*

☑ RACF_UNIX_ID - *it is best practice to assign to each user and each group that needs access to z/OS UNIX functions and resources a unique identifier rather than shared identity.*

- Detects whether RACF is enabled to perform the automatic assignment of unique UNIX identities when users without OMVS segments access System UNIX Services.

Security - What's New in V2R1!

IBM Health Checker for z/OS: User's GuideSC23-6843-00

Selected RACF Health Checks

☑ RACF_AIM_STAGE - *AIM stage 3 allows RACF to handle authentication and authorization requests from z/OS® UNIX and is required to use some RACF functions. For example, when a large number of users without OMVS segments need access to z/OS UNIX services, such as FTP, but don't have UNIX identities. If the RACF database has been converted to AIM stage 3, it will enable RACF to automatically assign unique UNIX UIDs and GIDs as they are needed.*

- Examines the RACF database application identity mapping (AIM) to determine whether it is configured at the recommended AIM stage 3.

☑ RACF_SENSITIVE_RESOURCES - *examines the security characteristics of several system-critical data sets and general resources. The output of this check is a list of exceptions flagged.*

- *Updated to check additional/new "static" and "dynamic" resources names:*

Security - What's New in V2R1!

CICS V5R1

☑ *RACFSYNC - The system initialization table (SIT) parameter specifies whether CICS listens for type 71 Events.*

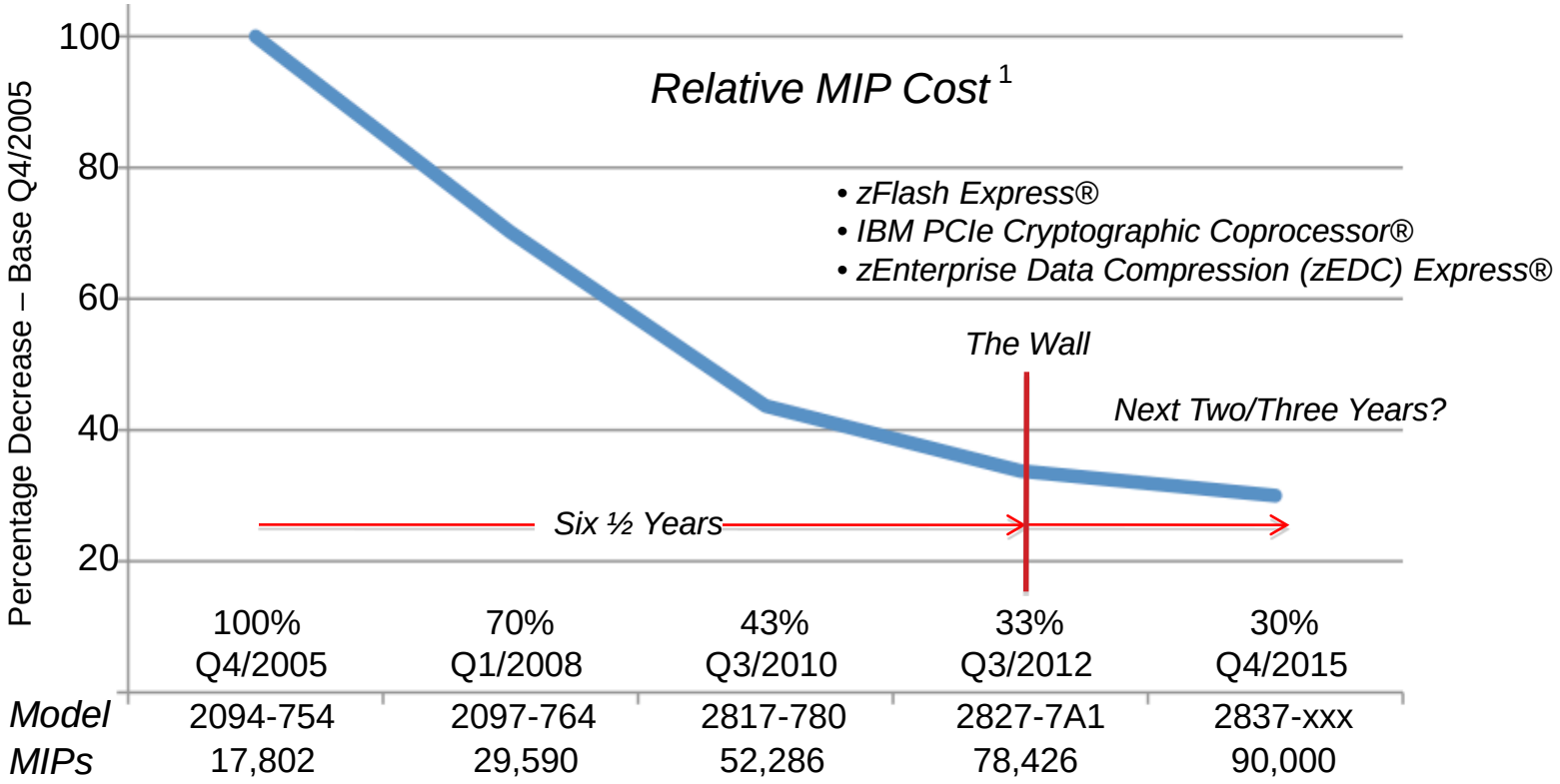
- When CICS receives a type 71 ENF event for a user ID, all cached user tokens for the user ID are invalidated, irrespective of the setting of the USRDELAY parameter. Subsequent requests from that user ID force a full RACF RACROUTE VERIFY request, which results in a refresh of the user's authorization level. User tokens for tasks that are currently running are not affected.

