reducing the risk of software outages

Bruce Henderson
Laurie Schoenbaum
Hewlett Packard

preliminary version

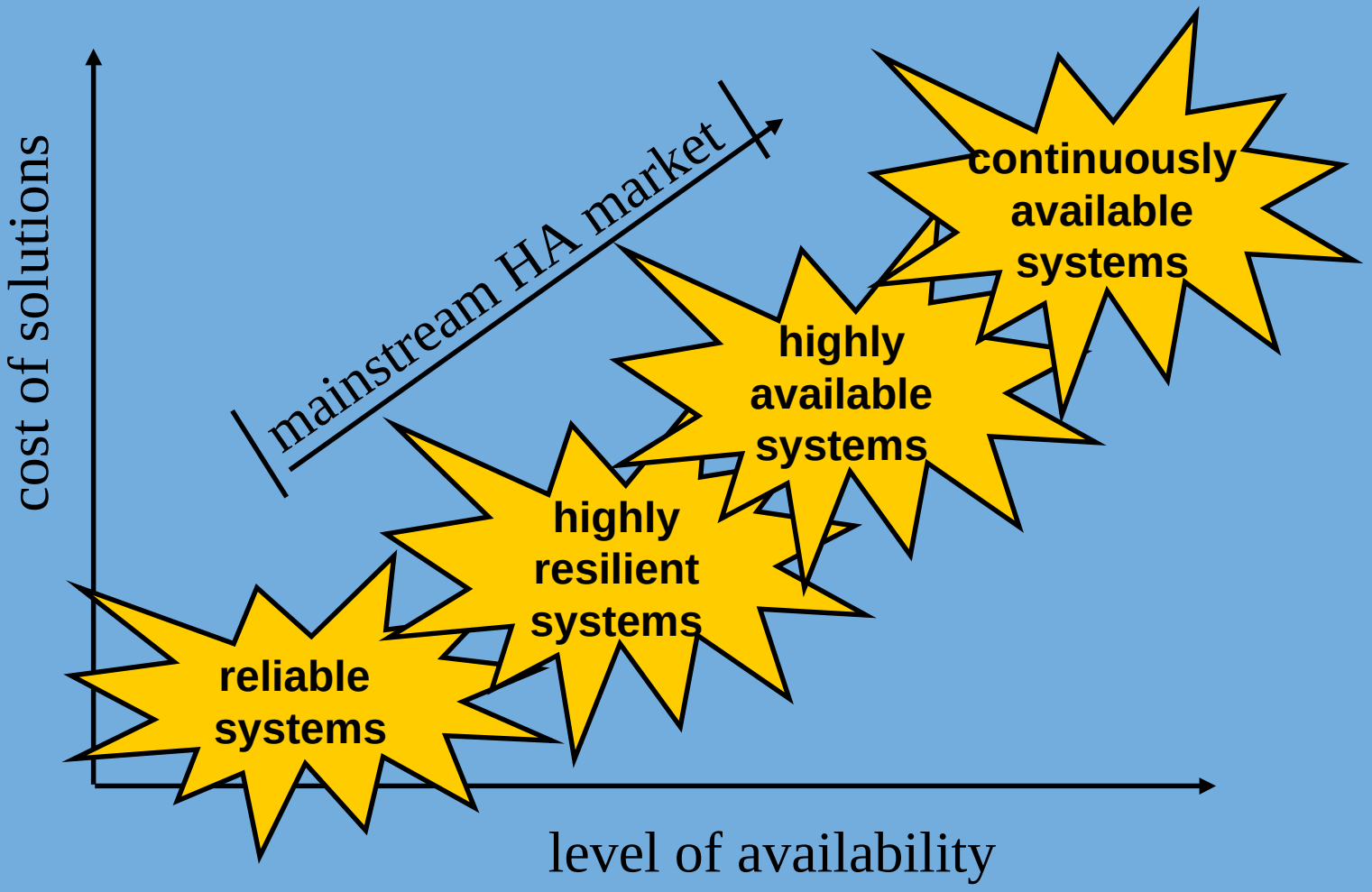
this is a preliminary version of the paper. the final version of “reducing the risk of software outages” can be found at the Interex Patch SIG web site:

