Daily DR Exercise

Mike Shorkend

Shorkend Associates

IBM
Champion
2025

IBM

Awarded through the program

IBM Champion

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

HiperSockets
SafeGuard
IBM*
IBM logo*
IMS
DB2
DS8890/DS8880
CICS
Z14,z15,z16,x17
z/OS*
z/VM*
zSeries*
Metro Mirror
Global Mirror
XRC

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Control-M and Control-O are trademarks of BMC
ZDP™,SRDF,VMAX and TimeFInder are trademarks of EMC
Hitachi Mainframe Cyber Resiliency, VSP, TrueCopyand HUR are trademarks of Hitachi

* All other products may be trademarks or registered trademarks of their respective companies.

About me

- *Independent Consultant*

- *35+ years of Mainframe Infrastructure Experience*

- *Experience includes z/OS system programming,capacity planning and control, performance tuning, software pricing, architecture, BCP/DRP, software development and support, management and training.*

- *Customers include financial institutes, government agencies, VARs, ISVs and training companies*

DR Test everyday?

- Why?

- How?

- What do you need?

- A case study

- REXX and BCPii

DR Test everyday?

Why?

Old Threats

WINSTON-SALEM JOURNAL

Truist agrees to confidential settlement over major system outage lawsuit

UK Parliament

Committees

UK Parliament > Business > Committees > Treasury Committee > News Article

More than one month's worth of IT failures at major banks and building societies in the last two years

6 March 2025

Top Turkish Bank Suffers System Outage, Sees No Cyber Attack

People posted more than 57,000 times about the issue on Twitter, with many ridiculing the bank's technical capabilities.

Bloomberg | Jul 08, 2021

Asli Kandemir (Bloomberg) -- Akbank TAS, Turkey's second-largest lender by market value, said it will gradually restore operations after suffering widespread system outages since early Tuesday, which prompted it to accept a delay in payments owed by customers.

Loan and credit card payments can be made a day later without accruing any interest because an issue in the bank's mainframe computer was affecting all customer services, Akbank said in an emailed statement on Wednesd: outages were the result of a cyber attack and said clients' data haven't

RealClear Defense

# Ransomware and the IBM Z/OS Mainframe, Big Iron

Paul F. Renda **CYBER December 21, 2021**

Ten years ago, I would have said that it's impossible for a mainframe to become infected with ransomware. Today, I no longer feel so confident, having read a number of articles about methodologies for how such an infection could take place.

New Threats

Ransomware on the Mainframe
—
Checkmate!

YOUR
EDUCATION · NETWORK · INFLUENCE
SHARE
Orlando 2024
Celebrating 60 years of the mainframe

Mark Wilson
Technical Director
Vertali
markwilson@Vertali.com

GSUK In-person Conference25
= Do more at the Core. Built to Learn, Engineered to Lead.
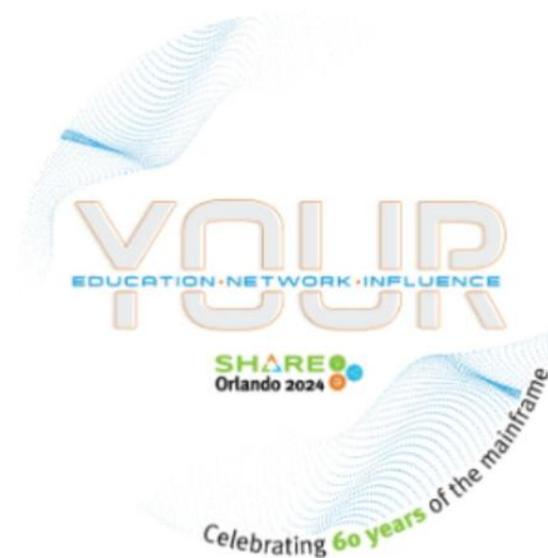
Not GDPS related, but still a great slide for our topic

GDPS with Logical Corruption Protection

1. GDPS now includes Logical Corruption Protection support to protect against cyber attacks and more.
2. A licensed offering that can be deployed in a range of different GDPS solutions.
   - LCP-Manager(MM) and LCP-Manager(GM)
3. Provides the ability to secure Point-In-Time captures of critical data using either FlashCopy or Safeguarded Copy.
4. These Point-In-Time captures can be used for a variety of purposes

Catastrophic
Recover the entire environment back to the point in time of the copy as this is the only recovery option

Forensic
Recover the copy and use the copy to investigate the problem and determine what final recovery action is required.