☑ *SECVFYFREQ* - {NEVER|USRDELAY} *The system initialization table (SIT) parameter specifies whether or not CICS makes a full verification request at least once a day for each user ID that is used to log on to the CICS region.*

- NEVER - When the login process uses password verification, CICS makes a full verification request only if an attempt at password verification fails.
- USRDELAY - CICS makes a full verification request at least once a day for each user ID that is used to log on to the CICS region.

Security - What's New in V2R1!

Hardware Updates!



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

Security - What's New in V2R1!

http://publibz.boulder.ibm.com/epubs/pdf/cbd2ug00.pdf

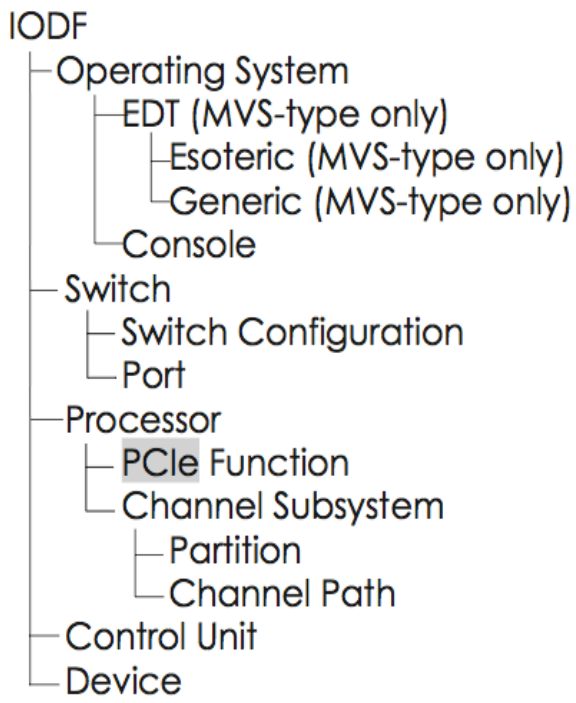
HCD/HCM

☑ PCIe - *Peripheral Component Interconnect Express adapters attached to a 2827 type system can provide the operating system with a variety of so-called PCIe functions to be exploited by entitled logical partitions (LPARs).*

☑ HCD - *allows you to define, change, delete, and view PCIe functions controlling which LPARs have access to their functions.*

- Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE). PCIe functions of type RoCE may be assigned to external physical networks by specifying corresponding PNET IDs.
- zEDC-Express. For PCIe functions of type zEDC-Express, a virtual function number between 1 and 15 must be specified.

Structure:



Security - What's New in V2R1!

http://publibz.boulder.ibm.com/epubs/pdf/cbd2ug00.pdf

HCD/HCM

- PCIe - *Specified on IODF FUNCTION Statement*:

```
FUNCTION FID=05A,UNIT=ROCE,PCHID=54A
         PNETID=(PNET01,PNET02,PNET03)
         PART=((LP01,(LP03,LPO8)
         DESC='zEDC Express one'
```

- PCIe - *Activity Report:*
  - Provides statistics and performance measurements on PCI Express based functions (PCIE functions) allocated by at least one z/OS address space for a period of time within the reporting interval.
  - SMF data required for this report is gathered by default. PCIE functions are captured by the report if hardware feature activities has been detected.

Syntax:

Partition	Name
	Number
	Usage
	Description
PCIe function	ID
	Unit
	PCHID
	Virtual function number
	Description
	PNET IDs
	Partition access list
	Partition candidate list

Security - What's New in V2R1!

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

DMA Attacks

☑ *A type of side channel attack where the corruption of basic OS security mechanisms or theft of cryptographic keys can be conducted by an attacker with direct access to the physical memory address space of the computer.*

- Systems are vulnerable to a DMA attack by an external device if they have port like PCI and PCI-Express that can be hooked up directly to a physical address space. Security concerns argue against the use of PCIe as a host-to-host interconnect. See Federal Information Processing Standards - FIPS 140-2 - Levels of Defenses.

☑ *IQPPRMxx*

- A z/OS parmlib member who's suffix is specified in IEASYSxx on the IQP Keyword is used to define parameters that manage applications that require the utilization of System z PCIe-related features, such as:

  - *zFlash Express®*
  - *IBM PCIe Cryptographic Coprocessor®*
  - *zEnterprise Data Compression (zEDC) Express®*

Security - What's New in V2R1!

z/OS V2R1.0 MVS Initialization and Tuning Reference, Page 591 - 592

IQPPRMxx

☑ ZEDC - *Use the ZEDC statement to specify parameters for managing application requests that use zEnterprise Data Compression (zEDC) features.*

- MAXSEGMENTS - A Keyword
  Specifies the maximum number of 16 MB storage areas (segments) to allow for problem state compression (deflation) and decompression (inflation) requests.
- DEFMINREQSIZE - A Keyword
  Specifies the minimum size in kilobytes of the data to be compressed in order for request to be eligible for zEDC compression.
- INFMINREQSIZE - A Keyword
  Specifies the minimum size in kilobytes of the data to be decompressed in order for the request to be eligible for zEDC decompression.
- SET IQP - An Operator Command
  Used to change the MAXSEGMENTS value to a lower value, the change is ignored and the original value remains in effect, because the maximum number of segments cannot be decreased dynamically. If a higher value is specified, the value is accepted.

Security - What's New in V2R1!

z/OS Communications Server: IP Configuration GuideSC27-3650-00

TCP/IP

- ☑ *What is Remote Direct Memory Access (RDMA)?*

  For security reasons, it is undesirable to allow transmitters to read or write arbitrary memory on the receiver. Any RDMA scheme must prevent any unauthorized memory accesses. Most RDMA schemes protect memory by allowing RDMA reads/writes only to buffers that the receiver has explicitly identified to the NIC as valid RDMA targets. The process of informing the NIC about a buffer is called "registration". The name of a registered buffer is its Region Identifier (RID) - a memory buffer region reserved and registered for use with RDMA requests, and its unique identifier.