`http://www.interex.org/advocacy/mcgs/index.html#sigs`

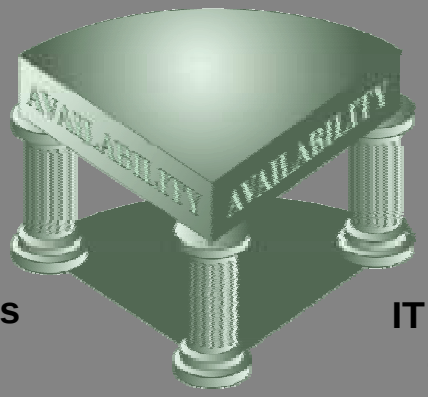
agenda

1. building a foundation
2. strategic importance of Use Models in attaining your HA goals.
3. strategies to handle unplanned outages.
4. strategies to handle planned outages.
5. applying changes to a running system.
6. appendix.

Availability continuum hierarchy



you should already have in place



hp's high availability strategy

requirements for HA solutions

data protection and disaster tolerance

- basic hardware reliability
- clusters

application restoration

- software quality
- ServiceGuard

system and Cluster monitoring

- EMS
- Clusterview
- Openview
- OnlineJFS

maintenance and support services

moving to HA

1. redundancy of components
2. use of hardware & software switching techniques
3. planning for scheduled downtime
4. eliminating human interaction with the system
5. defining automatic responses to error conditions and events
6. comprehensive acceptance test
7. defining and practicing disaster recovery processes

single points of failure

1. SPU
2. disks
3. interface cards, cables
4. networks
5. power

don’t forget about

staffing

1. hire the right people
2. provide training
3. get full buy-in to availability goals

processes

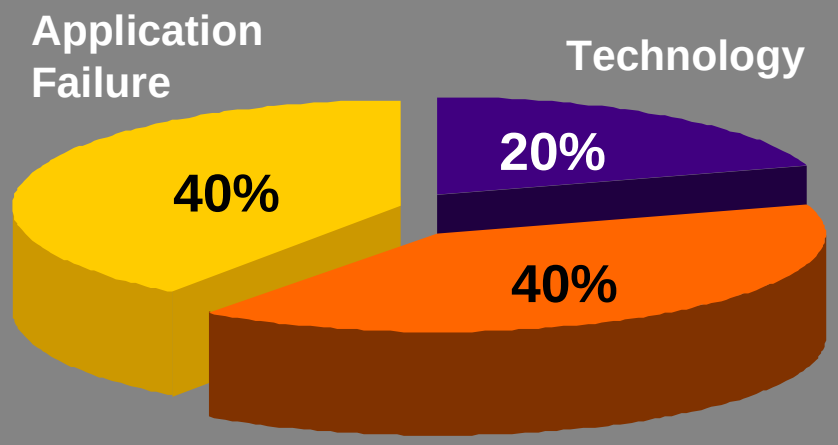
1. fully defined
2. documented
3. communicated
4. enforced
5. practiced/tested

attaining your HA goals

Change = Risk

what is your level of risk tolerance?

industry reports on causes of unplanned downtime



Source: GartnerGroup, October 1999

three levels of risk tolerance

Ex: Hardware or Software Development

- Most tolerant of downtime
- Need for latest features
- Downtime is an accepted cost of doing business

Ex: Bank Branch, Inventory Management

- High (but not life threatening) uptime requirement. Can switch to manual processing
- Only new features that increase uptime or are business critical

Ex: Telecomm, Patient Monitoring

- High uptime requirement
- Low requirement for new features
- Downtime = loss or risk of life, or business stops operation

patch levels provide

- minimized change
- leverage of maximum testing

making the tradeoff – hp patch levels

- In interest of assurance, patches undergo additional post release testing in hp in complex environments and application stacks
- In interest of timeliness, hp releases patches when they meet established hp quality standards
- Patches are assigned a progressive rating level--1, 2, or 3
- ITRC patch tools enable you to **make informed benefit/risk tradeoff** based on patch's rating

patch levels

Level	Meaning
	• Patch meets established HP quality standards • Patch fixes problem it purports to fix • No side-effects • Installs and de-installs in target environment
	• Patch sent to threshold number of customers • Patch is threshold number of days old • No problems reported
	• Tested under complex configurations • Tested with complex application stacks • Stress & Performance tested

