SHARE
Educate · Network · Influence

Defending System z - Session 16986

The Image Controls Environment (ICE) an Update

Tuesday, March 3, 2015: 4:30 PM - 5:30PM
Sheraton Seattle, Aspen

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

Abstract and Speaker

- The Image Control Environment (ICE) is a System z Software Utility that reinforces and extends the continuum of security and control provided by IBM's RACF, CA-ACF2 and CA-Top Secret over z/OS and z/UNIX resources - datasets, members, files - and MVS/RACF operator commands.

- In this presentation, the following recent enhancements to ICE will be described:

  Break-Glass – Easily implements secondary password access controls over critical System z configuration datasets, files and commands, "raising the access bar" to vital production resources.

  TCE/OPER – An alternative to the conventional MVS Consoles, enforcing command access rights, fully documenting command usage and aiding productivity via Command Specific Wizards.

  CMDLog – A repository of defined MVS and/or RACF operator command events that is used to create an auditable "Real-Time History" of dynamic System z updates/changes.

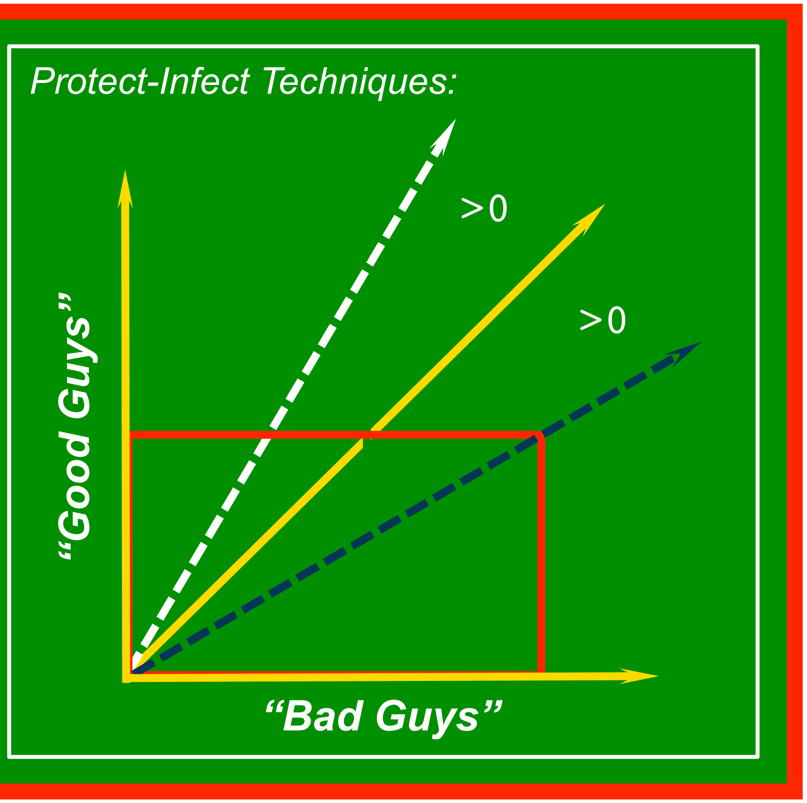
  RACF/SETR - "The one Check to Rule them All" operates totally under the control of the IBM Health Checker for z/OS reporting deviations in SETROPTS settings from conformed rules.

- 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 needed corrections and in doing so, continuously improve z/OS integrity.

Recent ICE Security/Control Enhancements

Secure is when "Bad Guys" have a Negligible Advantage!

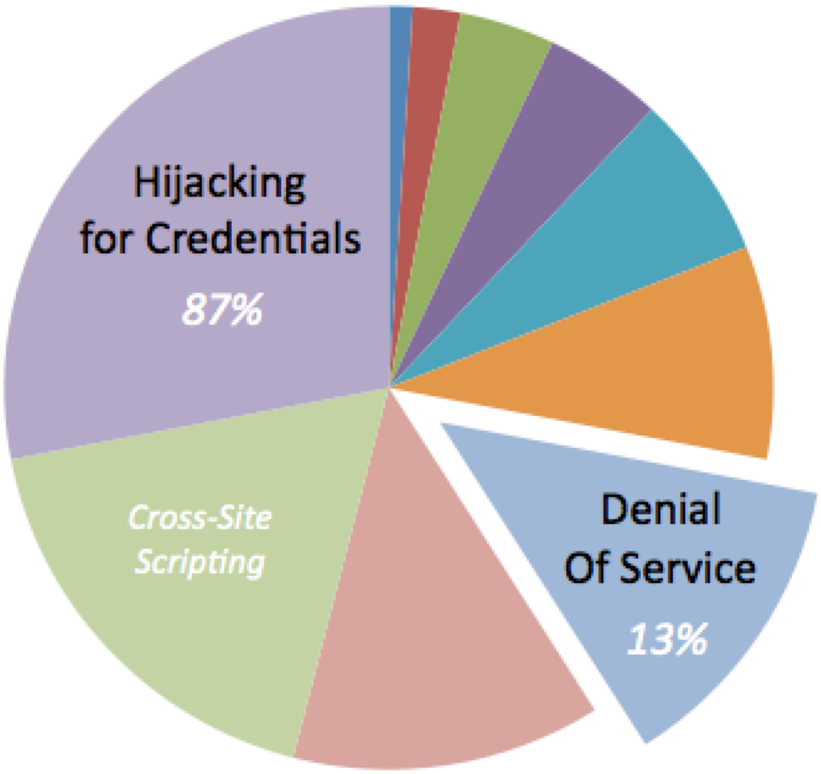


The Goal is to Reduce an Adversary's Advantage to "Zero"!

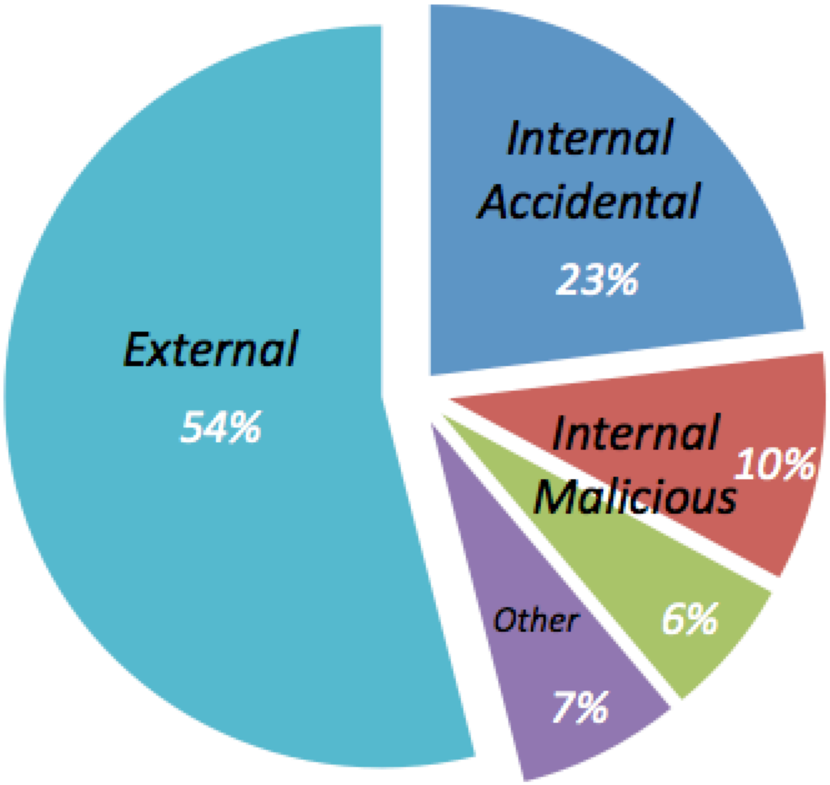
http://en.wikipedia.org/wiki/Advantage_(cryptography)

Recent ICE Security/Control Enhancements

The "Bad Guys" will use every "Trick in the Book"!



From the Outside



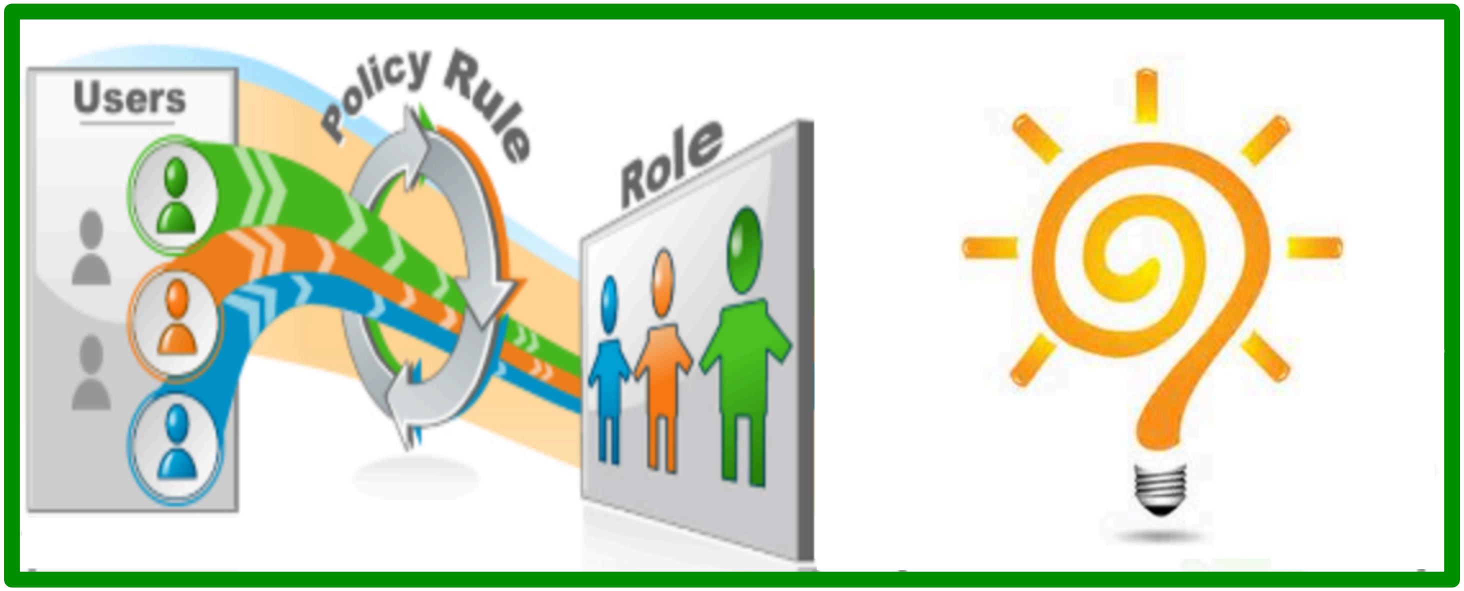
From the Inside

http://www.ibm.com/developerworks/security/library/se-sweep/index.html

Recent ICE Security/Control Enhancements

ESM can no longer do it alone! More needs to be done!

External Security Manager (ESM) *Role Based Access Controls*



Perimeter Configuration Boundary *Configuration - Micro Boundary*

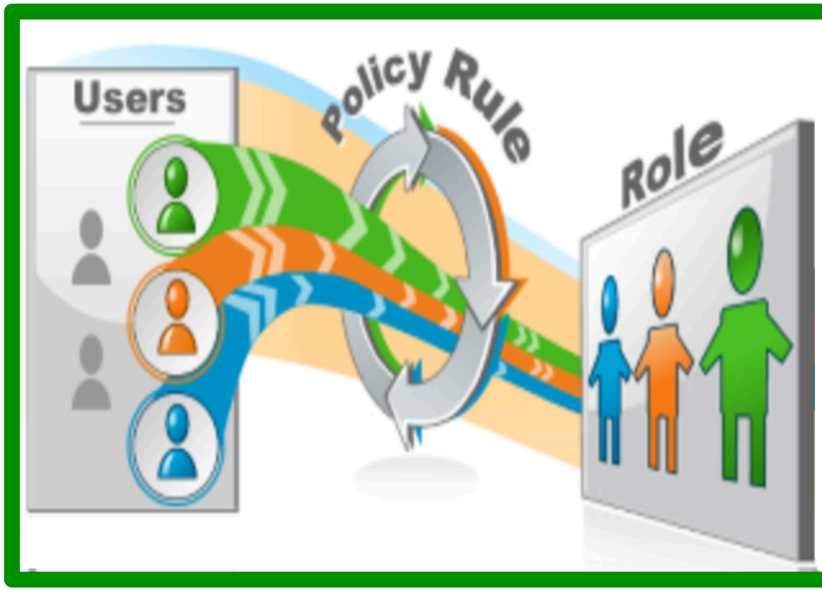
System z Configuration Security-Control Continuum

Recent ICE Security/Control Enhancements

ESM can no longer do it alone! More needs to be done!

External Security Manager (ESM)

Role Based Access Controls



- Change-Event Descriptors
- Reinforce ESM Boundaries
- Multi-Level Authentication
- Event Detection & Logging
- Configuration Conformity

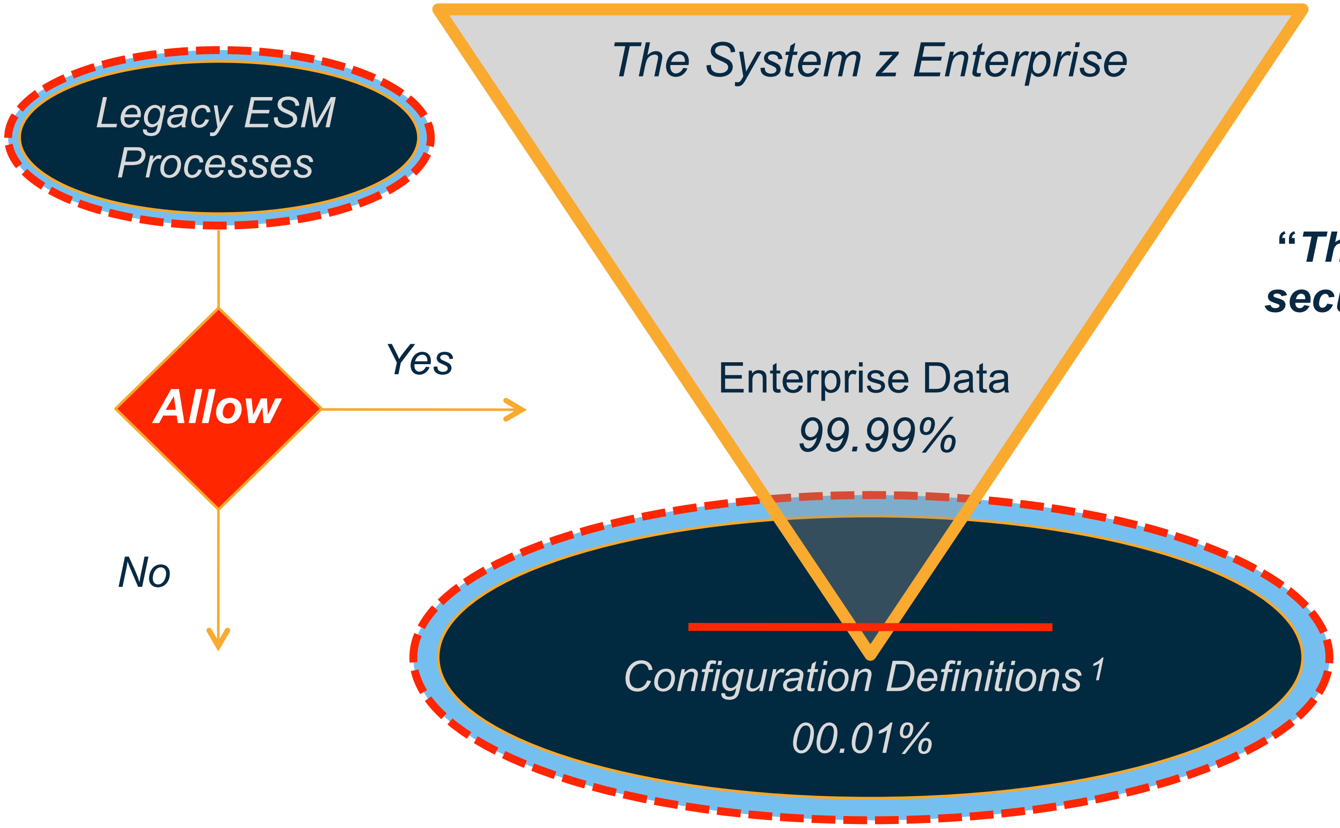
Perimeter Configuration Boundary

Configuration - Micro Boundary

System z Configuration Security-Control Continuum

Recent ICE Security/Control Enhancements

ESM and TCE working Together to Extend the Continuum!