- ☑ *PORT and/or PORTRANGE STATEMENT*

  Keyword - NOSMCR - Indicates that Shared Memory Communications via Remote Direct Memory Access (SMC-R) communications are not permitted for TCP connections by using a named port and/or any port in a specified range.

Security - What's New in V2R1!

z/OS Communications Server: IP Configuration GuideSC27-3650-00

TCP/IP

- ☑ *What is Remote Direct Memory Access (RDMA)?*

  For security reasons, it is undesirable to allow transmitters to read or write arbitrary memory on the receiver. Any RDMA scheme must prevent any unauthorized memory accesses. Most RDMA schemes protect memory by allowing RDMA reads/writes only to buffers that the receiver has explicitly identified to the NIC as valid RDMA targets. The process of informing the NIC about a buffer is called "registration". The name of a registered buffer is its Region Identifier (RID) - a memory buffer region reserved and registered for use with RDMA requests, and its unique identifier.

- ☑ *PORT and/or PORTRANGE STATEMENT*

  Keyword - NOSMCR - Indicates that Shared Memory Communications via Remote Direct Memory Access (SMC-R) communications are not permitted for TCP connections by using a named port and/or any port in a specified range.

Security - What's New in V2R1!

z/OS Communications Server: IP Configuration GuideSC27-3650-00

TCP/IP

☑ *SMFCONFIG STATEMENT*

- *SMCR* | *NOSMCRGROUPStatistics* - Requests, or not, that SMF type 119 records of subtype 41 containing statistics related to SMC-R link groups are created. These records are created periodically based on the SMF interval in effect. This operand is valid if the current record type setting is TYPE119. Default - No Record.

- *SMCR* | *NOSMCRLINKEvent* - Requests, or not, that SMF type 119 records of subtype 42 and 43 are created. The SMF records of subtype 42 are created when SMC-R links are started, and the SMF records of subtype 43 are created when SMC-R links are ended. Default - No Record.

☑ *New command to verify TCP profile syntax*

- V TCPIP,,SYNTaxcheck,dsname
- Can run on any system at the same level

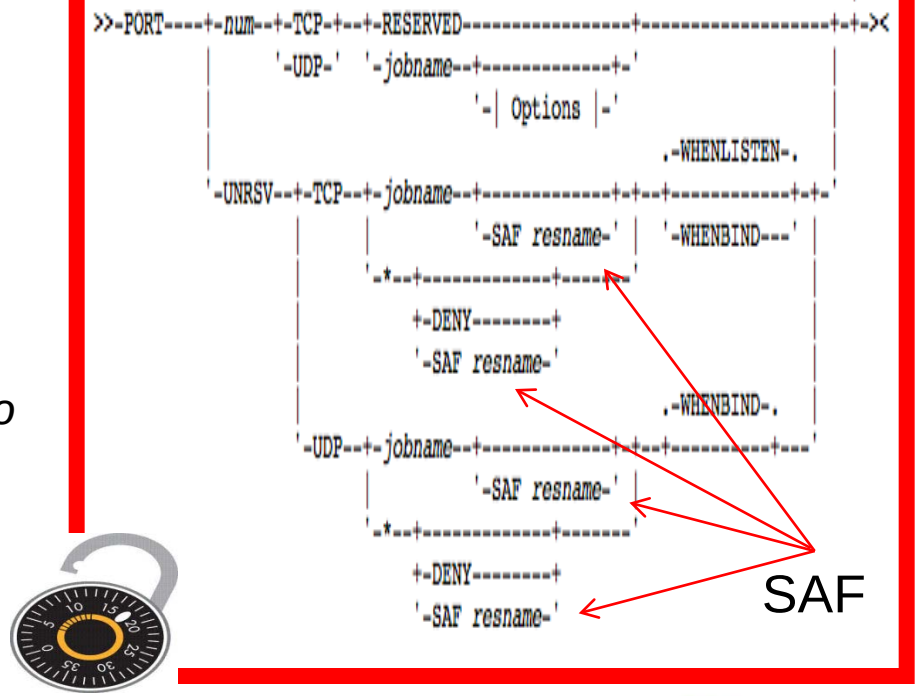
Security - What's New in V2R1!

z/OS Communications Server: IP Configuration GuideSC27-3650-00

TCP/IP - Profile Configuration

- *The PORT statement is used to reserve a port for one/more job names or to control application access to unreserved ports.*
- *For example, use the PORT statement to control the port that will be used by the SMTP server for receiving mail. If PORT is not coded, SMTP defaults to the value 25, the well known port for mail service.*
- *Note that port 25 is typically reserved in hlq.PROFILE.TCPIP for the SMTP server to accept incoming mail. If another port number is selected for the SMTP server, then update the hlq.PROFILE.TCPIP file accordingly.*