Surgical
Extract data from the copy and logically restore back to the production environment

Validation
Regular analytics on the copy to provide early detection of a problem or reassurance that the copy is a good copy prior to a further action

Offline Backup
Backup the copy of the environment to offline media to provide a second layer of protection

With thanks to Terry O'Connor

What are our goals

- Protect against logical corruption – e.g. human error, ransomware

- Protect against human error in configuration files (aka PARMLIB)

- Test DR Hardware on a regular basis

- Provide a mirror of a production environment

  - For forensics

  - For testing new software releases
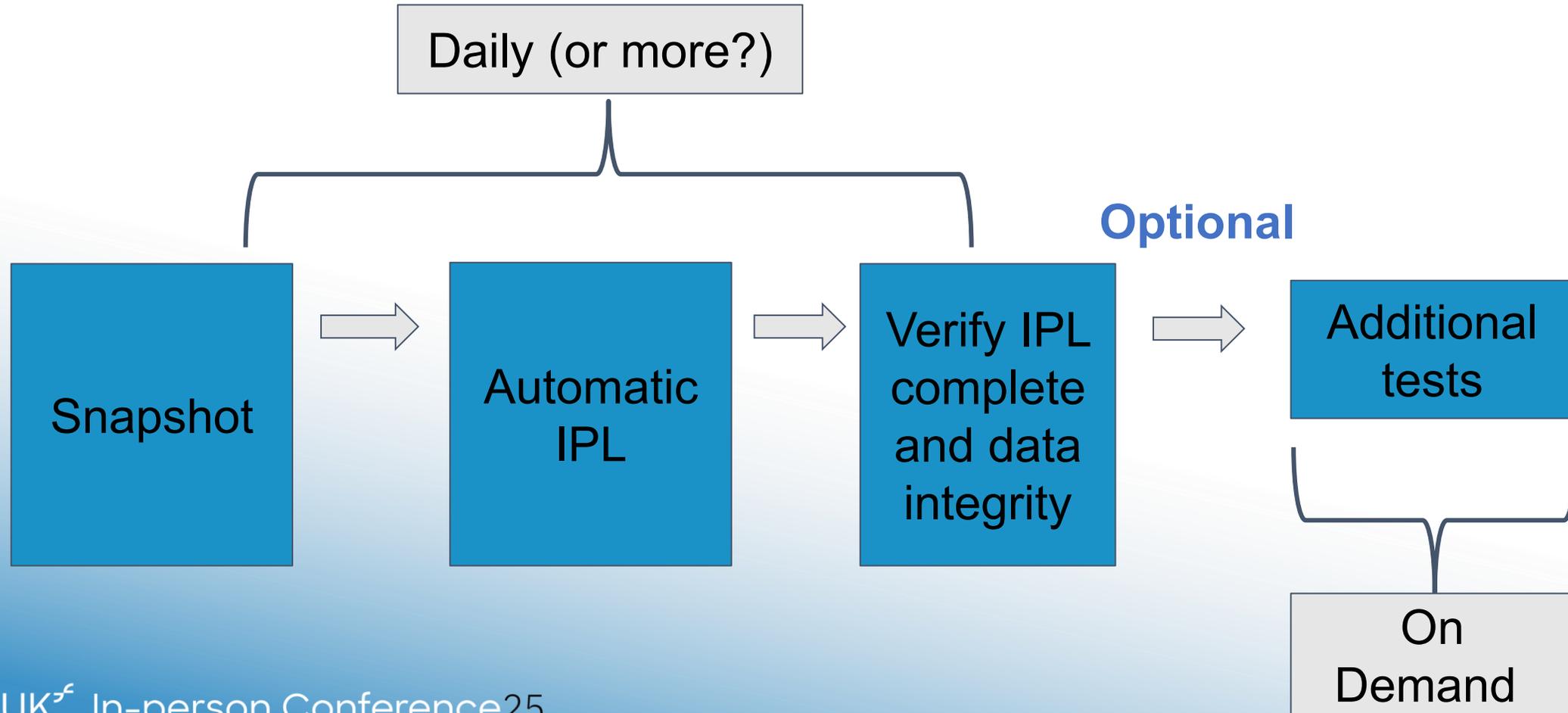
  - For testing new features

  - For training

DR Test everyday?

How?

GSUK In-person Conference25

= Do more at the Core. Built to Learn, Engineered to Lead.

The Big Picture

Daily (or more?)

Optional

Snapshot → Automatic IPL → Verify IPL complete and data integrity → Additional tests

On Demand

= Do more at the Core. Built to Learn, Engineered to Lead.

The solution and its benefits (1/2)

Daily (or more frequent) Test

- o Automate the process of taking a copy of the production DASD and then IPL the system from a separate LPAR(ideally using the DR hardware)

- o Verify that the IPL completes successfully

- o Improves MTTR – picks up IPL time errors

- o If performed on DR hardware - a daily test that the hardware works.

- o Daily test that the DASD replication is valid

The solution and its benefits (2/2)

o On Demand IPL

o A real production environment to test

- A new SYSRES

- Software upgrade (DB2, CICS….)

- Major changes

- When last did you cold start JES?