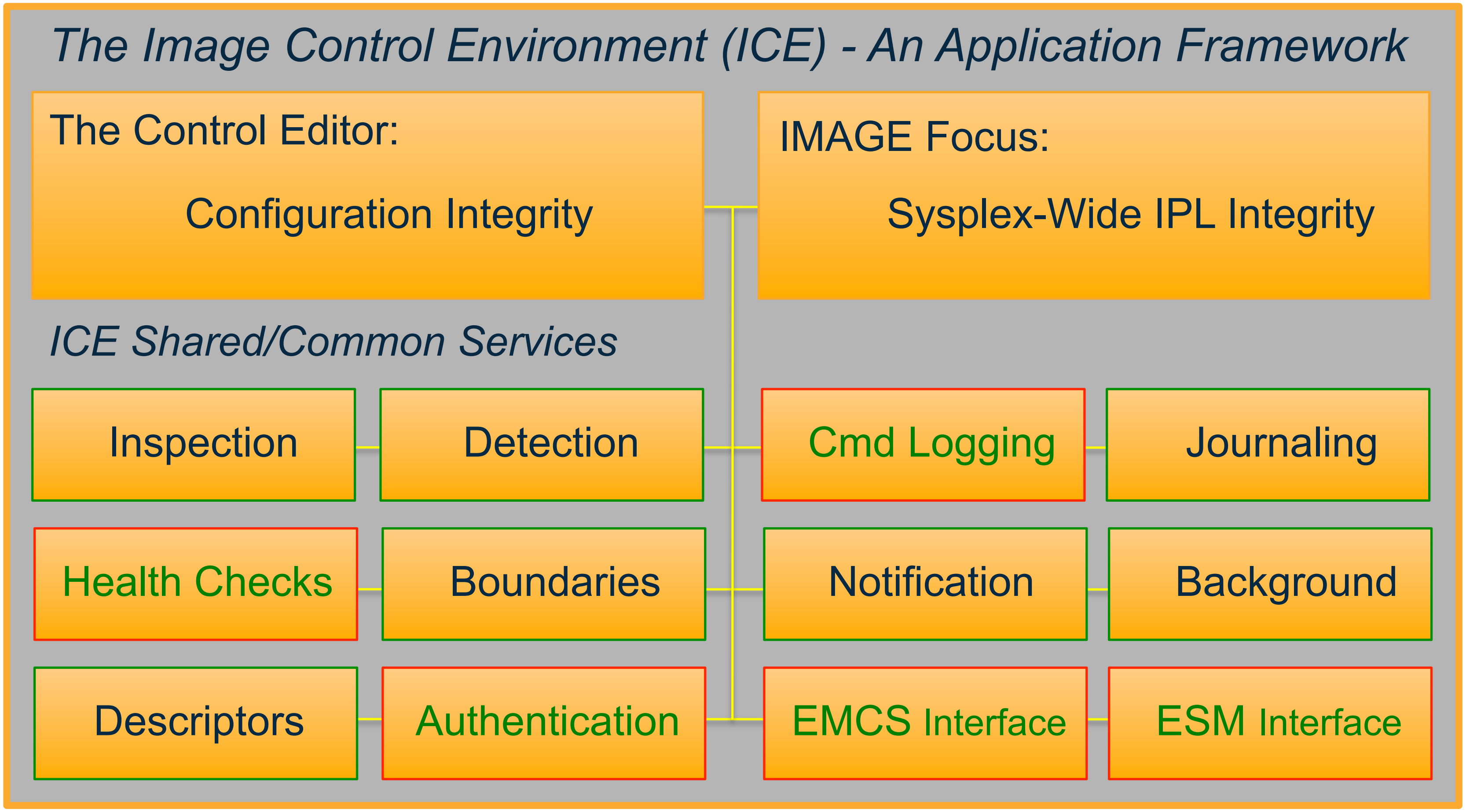


"There can be no system security without operating system integrity."
Barry Schrager

"A Secondary Layer of Control!"

[1] BCP, UNIX, JES, VTAM, TCP/IP, CICS, SMF, ESM, JCL, PARMs & PROCs

Recent ICE Security/Control Enhancements



The Image Control Environment (ICE) - An Application Framework

The Control Editor:

Configuration Integrity

IMAGE Focus:

Sysplex-Wide IPL Integrity

ICE Shared/Common Services

Inspection

Detection

Cmd Logging

Journaling

Health Checks

Boundaries

Notification

Background

Descriptors

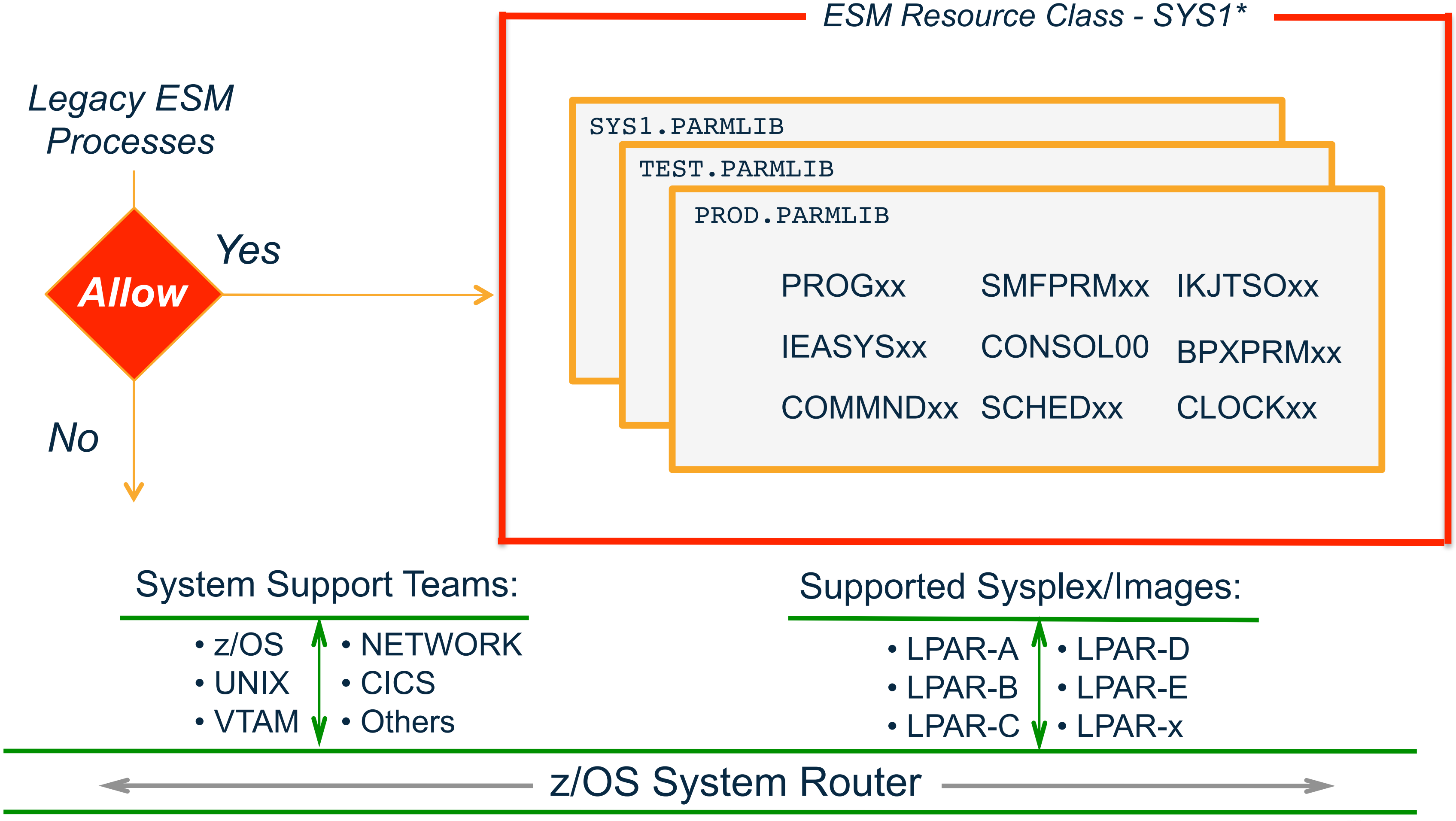
Authentication

EMCS Interface

ESM Interface

ICE Applications and Services are delivered as a ‘Single-Binary’ Copy or SMP/E Installation

Recent ICE Security/Control Enhancements



Recent ICE Security/Control Enhancements

System z Configuration - Sysplex-Wide - Event Logging

☑ *Define Matching TCE Boundaries*!

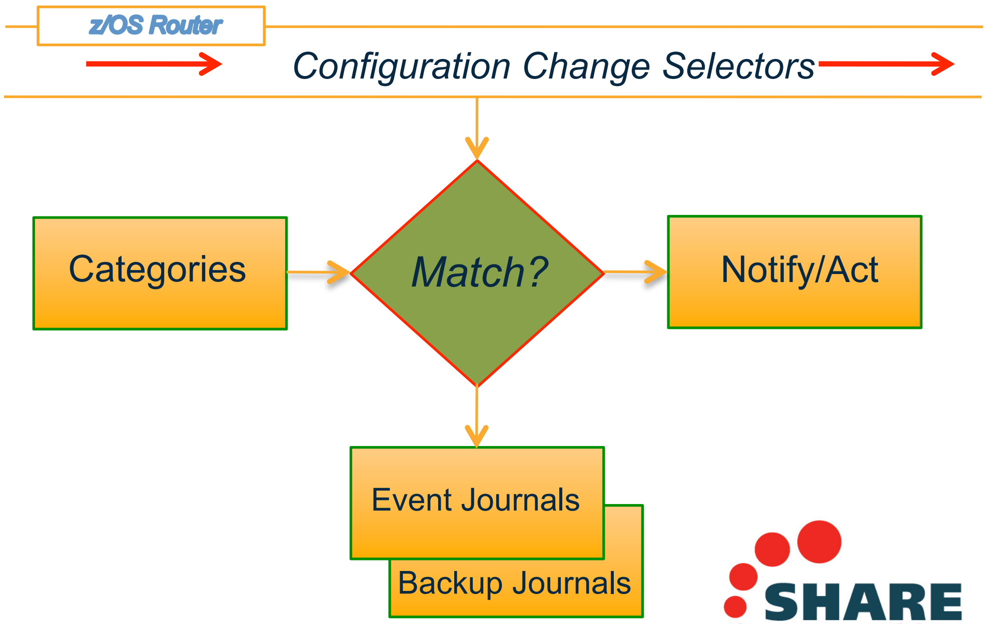
"...The Control Editor is configured using a set of TSO/ISPF Administration Dialogs. The resulting "Control Cards" are stored in members of the ICE Parmlib Dataset.

☑ *Listening for Controlled Events*!

"...One way to envision The Control Editor is to think of it as an *"Event Listener"* on a subsystem interface that allows it to "Hear" all "Events", recording only those that match a predetermined event profile (Control List) and optionally logging all defined events when forensic system analysis is required. These processes require no z/OS modifications, "Hooks" or "Exits" and are totally within the z/OS Administrators control."