TCP/IP - Port Configuration Statement Syntax



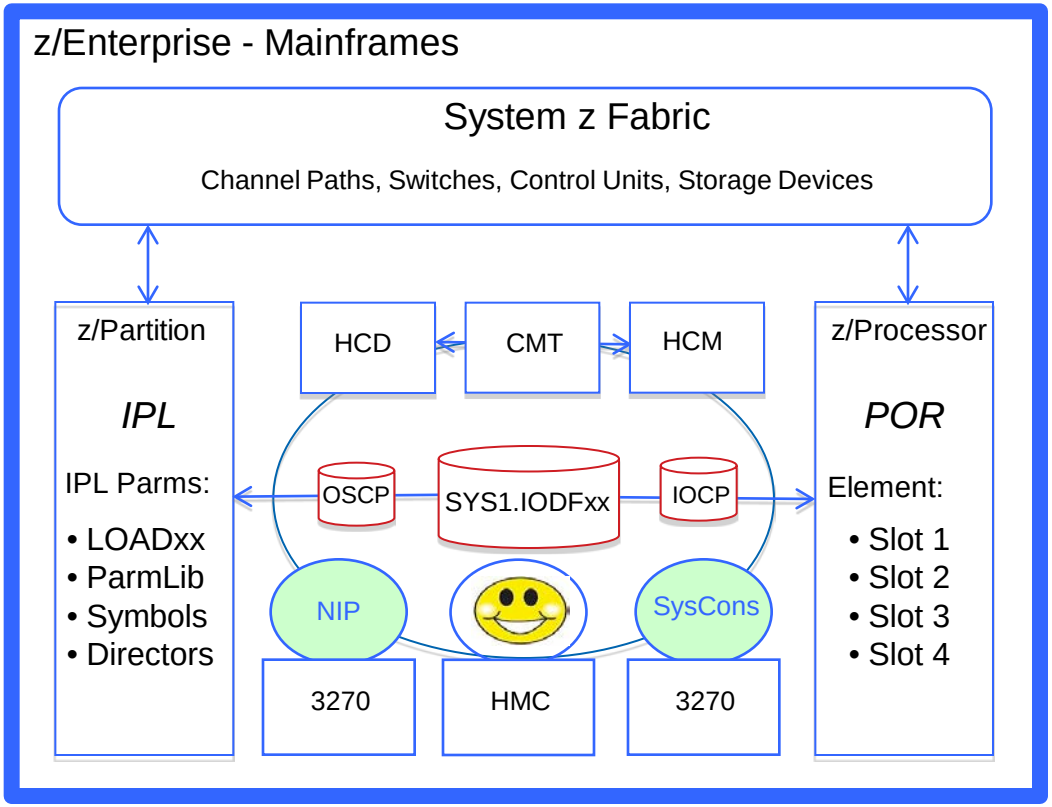
Source: IBM z/OS V2R1 CS TCP/IP Implementation
Note – TCP/IP Profile DECK, IPSECURITY Keyword on the IPCONFIG Statement

Security - What's New in V2R1!

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

HMC - Hardware Management Console

- *You can operate a z/OS system or an entire Sysplex using the Operating System OS Message Facility of the Hardware Management Console HMC. This can also be known as 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.*



Security - What's New in V2R1!

z/OS V2R1.0 MVS Initialization and Tuning Reference, Page 236 - 247

HMC - Hardware Management Console

- *The HMCS can be used as a NIP console if attached from the HMC to a z/OS LPAR, that is then IPLed. For "consistency" the HMCS NIPs interface is identical to that of NIP, MCS, SMCS consoles.*
- *If you want to use the HMCS consoles after NIP, you'll need to define it in the CONSOLxx member.*
- *To do this use the CONSOLxx Keyword "HMCS" to defines a new console type that bridges the gap between NIP and SMCS consoles allowing you to use the HMCS as a consoles during IPL, and before and after SMCS type consoles become availability.*
- *Likely in response to a SHARE Requirement to replace OSA-ICC style consoles previously needed in order to perform similar multi-role functions.*

Syntax:

```
CONSOLE DEVNUM {(devnum)}
        {(SUBSYSTEM)}
        {(SYSCONS)}
        {(SMCS)}
        {(HMCS)}
```

Attribution for Understanding: Thank you Marna Walle!

Security - What's New in V2R1!

HMC - Hardware Management Console

☑ *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 that system*.

- To use the SYSCONS console for command processing, first enter

  VARY CN(*),ACTIVATE

- This allows the HMC 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 HMC/SYSCONS remains active for the duration of the IPL, or until the command (to deactivate the system console) is entered.

  VARY CN(*),DEACT

Security - What's New in V2R1!

HMC - Hardware Management Console

☑ A particular user (an operator) is allowed access to a particular resource (command or console) via a security profile. The security administrator can define a security profile for:

- ✓ Each user of a console
- ✓ Each console that is to be automatically logged on
- ✓ Each MVS™ command issued from a console