- Train junior staff

o Forensics

o Surgical extraction

A Sample Topology(others are possible)

PROD LPAR

Primary Site

Secondary Site

DR LPAR ✔

IPL

Primary DASD

Replication

Secondary DASD
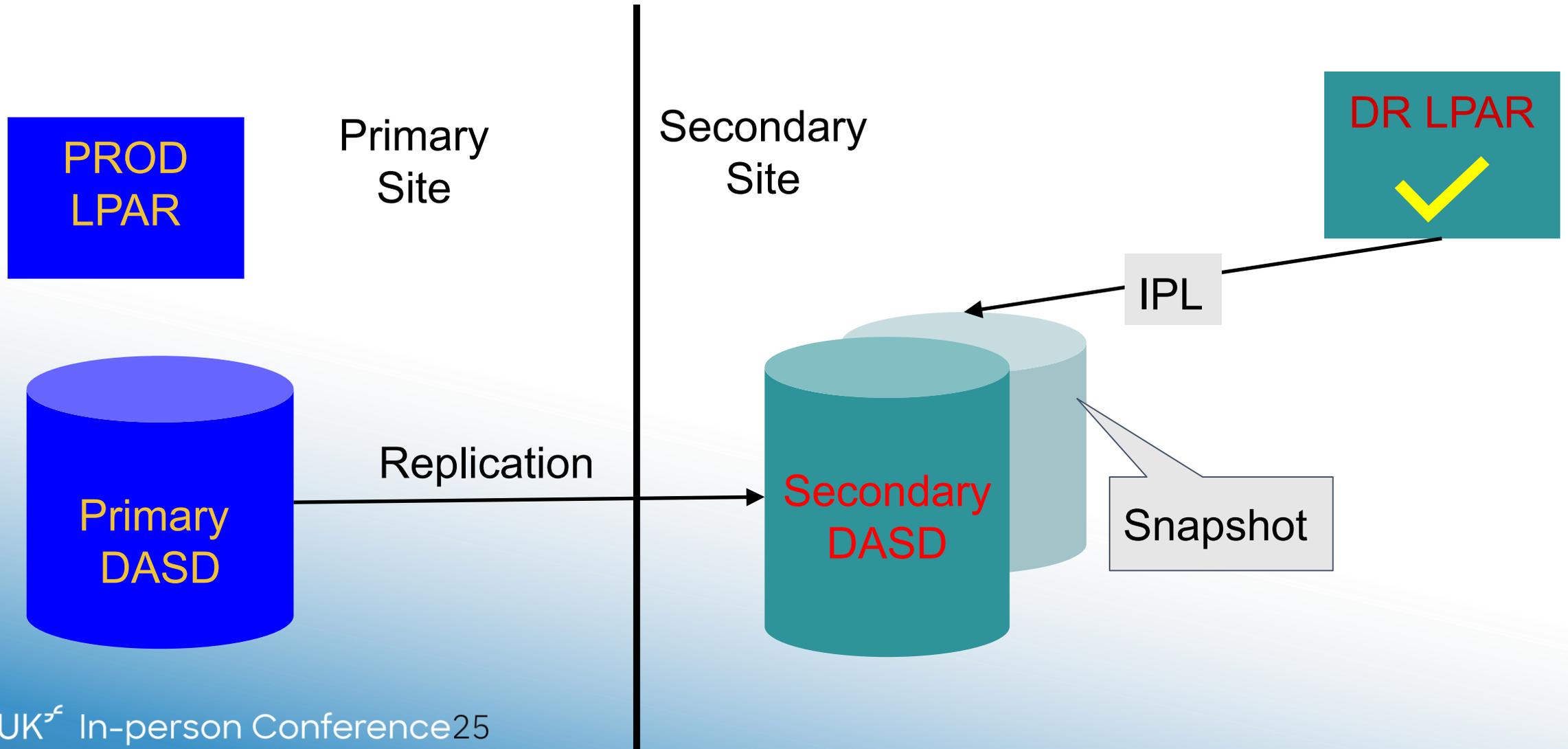
Snapshot

Snapshot

- Choose a time with minimal I/O

  - Time related

  - Business related

  - Not for SafeGuard copies

- Trigger your Storage Technology to create a consistent copy of your DASD(This might freeze I/O momentarily)

- The copy can be on the local controller or at a remote site

- With SafeGuard like solutions, you can take frequent copies

Automatic IPL

- Use your automation software to make your IPL completely automatic

- Load the target system with BCPii

- Use LOADxx logic to avoid errors and supply correct IPL parameters

- Use system symbols wherever possible

- Keep the differences between your real IPL and your test IPL to the absolute

  minimum

LOADxx

CONFIGID = PROD

CECPRIM

SYSA

1xxx

CONFIGID = DAILY1

CECSEC

DAILY1

Axxx

```
*-------------------------------------------------------
*           COMMON
*-------------------------------------------------------
NUCLEUS   1
NUCLST    00
SYSPARM   00
SYSPLEX   PLEX1
PARMLIB   SYS2.PARMLIB                                    SYS001
SYSCAT    CAT001143CCATALOG.MASTER.SYSA
*-------------------------------------------------------
*           SPECIFIC TO PRIMARY CEC
*-------------------------------------------------------
HWNAME    CECPRIM
IODF      ** IODF              PROD      0A
*                      SPECIFIC TO LPAR SYSA
LPARNAME SYSA
IEASYM    (00,0A,L)
*-------------------------------------------------------
*           SPECIFIC TO SECONDARY CEC
*-------------------------------------------------------
HWNAME    CECSEC
*                      SPECIFIC TO LPAR DAILY1
LPARNAME DAILY1
IODF      ** IODF              DAILY1    0A
IEASYM    (00,0A,D1,L)
```

= Do more at the Core. Built to Learn, Engineered to Lead.