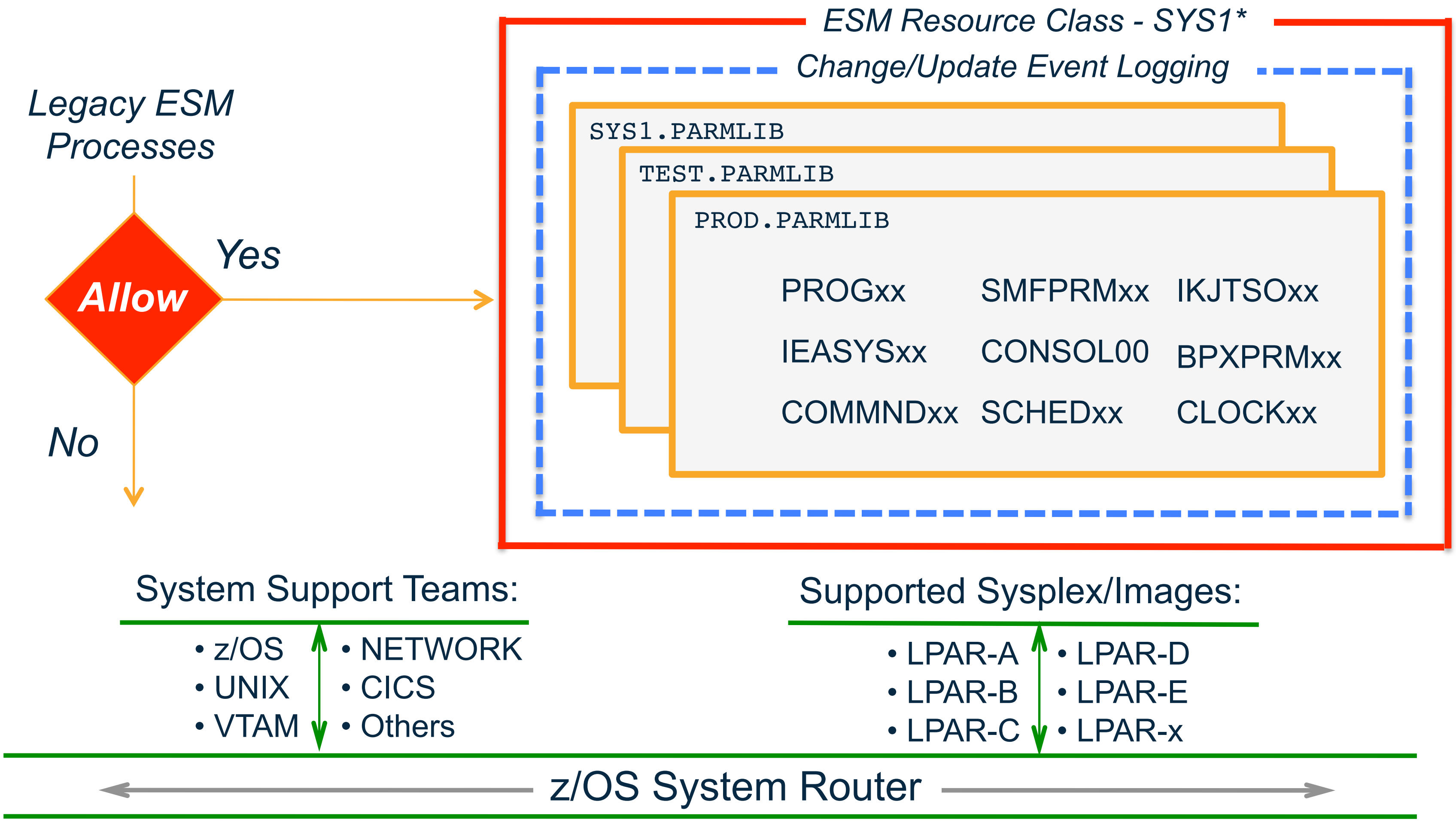
```
HLQ.ICE.Parmlib

  NSEPRMxx
  NSEJRNxx
  NSECTLxx  →
  NSESELxx
  NSEENSxx
```

```
NSECTLxx Control Cards

 CATEGORY IPLDATA.CONTROL
 DSN SYS1.PARMLIB
 DSN TEST.PARMLIB
 DSN PROD.PARMLIB
 CATEGORY .END
```



TCE can Detect Configuration Edits, z/OS & ESM Operator Commands and z/OS System Message Events.

Recent ICE Security/Control Enhancements



Legacy ESM Processes

Allow

Yes

No

ESM Resource Class - SYS1*

Change/Update Event Logging

SYS1.PARMLIB

TEST.PARMLIB

PROD.PARMLIB

PROGxx SMFPRMxx IKJTSOxx

IEASYSxx CONSOL00 BPXPRMxx

COMMNDxx SCHEDxx CLOCKxx

System Support Teams:

- z/OS
- UNIX
- VTAM
- NETWORK
- CICS
- Others

Supported Sysplex/Images:

- LPAR-A
- LPAR-B
- LPAR-C
- LPAR-D
- LPAR-E
- LPAR-x

z/OS System Router

Recent ICE Security/Control Enhancements

System z Configuration - Multi-Level Authentication

☑ *Secondary Access Passwords*!

“...Access to IPL Configuration Datasets for update is clearly the exception and not the rule in most shops. TCE supports “Break Glass” Policy 24X7 and/or by Date/Time.

Second Level Authentication

Passwords are never shown in the clear!

Three Access Prompt Control Scenarios:

1 - Prompt for Password 24X7 - DENY

```
CATEGORY IPLDATA
PROMPT DNY(SDXZD:123NNNM%7)
DSN SYS1.PARMLIB
DSN TEST.PARMLIB
DSN PROD.PARMLIB
CATEGORY .END
```

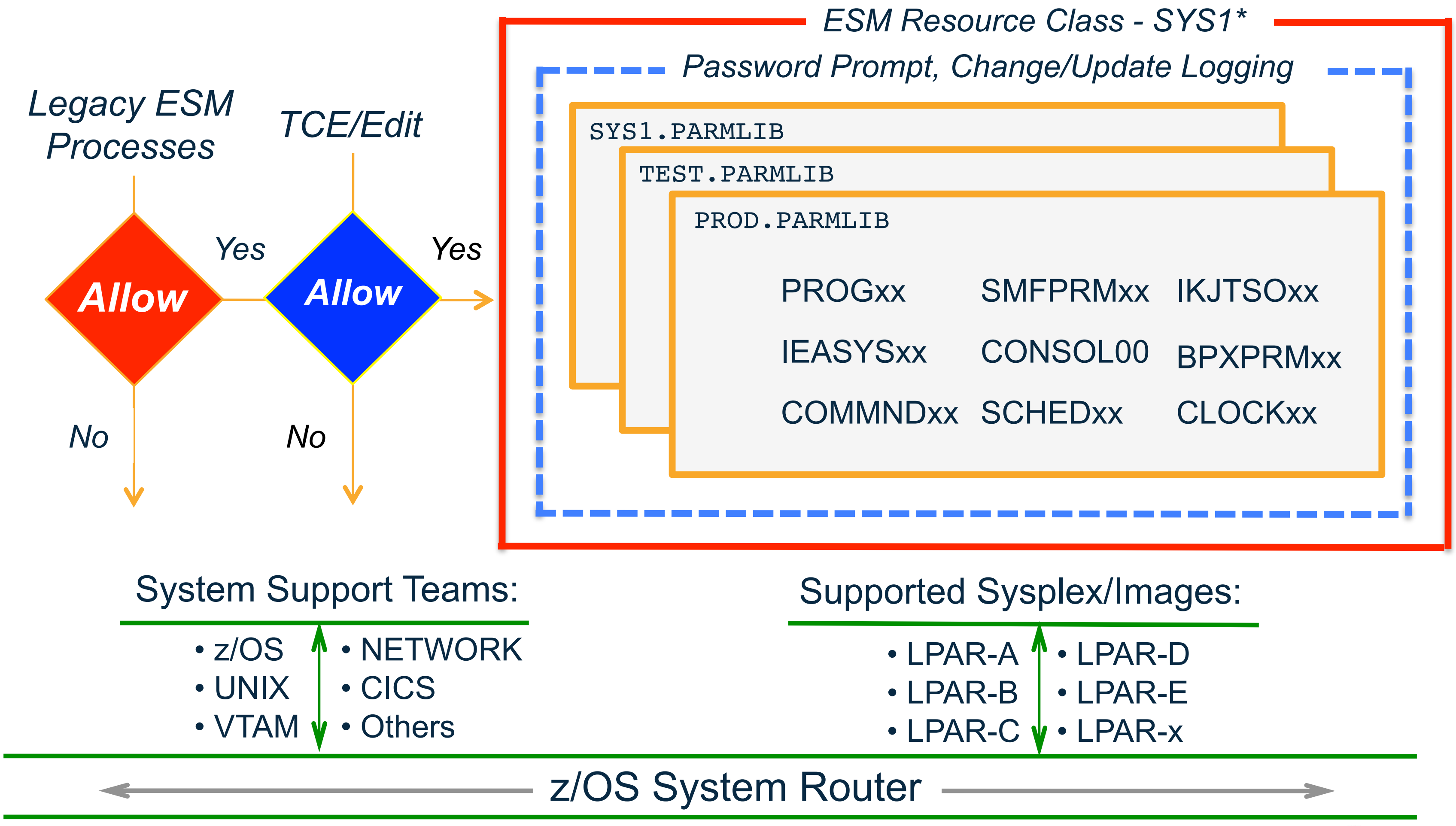
2 - Prompt from 1400 to 0800 Daily - WARN

```
CATEGORY IPLDATA
PROMPT STM(1400) WRN(XZDSD:KLDGGIODF)
DSN SYS1.PARMLIB
DSN TEST.PARMLIB
DSN PROD.PARMLIB
CATEGORY .END
```

3 - Prompt Beginning 14/09/01 then 24X7 - NONE

```
CATEGORY IPLDATA
PROMPT SDT(140901) NOP(CBOFX$BTTXPS!520)
DSN SYS1.PARMLIB
DSN TEST.PARMLIB
DSN PROD.PARMLIB
CATEGORY .END
```

Recent ICE Security/Control Enhancements



Legacy ESM Processes

TCE/Edit

Allow

Yes

Allow

Yes

No

No

ESM Resource Class - SYS1*

Password Prompt, Change/Update Logging

SYS1.PARMLIB

TEST.PARMLIB

PROD.PARMLIB

PROGxx	SMFPRMxx	IKJTSOxx
IEASYSxx	CONSOL00	BPXPRMxx
COMMNDxx	SCHEDxx	CLOCKxx

System Support Teams:

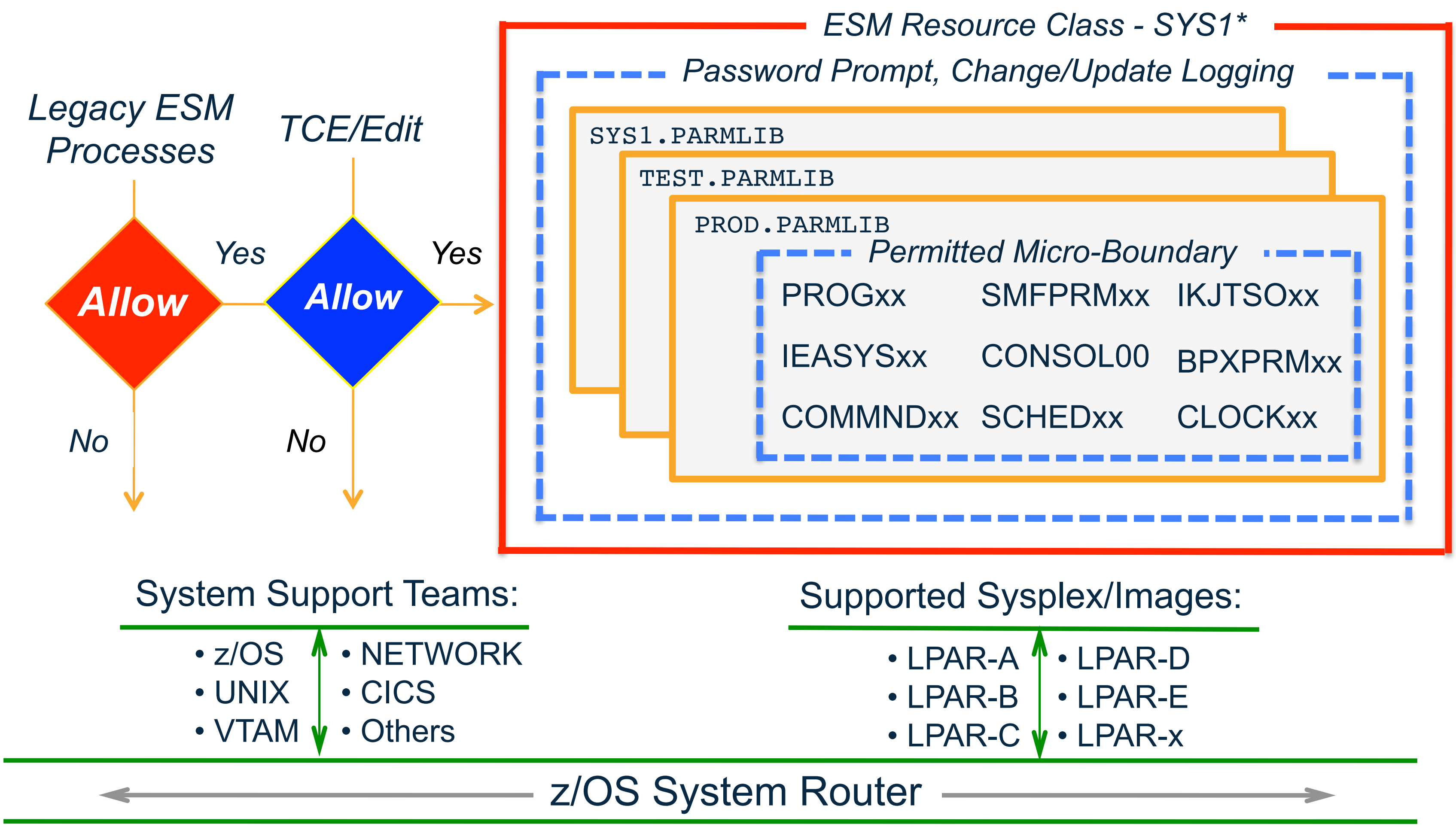
- z/OS
- UNIX
- VTAM
- NETWORK
- CICS
- Others

Supported Sysplex/Images:

- LPAR-A
- LPAR-B
- LPAR-C
- LPAR-D
- LPAR-E
- LPAR-x

z/OS System Router

Recent ICE Security/Control Enhancements



Legacy ESM Processes

TCE/Edit

Allow — *Yes* → **Allow** — *Yes* →

No — *No*

*ESM Resource Class - SYS1**

Password Prompt, Change/Update Logging

SYS1.PARMLIB

TEST.PARMLIB

PROD.PARMLIB

Permitted Micro-Boundary

PROGxx	SMFPRMxx	IKJTSOxx
IEASYSxx	CONSOL00	BPXPRMxx
COMMNDxx	SCHEDxx	CLOCKxx

System Support Teams:

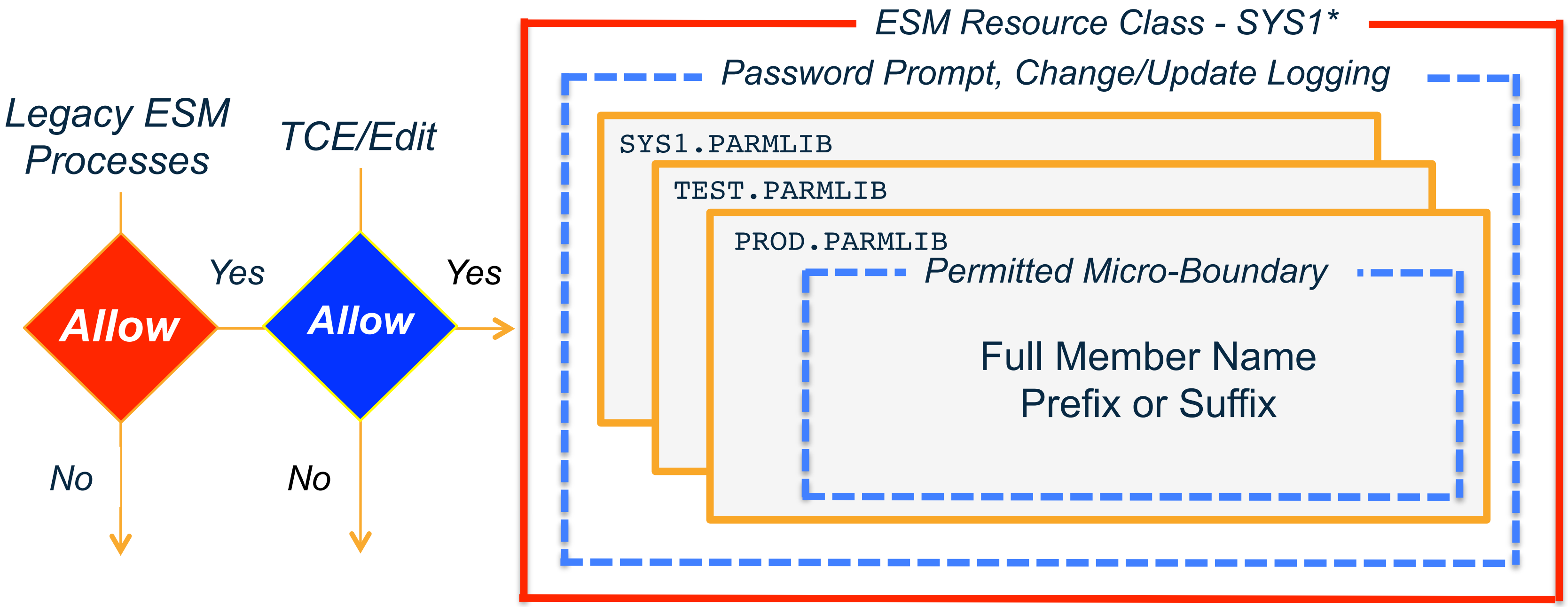
- z/OS
- UNIX
- VTAM
- NETWORK
- CICS
- Others