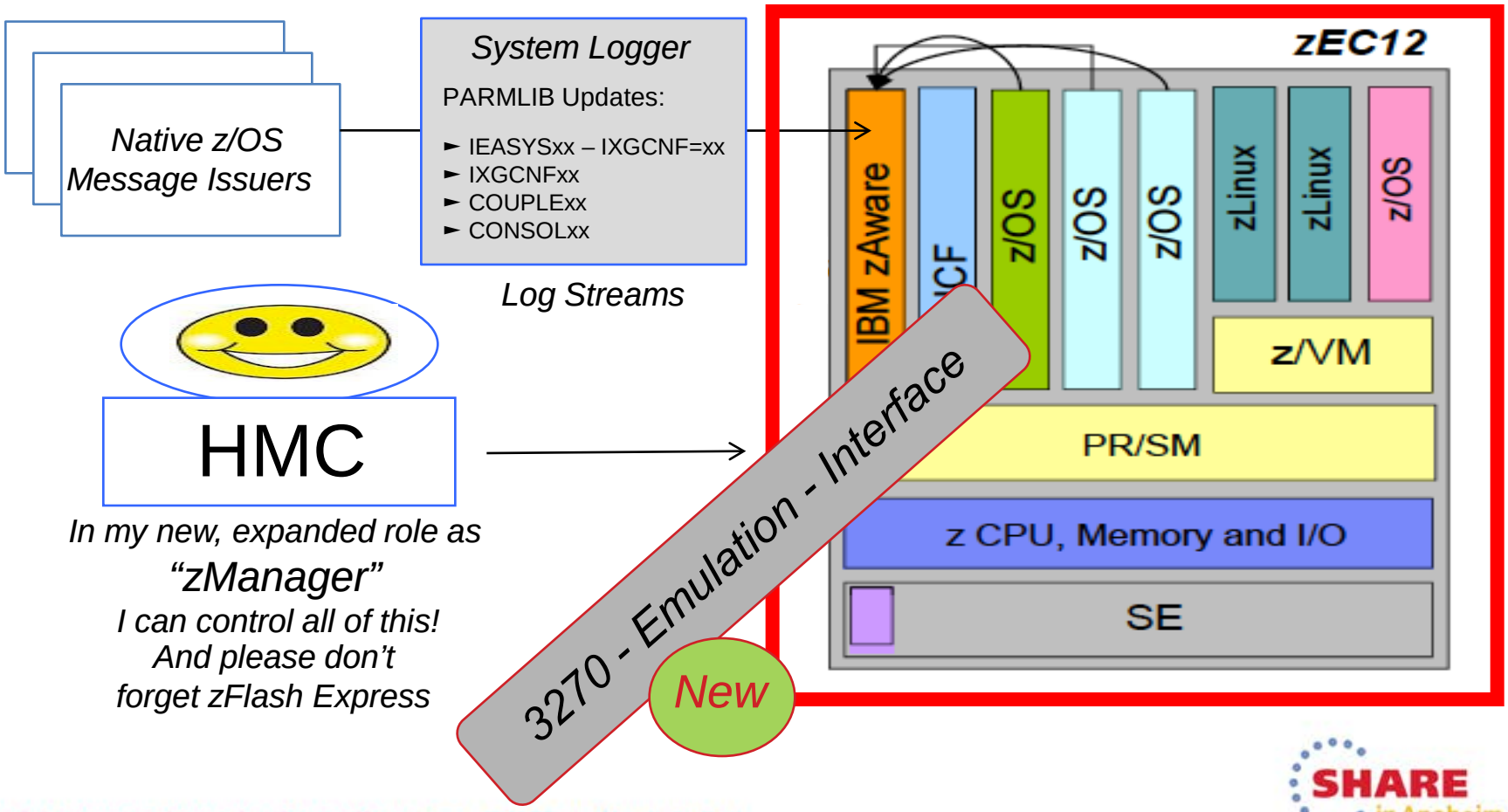
If security policy requires an audit of operator commands according to the identity of the user, then all operators must be defined by individual user profiles – who can issue what command or use a specific console or terminal - and the level of security auditing required by site best practices.

HCM events may not be sufficiently populated with user and/or terminal identity to satisfy these requirements.

Source: z/OS V1R11.0 MVS Planning Operations - SA22-7601-11

Security - What's New in V2R1!

HMC - Hardware Management Console - Now the "zManager"



Security - What's New in V2R1!

System Management Platforms are Converging!

TSO/ISPF
Classic Interface

z/Manager
Hardware Interface

EKFM Workstation
Enterprise Key Management

z/OSMF
Software Interface

zEC12

EKFM = Enterprise Key Foundation Workstation

Security - What's New in V2R1!

IBM z/OS Management Facility Configuration GuideSA38-0657-00

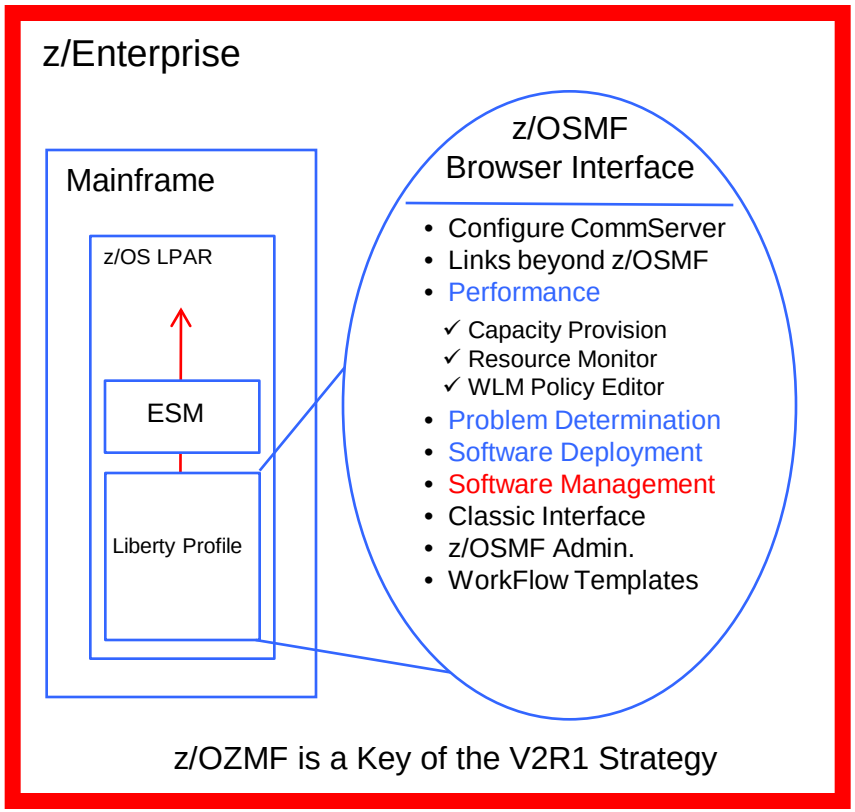
z/OSMF

☑ Supports for a modern, Web browser-based z/OS management console.

Helps system programmers to more easily manage a mainframe system by simplifying day to day operations and administration of a z/OS system.

Provides the intelligence needed to address the requirements of a diversified workforce, maximizing their productivity.

- ✓ Automation reduces the learning curve and improves productivity.
- ✓ Embedded assistance guides activities and simplifies operations.