Symbols

- IP Addresses

  HOME 172.16.7.&HOMEIP ETH1

- CTCs

- PARMLIB members like DEVSUPxx

- Coupling links

  PATHIN DEVICE(&PATHIN0,&PATHIN1)

- Software versions

  Use SYMBOLIC RELATE alias entries.

  &DB2VER = V12R1M6

  SYS2.SDSNLOAD points to SYS2.&DB2VER..SDSNLOAD

Some considerations

- In a SYSPLEX, if possible, bring up the SYSPLEX.
    - If you lack the hardware, zVM can be used

- DB2 maintenance mode might be required for members in a DB2 data sharing environment, for LPARs you do not IPL (for inflight transactions).

- IMS Data sharing ? VSAM RLS?

Some Gotchas

- You need to be really careful about leaks(the DR copy sending MQ messages, for example)

  - Consider using IPSEC or firewalls

- Writing to production "Tapes"

  - Use different DEVSUP members

  - Use security product

DR Test everyday?

What do you need?

DASD Snapshot (1/2)

- Use your DASD technology to create a snapshot

  - You will need extra DASD capacity and technology

  - First choice is a resilient copy(that cannot be overwritten)

    - SafeGuard Copy(IBM)

    - Hitachi Mainframe Cyber Resiliency

    - DELL/EMC ZDP™

DASD Snapshot (2/2)

- Second choice is one of the more traditional copy services

    - Local copy using FlashCopy(IBM), Shadow Image(Hitachi) or TimeFinder (EMC)

    - Remote copy (Metro Mirror, Global Mirror ,True Copy, XRC, HUR, SRDF etc.)

- Find a way to communicate with the replication driver. DS8K has DSCLI, Hitachi has BCM, VMAX has a batch interface.

- Automate this process using a job scheduler

BCPii

Programmatically issue HMC commands from a z/OS

Program in either Assembler, C ,REXX or RESTapi

Overview - What is BCPii?

Authorized z/OS application

- Monitor status or capacity changes
- Obtain configuration data related to CPC or image
- Re-ipl an image
- Change temp. capacity
- Query and update LPAR settings
- Set activation profiles
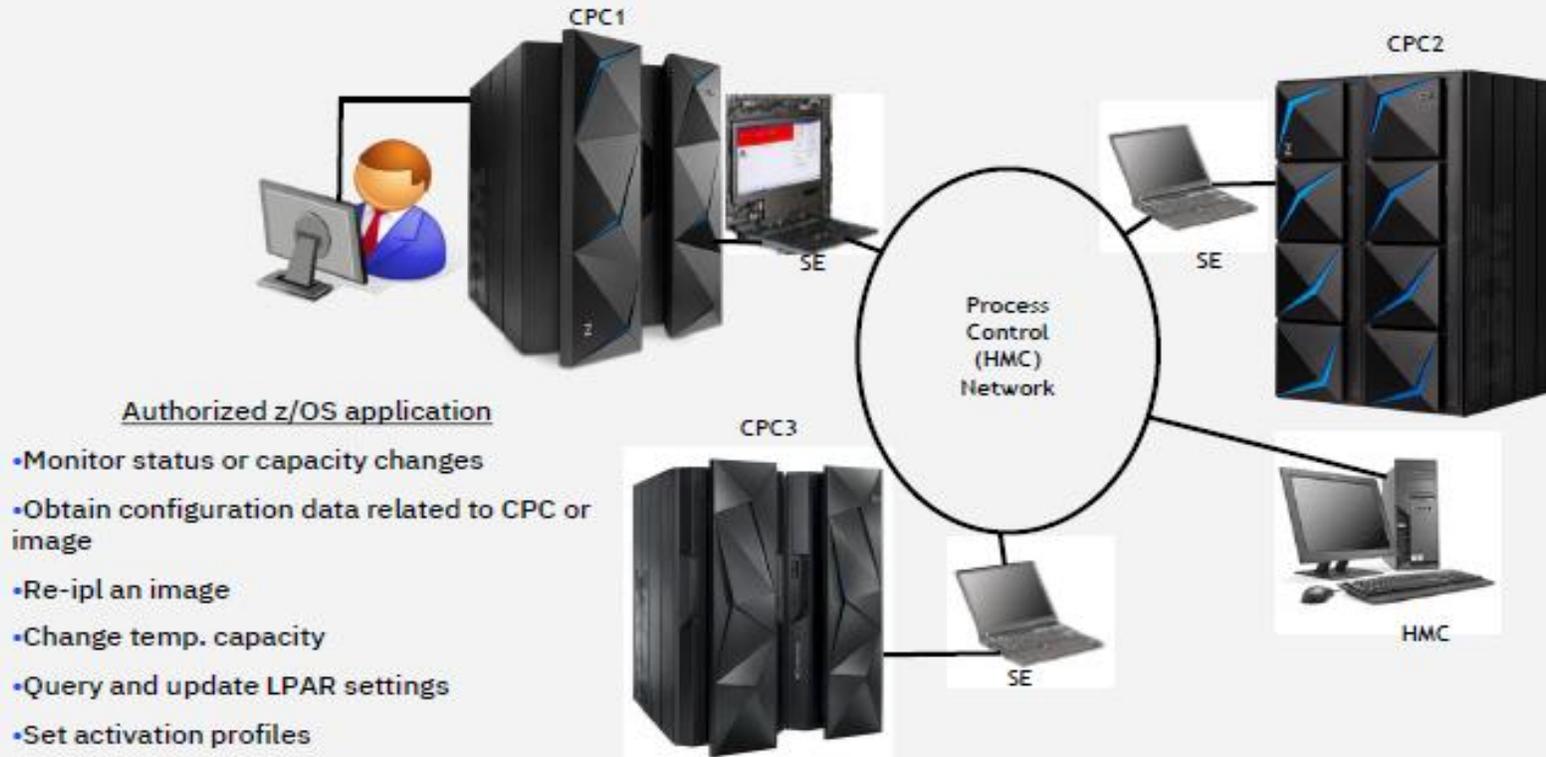
Automation and Scheduling Software