Supported Sysplex/Images:

- LPAR-A
- LPAR-B
- LPAR-C
- LPAR-D
- LPAR-E
- LPAR-x

z/OS System Router

Recent ICE Security/Control Enhancements



Legacy ESM Processes

TCE/Edit

Allow

Yes

No

Allow

Yes

No

ESM Resource Class - SYS1*

Password Prompt, Change/Update Logging

SYS1.PARMLIB

TEST.PARMLIB

PROD.PARMLIB

Permitted Micro-Boundary

Full Member Name
Prefix or Suffix

System Support Teams:

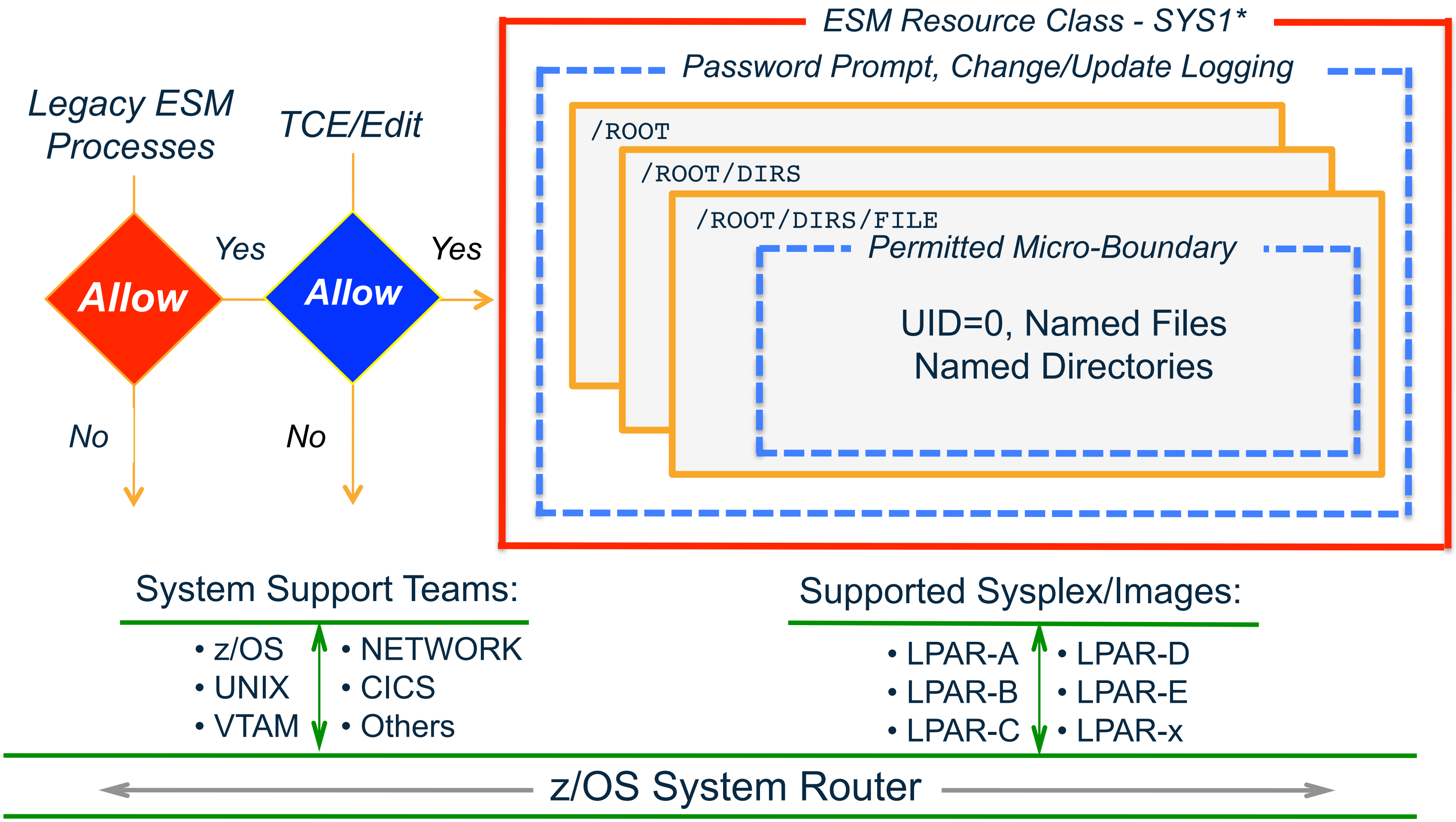
- z/OS
- UNIX
- VTAM
- NETWORK
- CICS
- Others

Supported Sysplex/Images:

- LPAR-A
- LPAR-B
- LPAR-C
- LPAR-D
- LPAR-E
- LPAR-x

z/OS System Router

Recent ICE Security/Control Enhancements



Legacy ESM Processes

TCE/Edit

Allow

Yes

No

Allow

Yes

No

*ESM Resource Class - SYS1**

Password Prompt, Change/Update Logging

/ROOT

/ROOT/DIRS

/ROOT/DIRS/FILE

Permitted Micro-Boundary

UID=0, Named Files
Named Directories

System Support Teams:

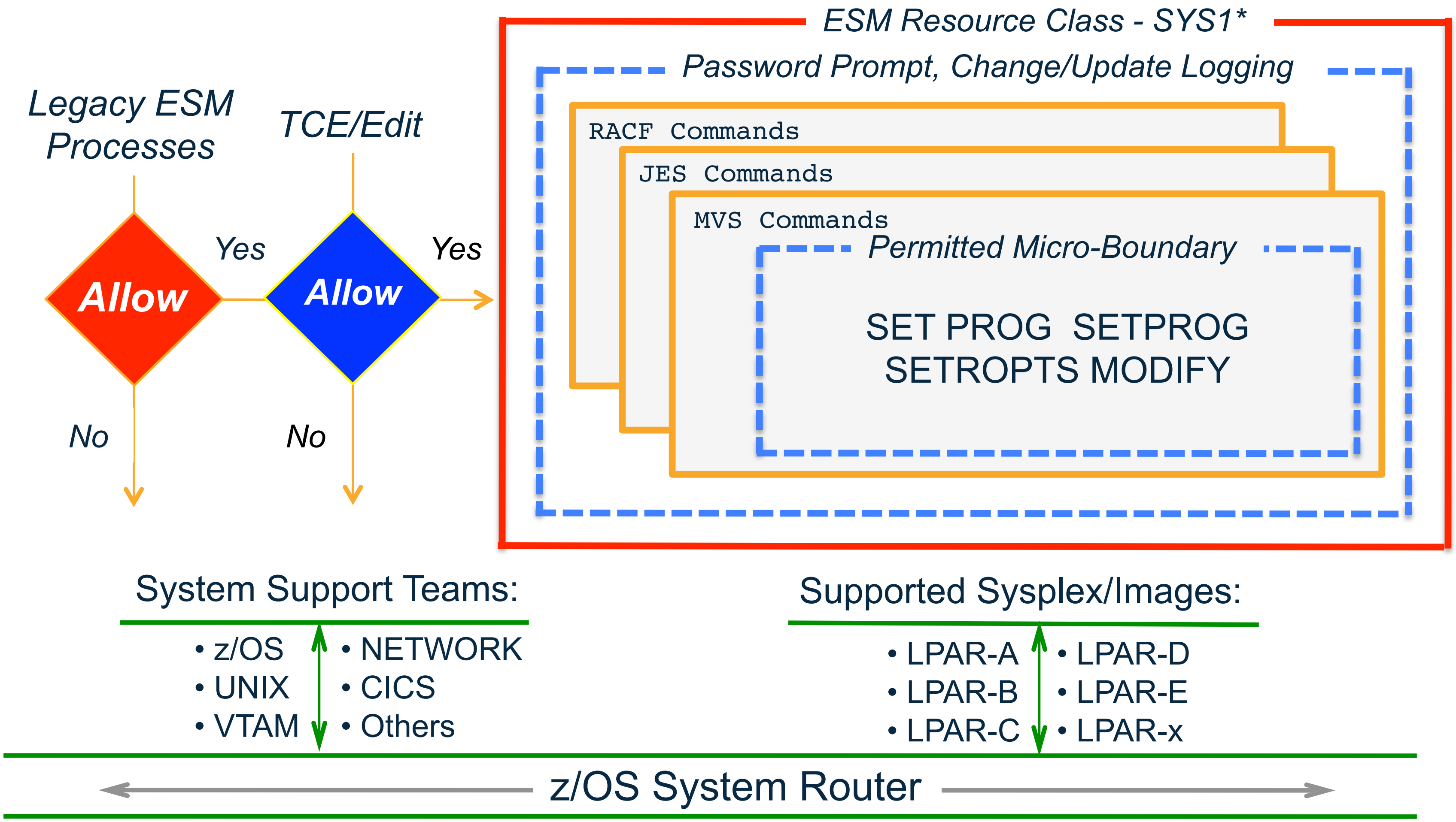
- z/OS
- UNIX
- VTAM
- NETWORK
- CICS
- Others

Supported Sysplex/Images:

- LPAR-A
- LPAR-B
- LPAR-C
- LPAR-D
- LPAR-E
- LPAR-x

z/OS System Router

Recent ICE Security/Control Enhancements



Legacy ESM Processes

TCE/Edit

Allow

Allow

Yes

Yes

No

No

ESM Resource Class - SYS1*

Password Prompt, Change/Update Logging

RACF Commands

JES Commands

MVS Commands

Permitted Micro-Boundary

SET PROG SETPROG
SETROPTS MODIFY

System Support Teams:

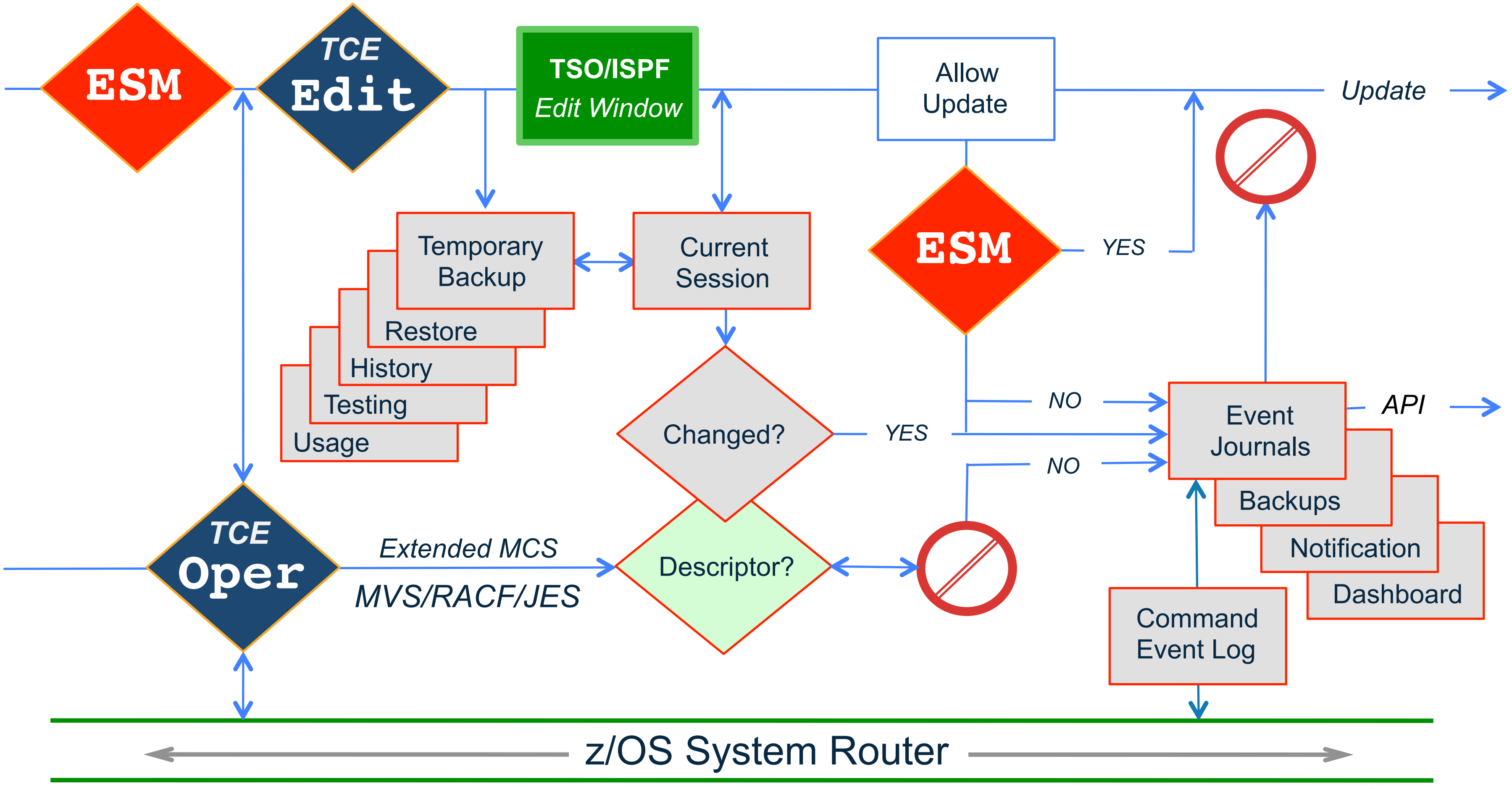
- z/OS
- UNIX
- VTAM
- NETWORK
- CICS
- Others

Supported Sysplex/Images:

- LPAR-A
- LPAR-B
- LPAR-C
- LPAR-D
- LPAR-E
- LPAR-x

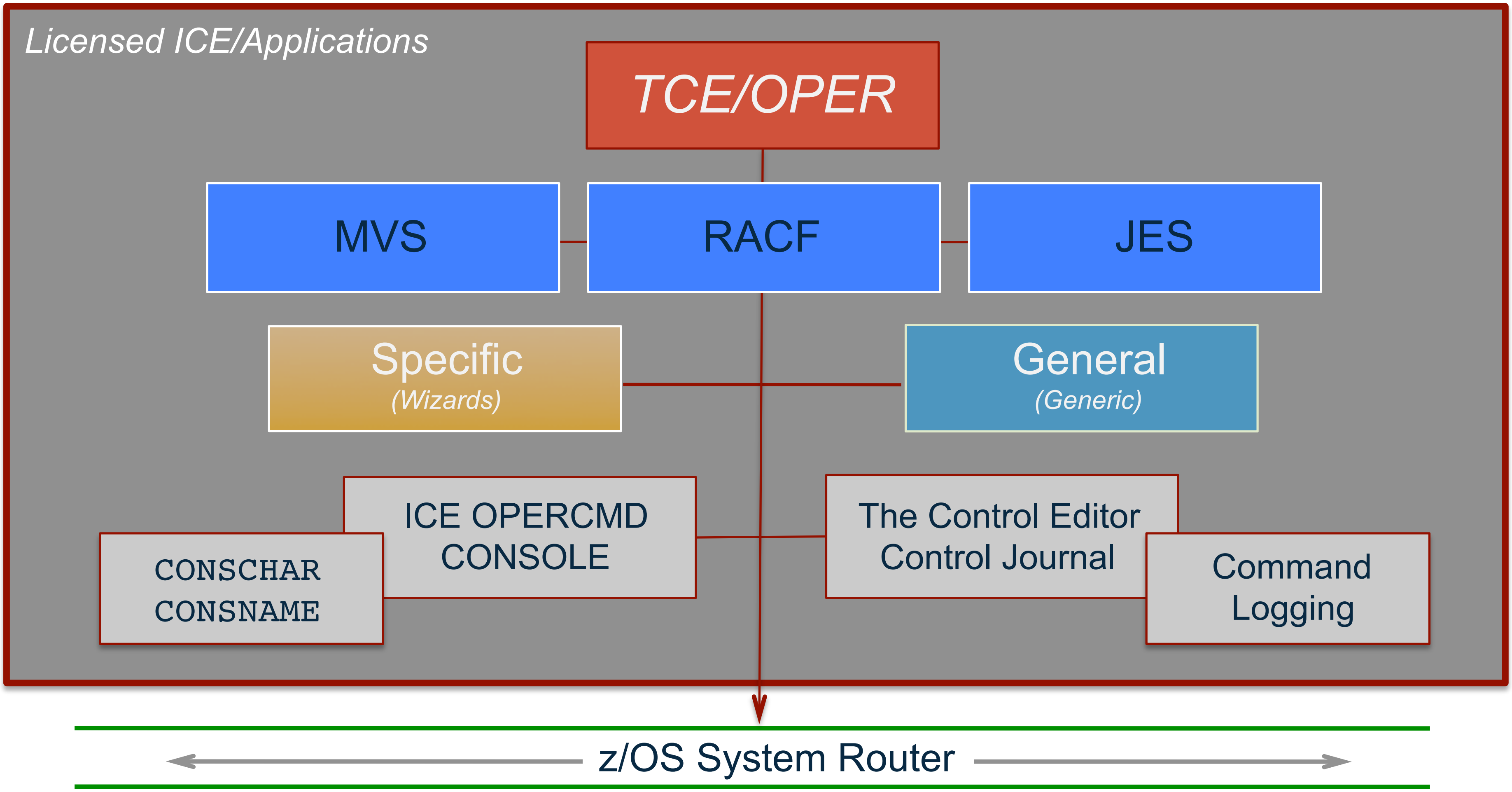
z/OS System Router

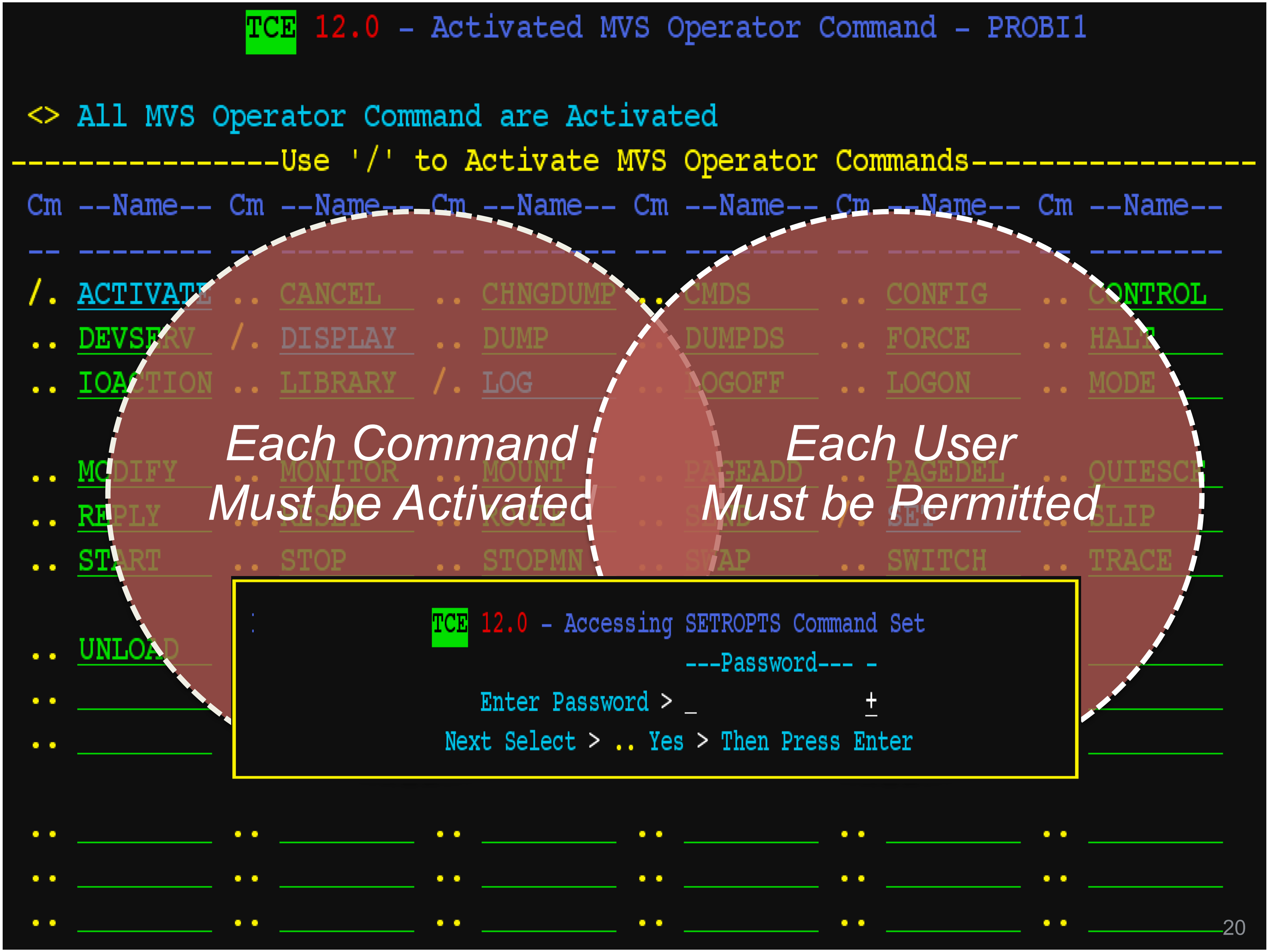
Recent ICE Security/Control Enhancements



Point-of-Change Documentation Requirement added to collect detail from the Change Maker!

Recent ICE Security/Control Enhancements



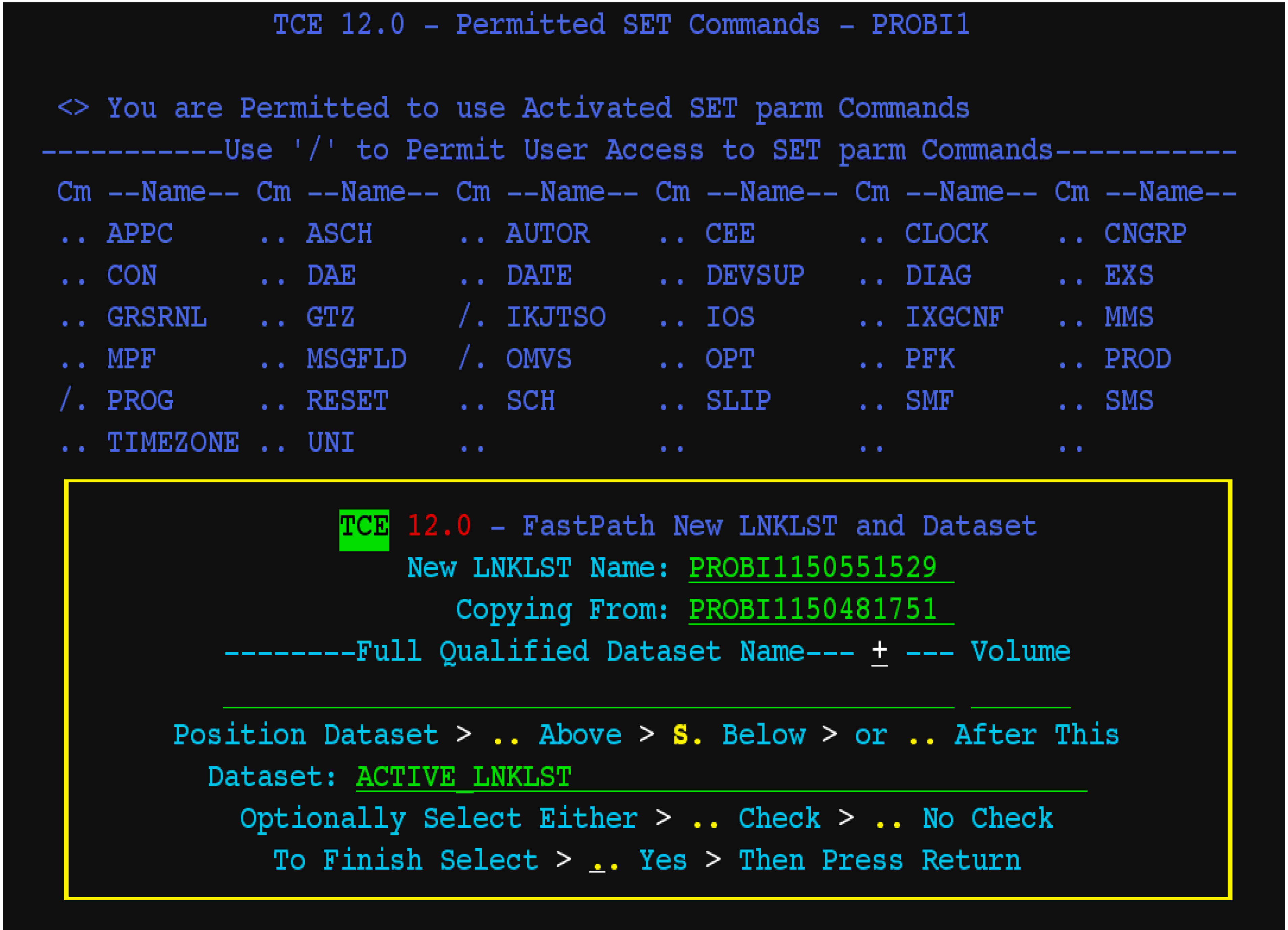


```
               TCE 12.0 - Activated MVS Operator Command - PROBI1

 <> All MVS Operator Command are Activated
----------------Use '/' to Activate MVS Operator Commands-----------------
 Cm --Name-- Cm --Name-- Cm --Name-- Cm --Name-- Cm --Name-- Cm --Name--
 -- -------- -- -------- -- -------- -- -------- -- -------- -- --------
 /. ACTIVATE .. CANCEL   .. CHNGDUMP .. CMDS     .. CONFIG   .. CONTROL
 .. DEVSERV  /. DISPLAY  .. DUMP     .. DUMPDS   .. FORCE    .. HALT
 .. IOACTION .. LIBRARY  /. LOG      .. LOGOFF   .. LOGON    .. MODE

 .. MODIFY   .. MONITOR  .. MOUNT    .. PAGEADD  .. PAGEDEL  .. QUIESCE
 .. REPLY    .. RESET    .. ROUTE    .. SEND     /. SET      .. SLIP
 .. START    .. STOP     .. STOPMN   .. SWAP     .. SWITCH   .. TRACE

 .. UNLOAD                                                   ________
 .. ________                                                 ________
 .. ________                                                 ________

 .. ________ .. ________ .. ________ .. ________ .. ________ .. ________
 .. ________ .. ________ .. ________ .. ________ .. ________ .. ________
 .. ________ .. ________ .. ________ .. ________ .. ________ .. ________
```