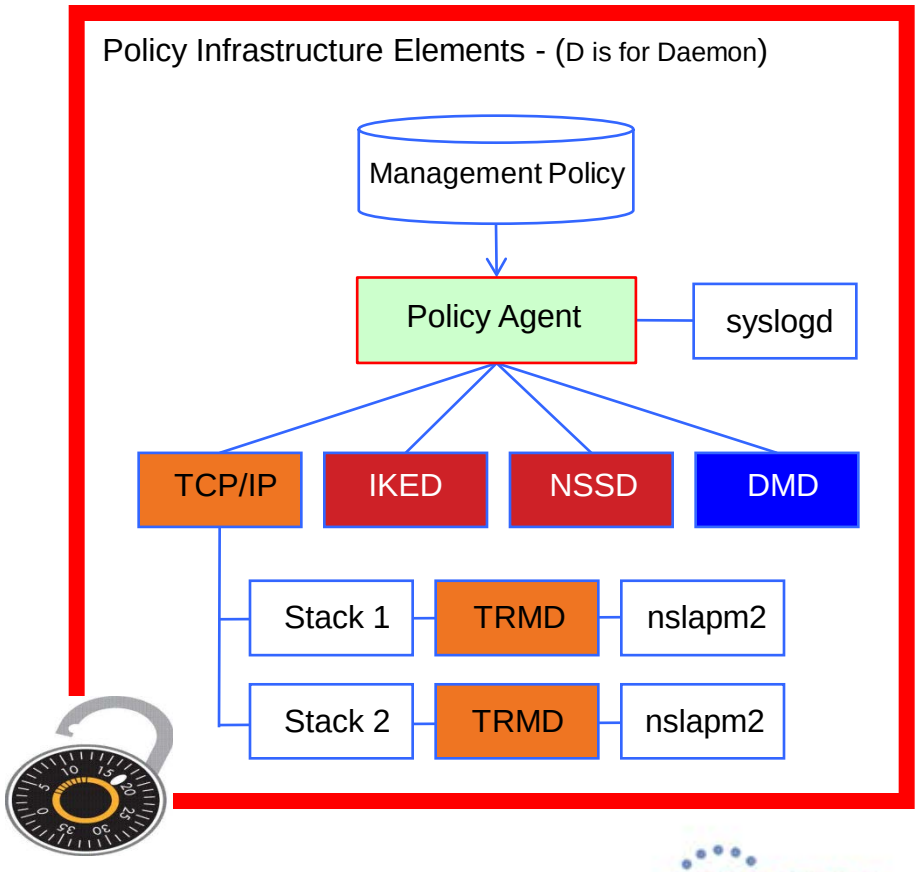
Source: zZS02 - What is z/OSMF - Why Would I Want It? - Greg Daynes, IBM Corporation

Security - What's New in V2R1!

z/OS V2R1.0 Communications Server Glossaryxxxx-xxxx-00

z/OS Communication Server

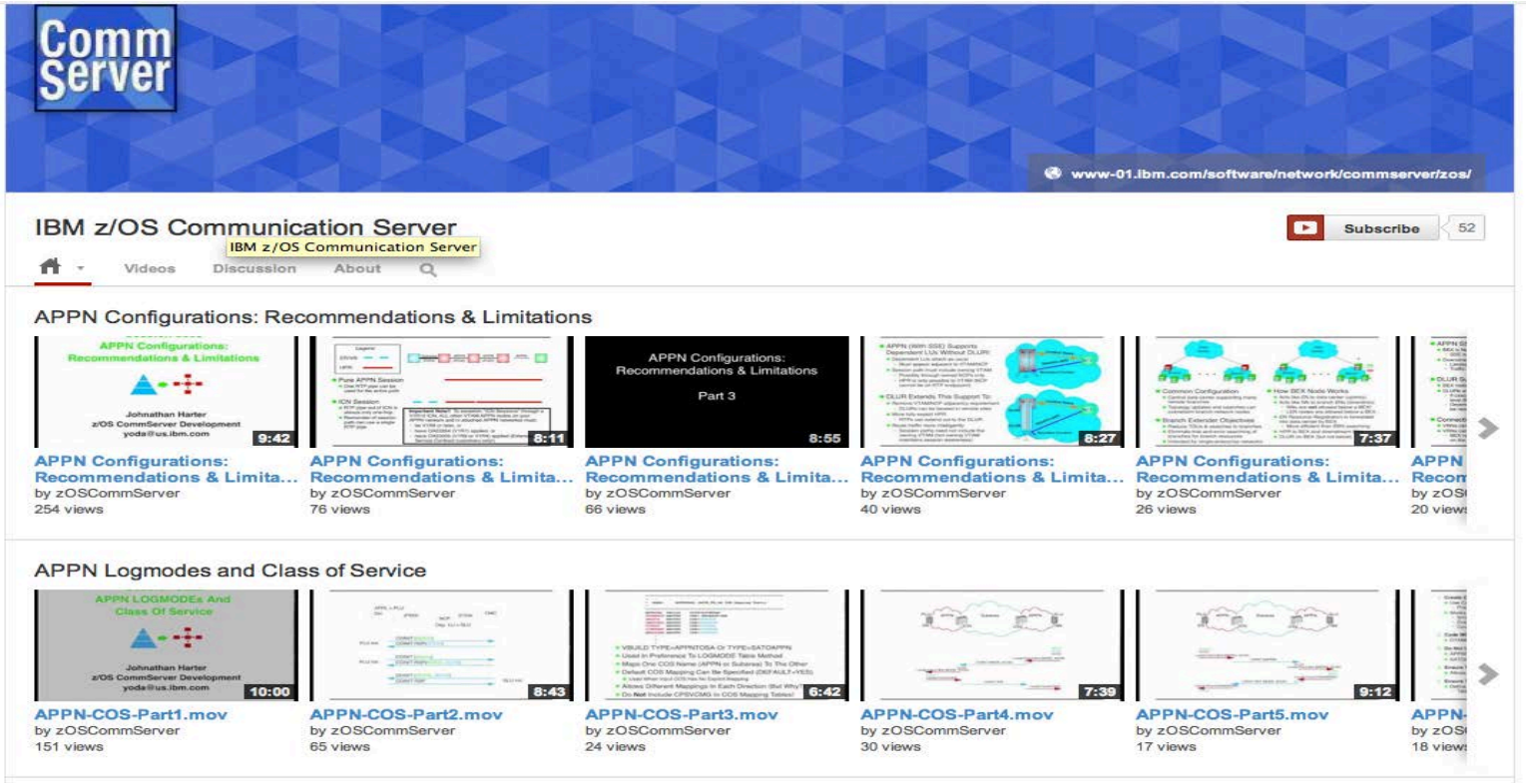
- Server Configuration:
  - *z/OSMF in, Windows Assistant is out*
- TCP/IP Profile:
  - *Syntax Checking*
  - *Not semantic (configuration) errors*
- PAGENT Defense Filtering (DMD):
  - *Resolves Flooding of syslogd*
  - *Event Logging Control Options*
- NetAccess Zone Control:
  - *Better Caching Controls*
  - *More IP Address Audit Detail*
- System SSL in FIPS-140 mode:
  - *IKED and NSSD Require ICSF*
  - *ICSF status during Initialization*