1. Schedule the time that the snapshot is taken

2. Perform IPL via a BCPii job after (1) has happened

3. Completely Automated IPL after (2) has completed

4. Verify that the copy is good. Could be done by running a transaction or job

5. Notify the right people in case of problems

Project Management

- Management Buy-in

- Budget

- Sysprogs

- Storage team and vendor

- Operations

- Production Support

- Networking

- Security

- Project Manager

DR Test everyday?

Case Study

Hardware Infrastructure

Primary Site

Z16-A02
4-way
Sysplex

IBM DS8910F

Secondary Site

Z15-T02
DR

IBM DS8910F

MM

GM

Tertiary Site

IBM DS8910F
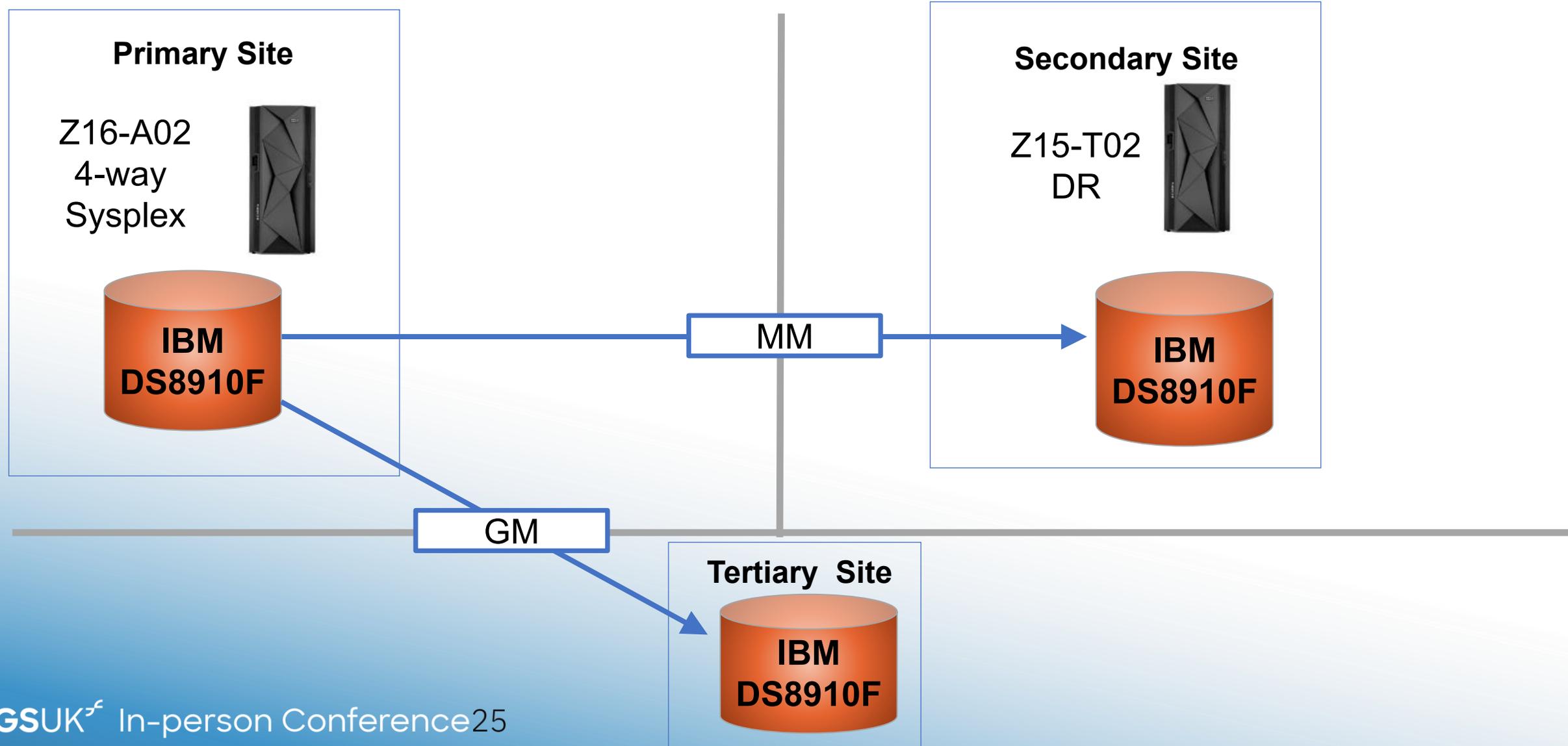
Software Infrastructure

- z/OS 2.5

- Two-way Db2 13 data sharing

- CICS TS 5.6

- BMC CONTROL-M(z/OS and Distributed) and CONTROL-O

- Spectrum Control

The Big Picture

Production z/OS
End of Day Processing
→ CTM →
DS8910F
DSCLI creates a new flash
→ CTM →
Production z/OS
BCPii loads z/OS at DR
→ BCPii / CTO →
DR z/OS
IPL + verification
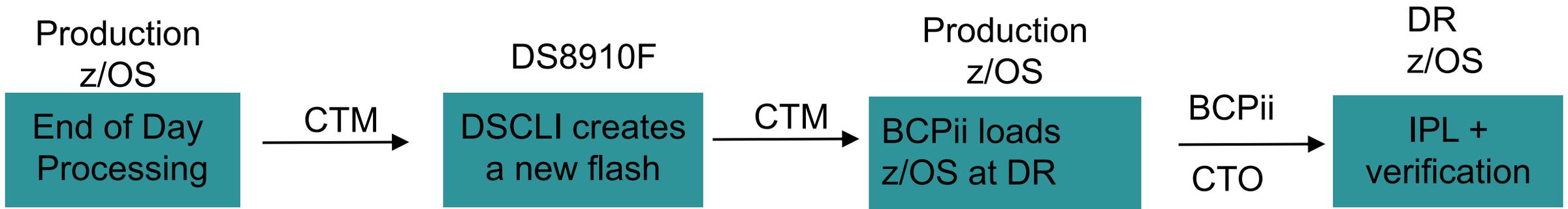
- When the job(on z/OS) indicating end of day processing has finished, a condition is raised by Control-M.

- This condition causes a DSCLI script to be run on the Spectrum control server that creates the flash copy.

- When the script ends, Control-M raises a condition that causes a job on z/OS to run that activates the coupling facility and the z/OS image at the DR site.

- Another job monitors the IPL console traffic

Automated load using BCPii

- Submit job that activates the coupling facility

- Submit job that listens on console traffic (of the IPLing image)

- Submit job that activates the z/OS image (load on activation set)

- Respond to WTORs using the listener job using CONTROL/O

- ControlO/Cosmos takes over the IPL process when it can

- When the system is up, run a CICS transaction (using the MODIFY command) to verify data integrity