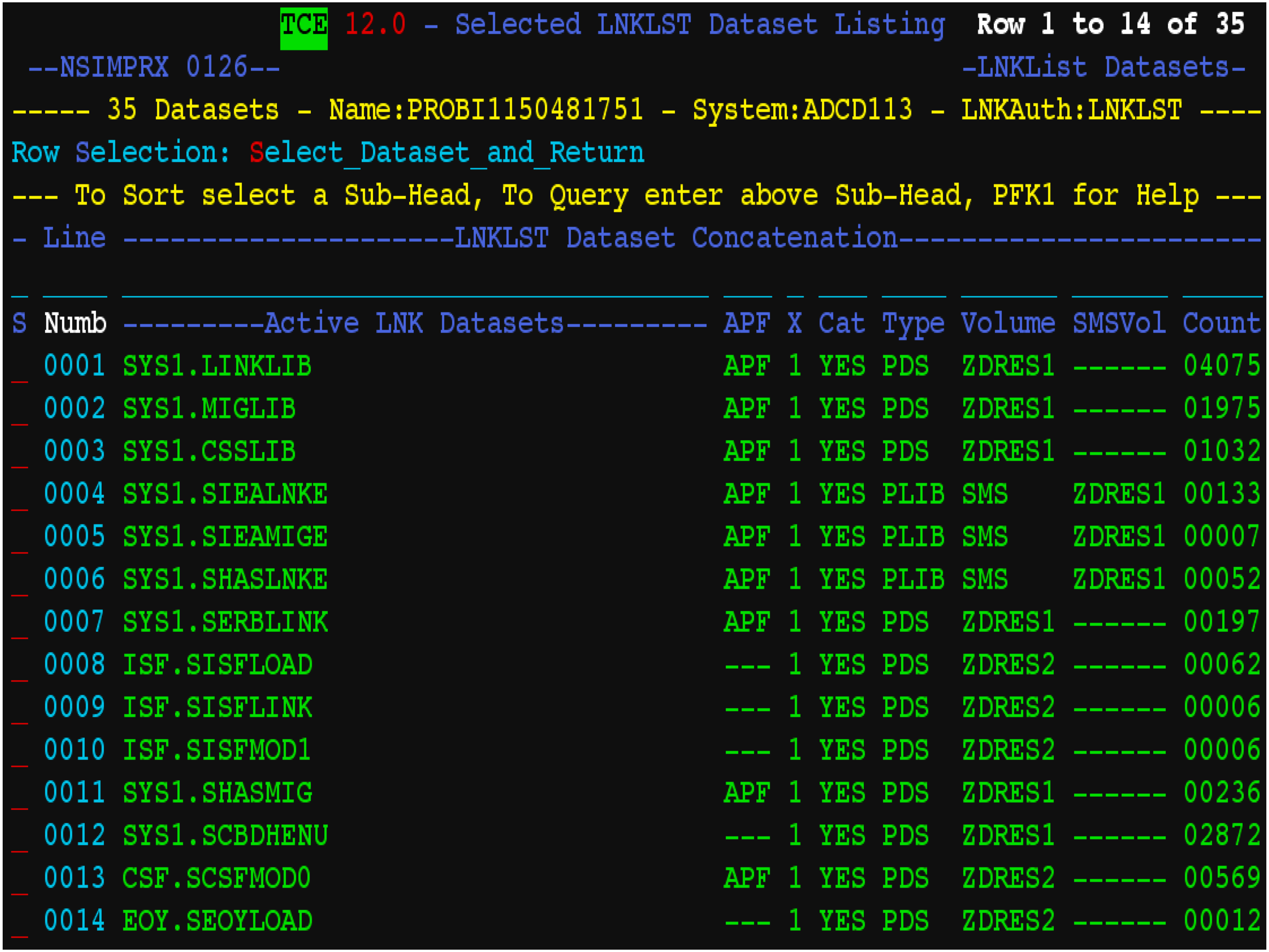
```
          TCE 12.0 - Accessing SETROPTS Command Set
                         ---Password--- -
          Enter Password > _            +
       Next Select > .. Yes > Then Press Enter
```

Each Command
Must be Activated

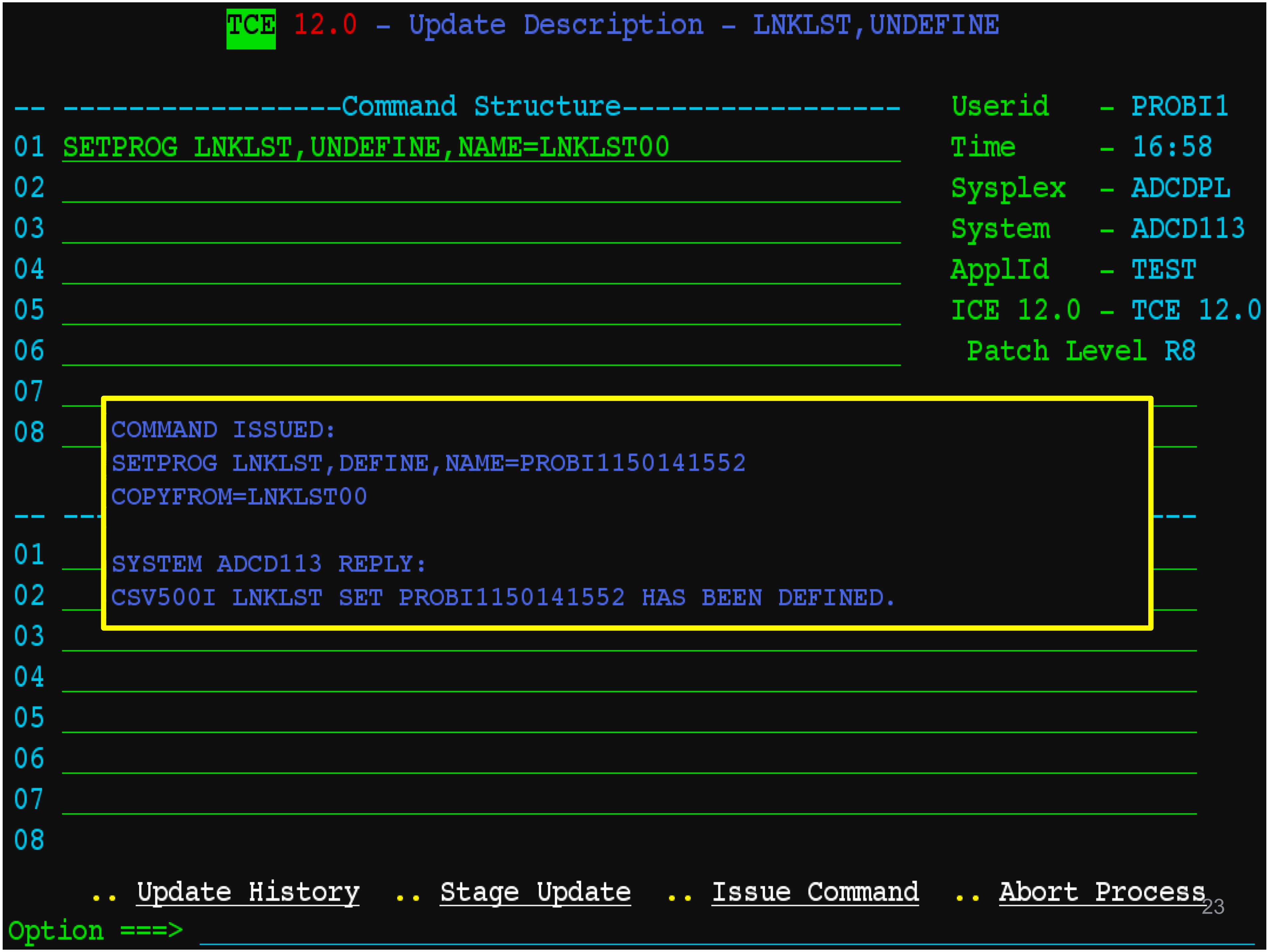
Each User
Must be Permitted



```
              TCE 12.0 - Permitted SET Commands - PROBI1

  <> You are Permitted to use Activated SET parm Commands
 -----------Use '/' to Permit User Access to SET parm Commands-----------
  Cm --Name-- Cm --Name-- Cm --Name-- Cm --Name-- Cm --Name-- Cm --Name--
  .. APPC     .. ASCH     .. AUTOR    .. CEE      .. CLOCK    .. CNGRP
  .. CON      .. DAE      .. DATE     .. DEVSUP   .. DIAG     .. EXS
  .. GRSRNL   .. GTZ      /. IKJTSO   .. IOS      .. IXGCNF   .. MMS
  .. MPF      .. MSGFLD   /. OMVS     .. OPT      .. PFK      .. PROD
  /. PROG     .. RESET    .. SCH      .. SLIP     .. SMF      .. SMS
  .. TIMEZONE .. UNI      ..          ..          ..          ..

                TCE 12.0 - FastPath New LNKLST and Dataset
                    New LNKLST Name: PROBI1150551529
                       Copying From: PROBI1150481751
          --------Full Qualified Dataset Name--- + --- Volume

       Position Dataset > .. Above > S. Below > or .. After This
         Dataset: ACTIVE_LNKLST
           Optionally Select Either > .. Check > .. No Check
             To Finish Select > .. Yes > Then Press Return
```



```
                 TCE 12.0 - Selected LNKLST Dataset Listing  Row 1 to 14 of 35
 --NSIMPRX 0126--                                           -LNKList Datasets-
----- 35 Datasets - Name:PROBI1150481751 - System:ADCD113 - LNKAuth:LNKLST ----
Row Selection: Select_Dataset_and_Return
--- To Sort select a Sub-Head, To Query enter above Sub-Head, PFK1 for Help ---
- Line ---------------------LNKLST Dataset Concatenation------------------------

_ ____ _____________________________________ ___ _ ___ ____ ______ ______ _____
S Numb ---------Active LNK Datasets--------- APF X Cat Type Volume SMSVol Count
_ 0001 SYS1.LINKLIB                          APF 1 YES PDS  ZDRES1 ------ 04075
_ 0002 SYS1.MIGLIB                           APF 1 YES PDS  ZDRES1 ------ 01975
_ 0003 SYS1.CSSLIB                           APF 1 YES PDS  ZDRES1 ------ 01032
_ 0004 SYS1.SIEALNKE                         APF 1 YES PLIB SMS    ZDRES1 00133
_ 0005 SYS1.SIEAMIGE                         APF 1 YES PLIB SMS    ZDRES1 00007
_ 0006 SYS1.SHASLNKE                         APF 1 YES PLIB SMS    ZDRES1 00052
_ 0007 SYS1.SERBLINK                         APF 1 YES PDS  ZDRES1 ------ 00197
_ 0008 ISF.SISFLOAD                          --- 1 YES PDS  ZDRES2 ------ 00062
_ 0009 ISF.SISFLINK                          --- 1 YES PDS  ZDRES2 ------ 00006
_ 0010 ISF.SISFMOD1                          --- 1 YES PDS  ZDRES2 ------ 00006
_ 0011 SYS1.SHASMIG                          APF 1 YES PDS  ZDRES1 ------ 00236
_ 0012 SYS1.SCBDHENU                         --- 1 YES PDS  ZDRES1 ------ 02872
_ 0013 CSF.SCSFMOD0                          APF 1 YES PDS  ZDRES2 ------ 00569
_ 0014 EOY.SEOYLOAD                          --- 1 YES PDS  ZDRES2 ------ 00012
```



```
             TCE 12.0 - Update Description - LNKLST,UNDEFINE

-- ----------------Command Structure-----------------  Userid   - PROBI1
01 SETPROG LNKLST,UNDEFINE,NAME=LNKLST00                Time     - 16:58
02                                                      Sysplex  - ADCDPL
03                                                      System   - ADCD113
04                                                      ApplId   - TEST
05                                                      ICE 12.0 - TCE 12.0
06                                                       Patch Level R8
07
08    COMMAND ISSUED:
      SETPROG LNKLST,DEFINE,NAME=PROBI1150141552
      COPYFROM=LNKLST00
-- ---
      SYSTEM ADCD113 REPLY:
01    CSV500I LNKLST SET PROBI1150141552 HAS BEEN DEFINED.
02
03
04
05
06
07
08

     .. Update History  .. Stage Update  .. Issue Command  .. Abort Process
Option ===>
```

“Taming SETROPTS”

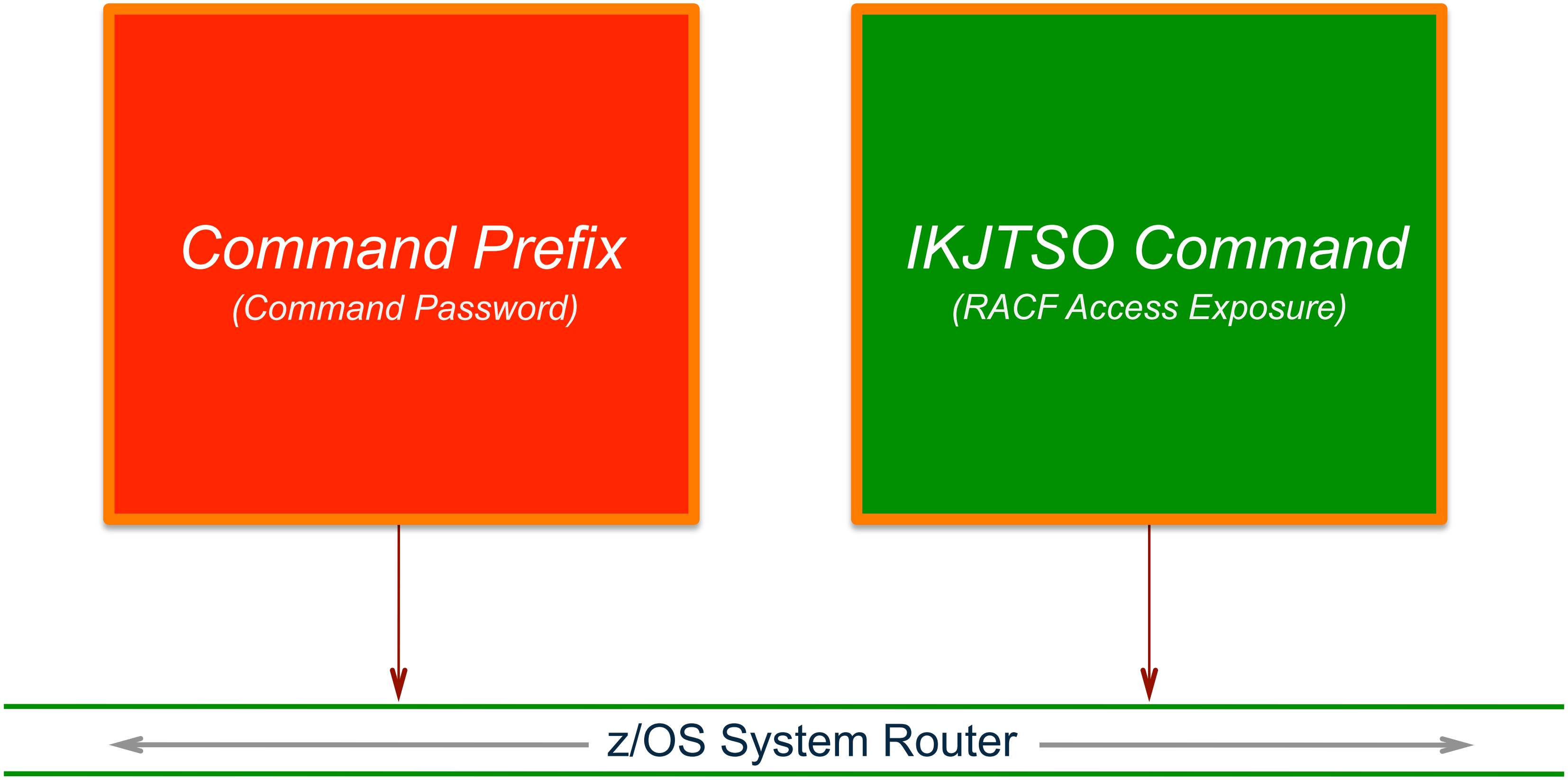
ADDCREATOR | NOADDCREATOR
ADSP | NOADSP
APPLAUDIT | NOAPPLAUDIT
AT | ONLYAT([node].userid)
AUDIT | NOAUDIT (class-name)
CATDSNS (FAIL | WARN) | NOCAT
CLASSACT | NOCLASSACT} (class-name)
CMDVIOL | NOCMDVIOL
COMPATMODE | NOCOMPATMODE
EGN | NOEGN
ERASE(ALL|SECLEVEL | NOSECLEVEL | NOERASE
GENCMD | NOGENCMD (class-name)
GENERIC | NOGENERIC (class-name)
GENERICOWNER | NOGENERICOWNER
GENLIST | NOGENLIST (class-name)
GLOBAL | NOGLOBAl (class-name)
GRPLIST | NOGRPLIST
INACTIVE(unused-userid-interval) | NOINACTIVE
INITSTATS | NOINITSTATS
BATCHALLRACF | NOBATCHALLRACF
EARLYVERIFY | NOEARLYVERIFY
XBMALLRACF | NOXBMALLRACF
NJEUSERID(userid)
UNDEFINEDUSER(userid)
KERBLVL(0|1)
LANGUAGE(PRIMARY) or (SECONDARY)
LOGOPTIONS(ALWAYS(class-name)
LOGOPTIONS(NEVER(class-name)
LOGOPTIONS(SUCCESSES(class-name)
LOGOPTIONS(FAILURES(class-name)
LOGOPTIONS(DEFAULT({class-name)
MLACTIVE [(FAILURES | WARNING)] | NOMLACTIVE]
MLFSOBJ (ACTIVE | INACTIVE)
MLIPCOBJ (ACTIVE | INACTIVE)