Security - What's New in V2R1!

www.youtube.com/user/zOSCommServer

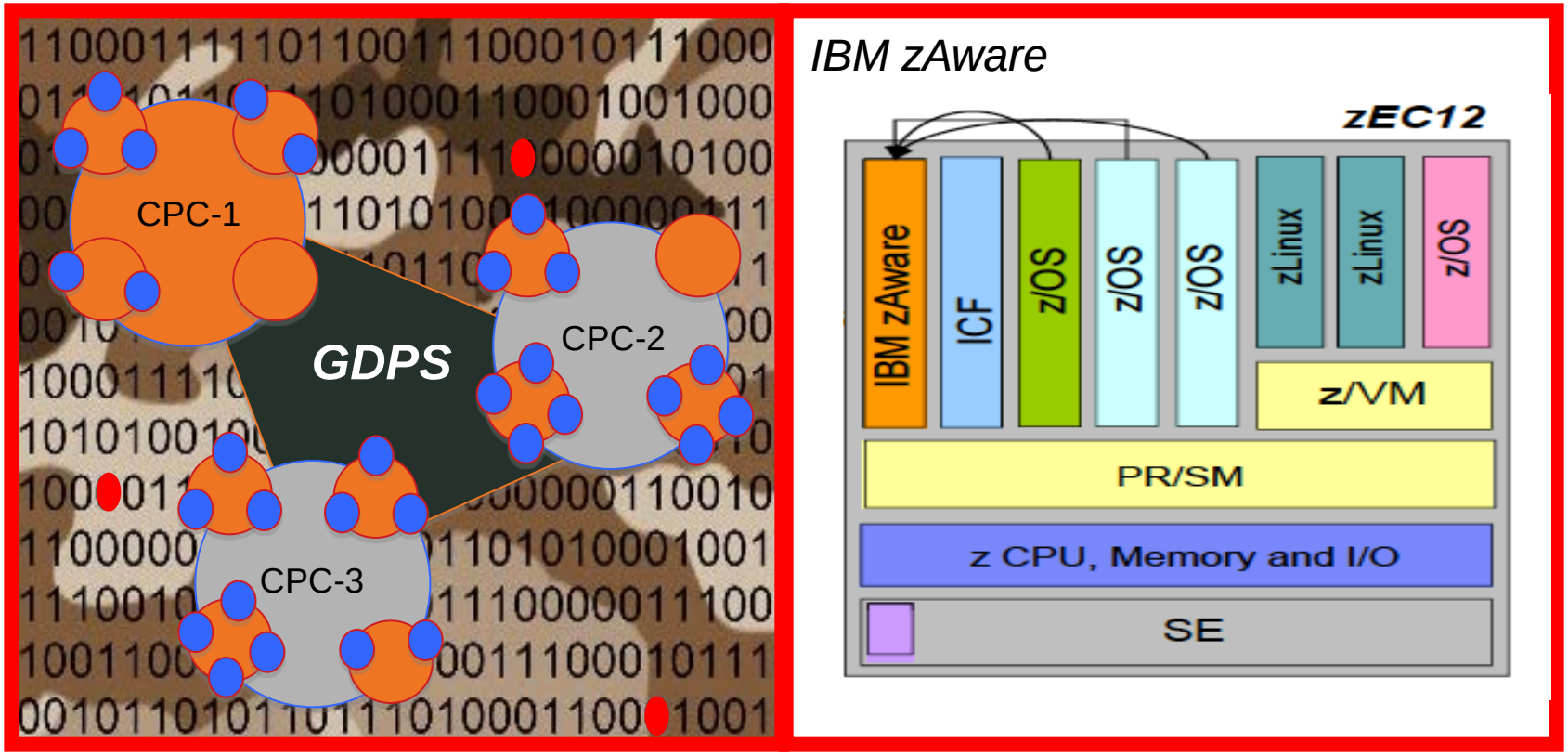
z/OS Communication Server



Security - What's New in V2R1!

The z/OS IBM System z Advanced Workload Analysis Reporter (IBM zAware)

The Future of Security > Self-Aware, Self-Healing, Automated!



Sources: The Father of IT Security, Founder of SHARE Security Project - Barry Schrager President, Xbridge

Security - What's New in V2R1!

Catch-All of Top 20 Changes!