- Daily alternate between 2nd and 3rd sites

Activate Coupling Facility
(from a job on the production system)

```
03.52.38 J0709797   BCPIIXEQ Connect
03.52.38 J0709797   BCPIIACT Querying current Status
03.52.38 J0709797   BCPIIXEQ Driven
03.52.38 J0709797   BCPIIXEQ Main
03.52.38 J0709797   BCPIIXEQ Query
03.52.39 J0709797   BCPIIACT CPC status CECSEC..............CFSHADW..00000008.NOT_ACTIVATED
03.52.39 J0709797   BCPIIACT to ask for approval
03.52.39 J0709797   *09 LPAR Activation approval  -  Please reply Y or N
03.52.39 J0709797   R 9,Y
03.52.39 J0709797   BCPIIACT activating LPAR ...
03.52.39 J0709797   BCPIIXEQ Driven
03.52.39 J0709797   BCPIIXEQ Main
03.52.39 J0709797   BCPIIXEQ Command
03.52.40 J0709797   BCPIIACT Querying after activation
03.52.40 J0709797   BCPIIXEQ Driven
03.52.40 J0709797   BCPIIXEQ Main
03.52.40 J0709797   BCPIIXEQ Query
03.52.40 J0709797   BCPIIACT CPC status CECSEC..............CFSHADW..00000008 NOT_ACTIVATED
03.52.40 J0709797   BCPIIACT Waiting ...
03.52.41 J0709797   BCPIIXEQ Driven
03.52.41 J0709797   BCPIIXEQ Main
03.52.41 J0709797   BCPIIXEQ Query
03.52.42 J0709797   BCPIIACT CPC status CECSEC..............CFSHADW..00000008 NOT_ACTIVATED
03.52.42 J0709797   BCPIIACT Waiting ...
03.52.43 J0709797   BCPIIXEQ Driven
03.52.43 J0709797   BCPIIXEQ Main
03.52.43 J0709797   BCPIIXEQ Query
03.52.44 J0709797   BCPIIACT CPC status CECSEC..............CFSHADW..00000001 OPERATING
03.52.44 J0709797   BCPIIACT Disconnecting from target LPAR
03.52.44 J0709797   BCPIIXEQ Driven
03.52.44 J0709797   BCPIIXEQ Main
03.52.44 J0709797   BCPIIXEQ Disconnect
03.52.44 J0709797   BCPIIACT Disconnecting from target CPC
03.52.44 J0709797   BCPIIXEQ Driven
03.52.44 J0709797   BCPIIXEQ Main
03.52.44 J0709797   BCPIIXEQ Disconnect
03.52.44 J0709797   BCPIIACT Cleaning Up
03.52.44 J0709797   BCPIIXEQ Driven
```