MLNAMES | NOMLNAMES
MLQUIET | NOMLQUIET
MLS [(FAILURES | WARNING)] | NOMLS
MLSTABLE | NOMLSTABLE
MODEL(GDG | NOGDG)
MODEL(GROUP | NOGROUP)
MODEL(USER | NOUSER)
NOMODEL
OPERAUDIT | NOOPERAUDIT
PASSWORD(HISTORY(number) | NOHISTORY))
PASSWORD(INTERVAL(maximum))
PASSWORD(MINCHANGE(minimum))
PASSWORD(MIXEDCASE | NOMIXEDCASE))
PASSWORD(REVOKE(attempts) | NOREVOKE))
PASSWORD(RULEn(LENGTH(m1:m2) content(position))
PASSWORD(NORULEn)
PASSWORD(NORULES)
PASSWORD(WARNING(days-before) | NOWARNING))
PREFIX(prefix) | NOPREFIX
PROTECTALL [(FAILURES | WARNING)] | NOPROTECTALL
RACLIST | NORACLIST} (class-name)
REALDSN | NOREALDSN
RETPD(nnnnn)
RVARYPW([SWITCH(switch-pw)] [STATUS(status-pw)])
SAUDIT | NOSAUDIT
SECLABELAUDIT | NOSECLABELAUDIT
SECLABELCONTROL | NOSECLABELCONTROL
SECLBYSYSTEM | NOSECLBYSYSTEM]
SECLEVELAUDIT (security-level) | NOSECLEVELAUDIT
SESSIONINTERVAL(n) | NOSESSIONINTERVAL
STATISTICS | NOSTATISTICS} ({class-name)
TAPEDSN | NOTAPEDSN
TERMINAL(NONE | READ)
WHEN | NOWHEN} (PROGRAM)

SETROPTS commands dynamically set system-wide RACF Security Control Options.

Recent ICE Security/Control Enhancements

More Control, More Productivity, More Flexibility!



Command Prefix

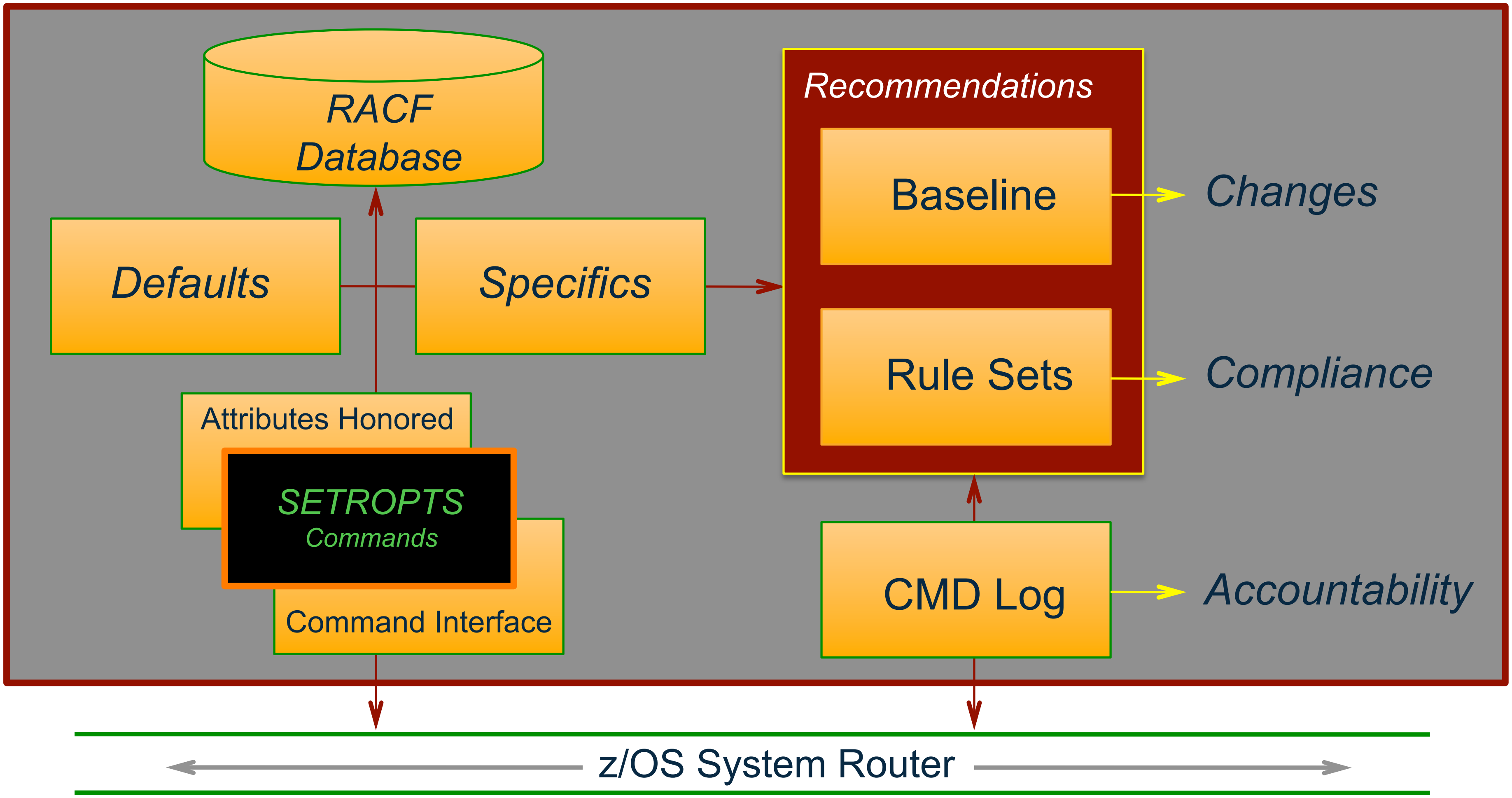
(Command Password)

IKJTSO Command

(RACF Access Exposure)

z/OS System Router

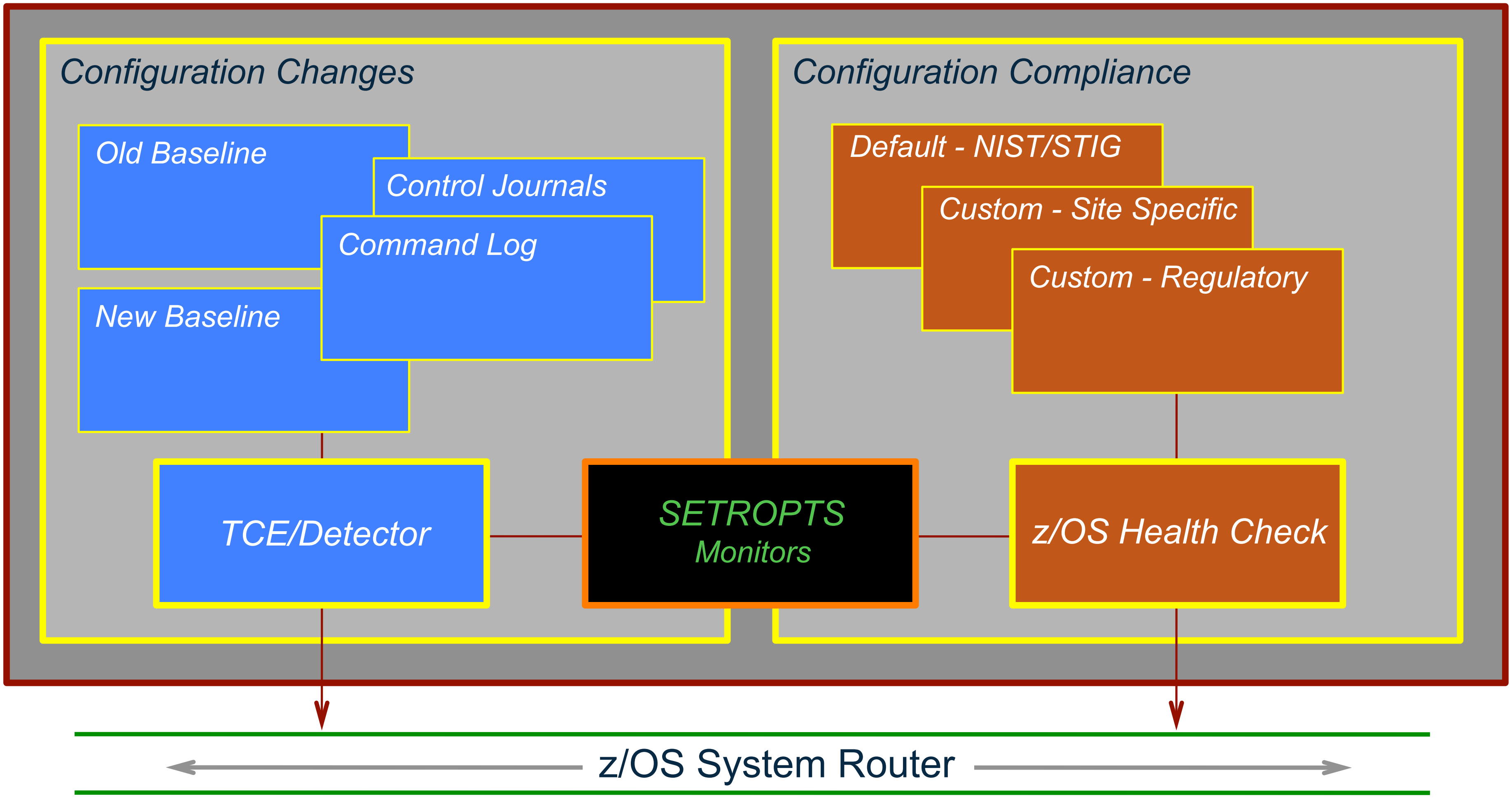
Recent ICE Security/Control Enhancements



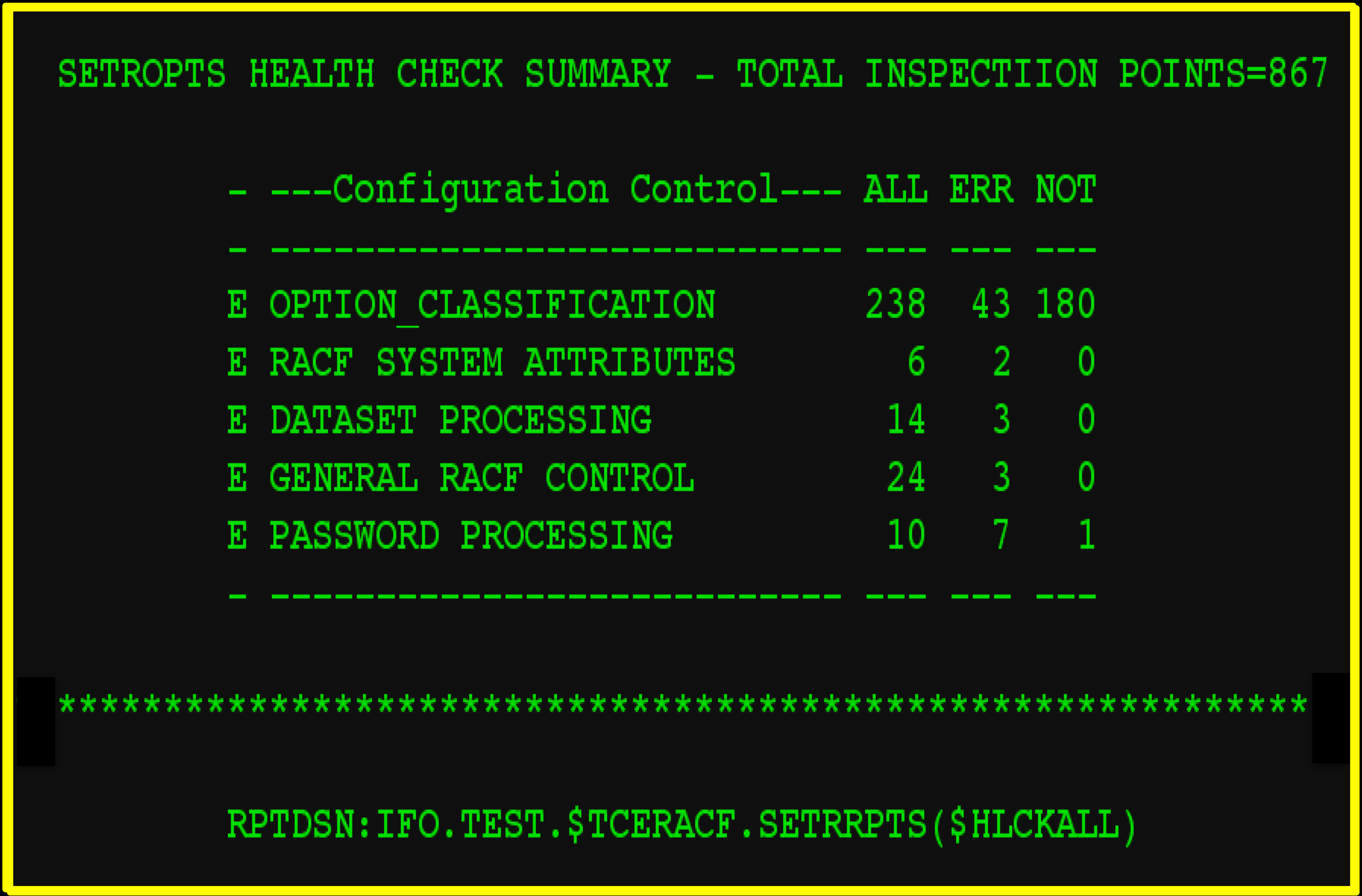
Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Recommandations based on: Risk Management Framework (RMF) for DoD IT - NIST z/OS RACF STIG v6r21