- *Support for z9EC/BC and Z10EC/BC - None for z800 and z900*
- *Download FTP is now Secure, no more Unsecured Downloads - 10/2013*
- *Command Line Syntax Checker for TCP/IP Profile*
- *ESCON gone with zEC12 - Compatibility options available*
- *Generic Tracker - Track any z/OS thing - GTZ - Starts at IPL Disabled*
- *Global LPAR Activation - IOCP Sysplex Wide from HMC*
- *HCD/HCM - zDAC - Will include Switch Discovery*
- *TSO Logon Procedure - Cause of Failure Message available*
- *New Web Server for z/OSMF - Liberty Profile - Smaller*
- *Health Checker started Automatically with IPL*
- *SETLOADxx {PARMLIB|IEASYM} - Update Symbols*
- *z/OS V2R1 is Big! Fonts now included, almost doubles download*
- *Windows Base Configuration Managers are gone - z/OSMF*
- *In V2R2 Book Manager Build and "Look At" are gone - Read available*
- *Really Big Page Datasets - 1Gb to 2Gb*
- *New IEASYSxx Keywords: PAGECM,LFAREA,HZS,HZSPROC,GTZ*
- *IEFSSNxx - Start Subsystems in Parallel: JES,SMS,Etc. 1st then all others*
- *Lots of New and/or Enhanced Operator Commands: SET CON, SETCON, FORCE, PPT*
- *Health Checks to warn when Digital Certificate about to expire.*
- *GDG's the way you like them: Old to New and/or New to Old*

Security - What's New in V2R1!

http://www.newera-info.com/V2R1-Exchange.html

More about What's New - I suggest you Stay Tuned!

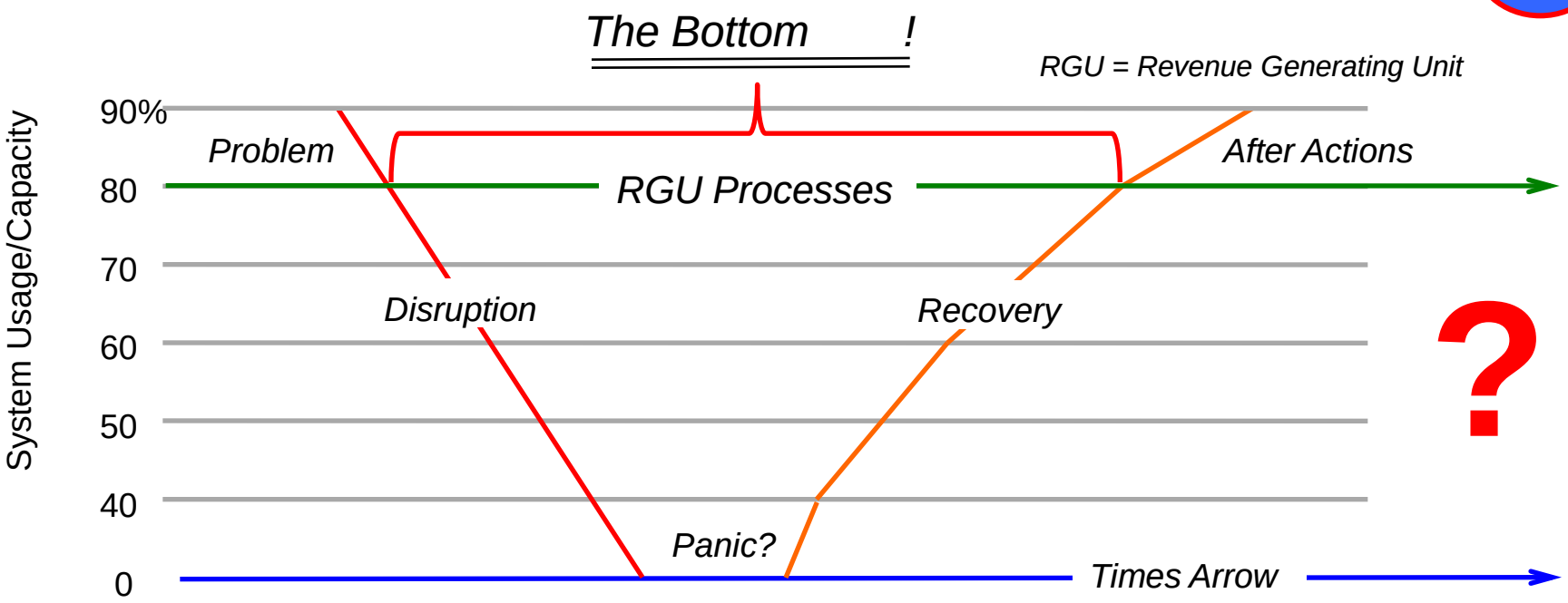
- Chiyang Chin, we call him *Mr. Chin, provides technical support to all NewEra* Software Customers and Prospects Worldwide. He is expert in the z/OS operating system and subsystems with a special interest in the Comm-Server.
- In compiling this document and updates for you, *Mr. Chin will use his* professional efforts to sort out changes and new things in V2R1 and beyond. His work is based on findings from generally available public documentation and presentations. His research, while extensive, is also ongoing, as he learns more expect updates.

Jerry Seefeldt - "Our Members are Leading the Mainframe Revolution!"

Security - What's New in V2R1!

This is all about RAS - Reliability, Availability and Securability

RAS



"…tracking and installing security and system integrity fixes will help to mitigate risk in the System z Environment. Recommended Service Upgrades (RSUs) help to minimize your exposure to security threats and system integrity issues." What level are you at?

Security - What's New in V2R1!

Session Evaluation - Session Number - 14798

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

Thursday, March13, 2014 - 8:00AM
Platinum Ballroom Salon 3
Anaheim Marriott Hotel

Session Number - 14798

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