IPL Job

```
03.52.50 J0709798 *10 LPAR Activation approval  -  Please reply Y or N
03.52.50 J0709798  R 10,Y
03.52.50 J0709798  BCPIIACT activating LPAR ...
03.52.50 J0709798  BCPIIXEQ Driven
03.52.50 J0709798  BCPIIXEQ Main
03.52.50 J0709798  BCPIIXEQ Command
03.52.51 J0709798  BCPIIACT Querying after activation
03.52.51 J0709798  BCPIIXEQ Driven
03.52.51 J0709798  BCPIIXEQ Main
03.52.51 J0709798  BCPIIXEQ Query
03.52.52 J0709798  BCPIIACT CPC status CECSEC           DAILY1  00000008 NOT_ACTIVATED
03.52.52 J0709798  BCPIIACT Waiting ...
03.52.53 J0709798  BCPIIXEQ Driven
03.52.53 J0709798  BCPIIXEQ Main
03.52.53 J0709798  BCPIIXEQ Query
03.52.53 J0709798  BCPIIACT CPC status CECSEC           DAILY1  00000008 NOT_ACTIVATED
03.52.53 J0709798  BCPIIACT Waiting ...
03.52.54 J0709798  BCPIIXEQ Driven
03.52.54 J0709798  BCPIIXEQ Main
03.52.54 J0709798  BCPIIXEQ Query
03.52.55 J0709798  BCPIIACT CPC status CECSEC           DAILY1  00000008 NOT_ACTIVATED
03.52.55 J0709798  BCPIIACT Waiting ...
03.52.56 J0709798  BCPIIXEQ Driven
03.52.56 J0709798  BCPIIXEQ Main
03.52.56 J0709798  BCPIIXEQ Query
03.52.57 J0709798  BCPIIACT CPC status CECSEC           DAILY1  00000008 NOT_ACTIVATED
03.52.57 J0709798  BCPIIACT Waiting ...
03.52.58 J0709798  BCPIIXEQ Driven
03.52.58 J0709798  BCPIIXEQ Main
03.52.58 J0709798  BCPIIXEQ Query
03.52.59 J0709798  BCPIIACT CPC status CECSEC           DAILY1  00000002 NOT_OPERATING
03.52.59 J0709798  BCPIIACT Disconnecting from target LPAR
03.52.59 J0709798  BCPIIXEQ Driven
03.52.59 J0709798  BCPIIXEQ Main
03.52.59 J0709798  BCPIIXEQ Disconnect
03.52.59 J0709798  BCPIIACT Disconnecting from target CPC
03.52.59 J0709798  BCPIIXEQ Driven
```

= Do more at the Core. Built to Learn, Engineered to Lead.