Recent ICE Security/Control Enhancements

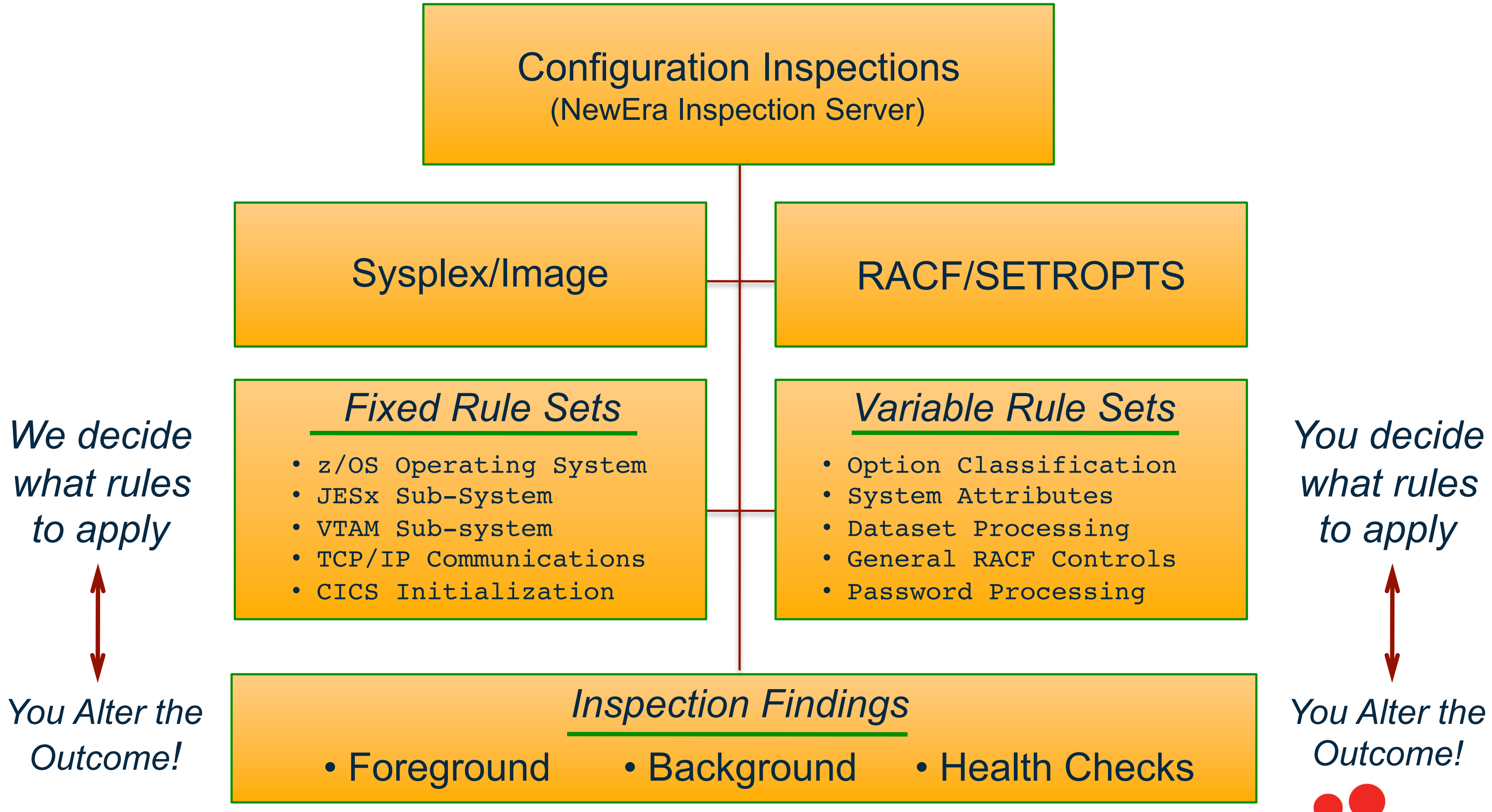


One Health Check to Rule them All!



```
SETROPTS HEALTH CHECK SUMMARY - TOTAL INSPECTIION POINTS=867

        - ---Configuration Control--- ALL ERR NOT
        - --------------------------- --- --- ---
        E OPTION_CLASSIFICATION       238  43 180
        E RACF SYSTEM ATTRIBUTES        6   2   0
        E DATASET PROCESSING           14   3   0
        E GENERAL RACF CONTROL         24   3   0
        E PASSWORD PROCESSING          10   7   1
        - --------------------------- --- --- ---

***********************************************************

        RPTDSN:IFO.TEST.$TCERACF.SETRRPTS($HLCKALL)
```

Recent ICE Security/Control Enhancements



Configuration Inspections
(NewEra Inspection Server)

Sysplex/Image

RACF/SETROPTS

Fixed Rule Sets

- z/OS Operating System
- JESx Sub-System
- VTAM Sub-system
- TCP/IP Communications
- CICS Initialization

Variable Rule Sets

- Option Classification
- System Attributes
- Dataset Processing
- General RACF Controls
- Password Processing

We decide what rules to apply

You Alter the Outcome!

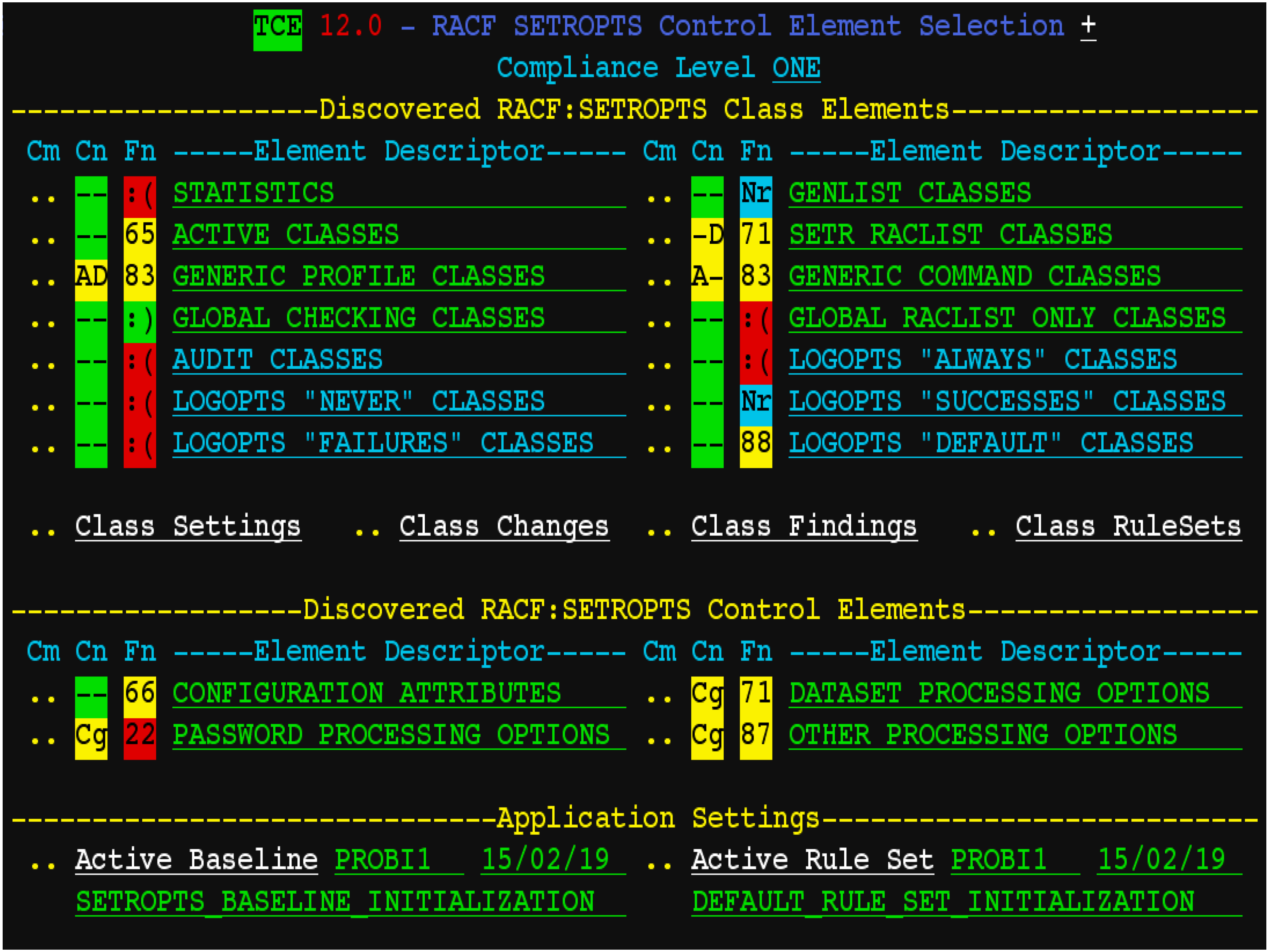
You decide what rules to apply

You Alter the Outcome!

Inspection Findings

- Foreground
- Background
- Health Checks

Point-of-Change Documentation Requirement added to collect detail from the Change Maker!



```
               TCE 12.0 - RACF SETROPTS Control Element Selection +
                              Compliance Level ONE
-------------------Discovered RACF:SETROPTS Class Elements--------------------
 Cm Cn Fn -----Element Descriptor----- Cm Cn Fn -----Element Descriptor-----
 .. -- :( STATISTICS                   .. -- Nr GENLIST CLASSES
 .. -- 65 ACTIVE CLASSES               .. -D 71 SETR RACLIST CLASSES
 .. AD 83 GENERIC PROFILE CLASSES      .. A- 83 GENERIC COMMAND CLASSES
 .. -- :) GLOBAL CHECKING CLASSES      .. -- :( GLOBAL RACLIST ONLY CLASSES
 .. -- :( AUDIT CLASSES                .. -- :( LOGOPTS "ALWAYS" CLASSES
 .. -- :( LOGOPTS "NEVER" CLASSES      .. -- Nr LOGOPTS "SUCCESSES" CLASSES
 .. -- :( LOGOPTS "FAILURES" CLASSES   .. -- 88 LOGOPTS "DEFAULT" CLASSES

 .. Class Settings   .. Class Changes  .. Class Findings   .. Class RuleSets

------------------Discovered RACF:SETROPTS Control Elements-------------------
 Cm Cn Fn -----Element Descriptor----- Cm Cn Fn -----Element Descriptor-----
 .. -- 66 CONFIGURATION ATTRIBUTES     .. Cg 71 DATASET PROCESSING OPTIONS
 .. Cg 22 PASSWORD PROCESSING OPTIONS  .. Cg 87 OTHER PROCESSING OPTIONS

------------------------------Application Settings----------------------------
 .. Active Baseline PROBI1   15/02/19  .. Active Rule Set PROBI1   15/02/19
    SETROPTS_BASELINE_INITIALIZATION      DEFAULT_RULE_SET_INITIALIZATION
```

Recent ICE Security/Control Enhancements

OPER/RACF/SETROPTS may be applied in different ways

✓ *As a SETROPTS Configuration Monitor*

- *As a Health Check Inspecting against your Compliance Rule Sets*
- *As a TCE/Detector Monitoring and Reporting Change Events.*

✓ *As a SETROPTS Control Enhancement*

- *Limit access to the SETROPTS Command Set Via TSO Command.*
- *Limit User access to SETROPTS Via EMCS and/or SDSF.*
- *Permit access to the ICE Command Subsystem.*

✓ *As a SETROPTS Communications Tool*

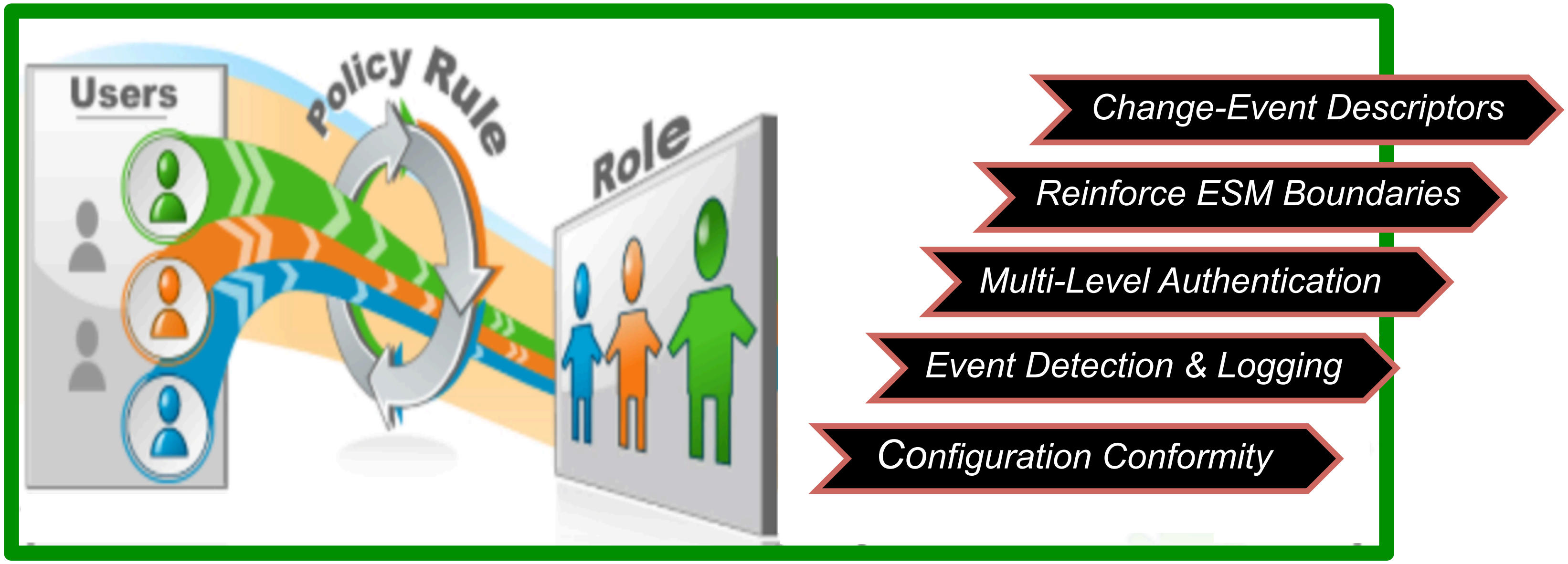
- *Use it to educate the next Generation of RACF Administrators.*
- *Use it to present the state of RACF Control Settings to Auditors.*
- *Use it to build organizational consensus for each RACF Setting.*

Recent ICE Security/Control Enhancements

ESM can no longer do it alone! More needs to be done!

External Security Manager (ESM)

Role Based Access Controls



Change-Event Descriptors

Reinforce ESM Boundaries

Multi-Level Authentication

Event Detection & Logging

Configuration Conformity

Perimeter Configuration Boundary

Configuration - Micro Boundary

System z Configuration Security-Control Continuum

Recent z/OS Security Enhancements

Thank you. Your evaluation please!

Defending System z - Session 16986

The Image Controls Environment (ICE) an Update

Tuesday, March 3, 2015: 4:30 PM - 5:30PM
Sheraton Seattle, Aspen

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