Listener Job

Automated load - Automation rule

Automated IPL - COSMOS

```
------------------------------- CONTROL-O COSMOS OBJECT STATUS  -------< D >---------(OC)
COMMAND ===>                                                   SCROLL===> CRSR
O OBJECT    CURRENT    DESIRED    CLASS      MODE      STATUS
  DBPIMSTR  UP         UP         DB2MSTR    FREE      STEADY UP
  DBPIDBM1  UP         UP         DEPDB2     FREE      STEADY UP
  DBPIDIST  UP         UP         DEPDB2     FREE      STEADY UP
  DBPIIRLM  UP         UP         DEPDB2     FREE      STEADY UP
  IMSPDBC   UP         UP         IMSMSTR    FREE      STEADY UP
  IMSPDBRC  UP         UP         DEPIMS     FREE      STEADY UP
  IMSPDSAS  UP         UP         DEPIMS     FREE      STEADY UP
  PSYCICSI  UP         UP         CICS       FREE      STEADY UP
  CICSPIN1  UP         UP         CICS       FREE      STEADY UP
  CICSPIV1  UP         UP         CICS       FREE      STEADY UP
  PSYCICSE  UP         UP         CICS       FREE      STEADY UP
_ CICSPTR1  DOWN       UP         CICS       FREE      CD=DU PR=CICSPIS1
  CICSPIS1  DOWN       DOWN       CICS       FREE      STEADY DOWN
```
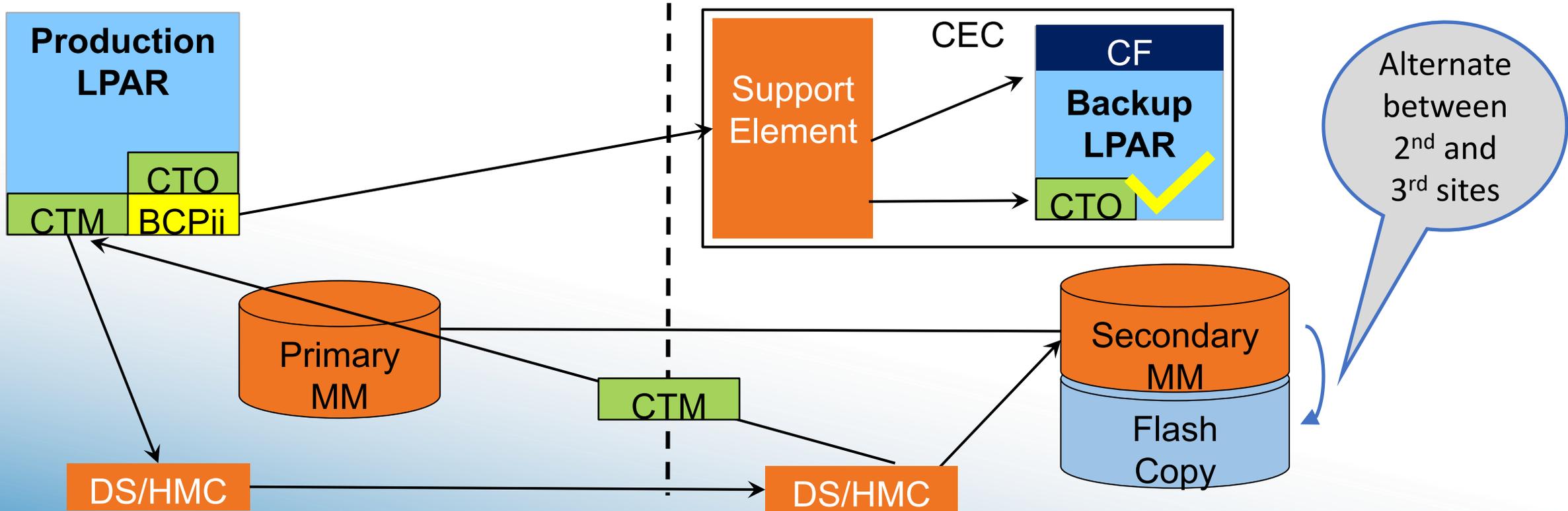
Who uses it?

- System programmers

- Storage administrators

- DBAs

- CICS and communications specialists

- Security administrators

- Operators

- Application programmers

Recap

DR Test everyday?

REXX and BCPii

GSUK In-person Conference25

≈ Do more at the Core. Built to Learn, Engineered to Lead.

System REXX

- Three types of REXX: SYSTEM,IVR,TSO. Each type supports a certain subset of BCPii commands(see manual)

- To make full advantage of BCPii REXX, System REXX should be used(TSO REXX does not support all BCPii commands)

- Grant read access to HWI.HWIREXX.rexxname in the FACILITY class

News Flash!
Many limitations lifted
With 2.5 CD

System REXX

- Dedicated Address Space called AXR

- PARMLIB(ATRxx) – controls AXR

  - REXXLIB ADD DSN(SYS3.PLX2.AXR.EXEC) – this is where your REXX execs reside

- START AXRPSTRT – starts system REXX stared task AXR

- Running system REXX

  - Via a command: F AXR,rexxname

  - Via assembler macro AXREXX

Job to run BCPii REXX

SYS1.SAMPLIB(HWIXMRJL)

This is a sample JOB that uses a provided program that acts as an interface to AXREXX *(for BCPii only).*

```
//STEP1   EXEC PGM=HWIREXX,REGION=1M,
//   PARM=('NAME=BCP1',              <- the name of the REXX to run
//         'DSN=MIKE.BCP.OUTPUT',    <- PDS. A member with the
//*                                     same name as the rexx gets the
//*                                     output
//         'TSO=N',
//         'SYNC=Y',
//         'TIMELIM=Y',
//         'TIME=40')
//STEPLIB  DD  DSN=SYS1.LINKLIB,DISP=SHR
//SYSPRINT DD  SYSOUT=*
```

Return Codes from HWIXMRJL

- Return codes:

  - Some are documented within the JCL

  - AXREXX - Authorized Assembler Programming Vol 1.

    (see Reference slide).

  - BCPii – return codes for each function can be found in

    Callable Services for HLL (see Reference slide).

- [MVS Programming: Callable Services for High-Level Languages](#) – BCPii

- [MVS Programming: Authorized Assembler Services Reference, Volume 1](#) – AXREXX

Thank you!

Mike Shorkend

mike@shorkend.com

IBM Champion 2025

IBM

Awarded through the program

IBM Champion

Session feedback

- Submit your feedback using the Whova app or at the conference website - https://conferences.gse.org.uk/2025/feedback/HF

- Make sure you are signed into Whova

  app or MyGSE if using the website

- The session code is HF

GSUK In-person Conference25
= Do more at the Core. Built to Learn, Engineered to Lead.