use models provide

change control

- defined process
- standardized process
- documented process

contained change

- only appropriate changes made

protection against new problems

- well tested standard solution

unplanned outages

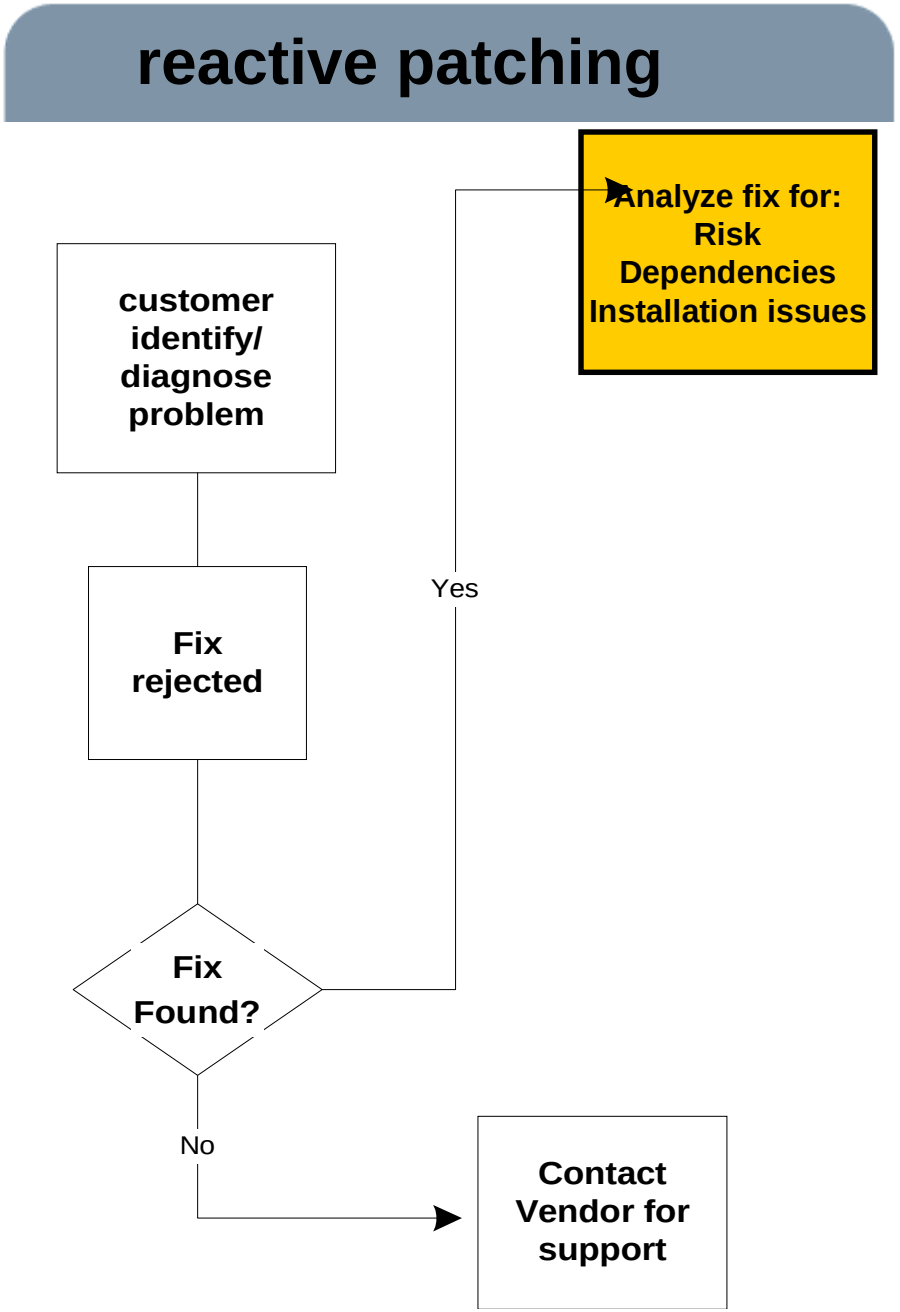
be prepared

- **get your system up and running fast**
- **get it right the first time**

reactive patching

Fix Found

ITRC Usage



reactive patching

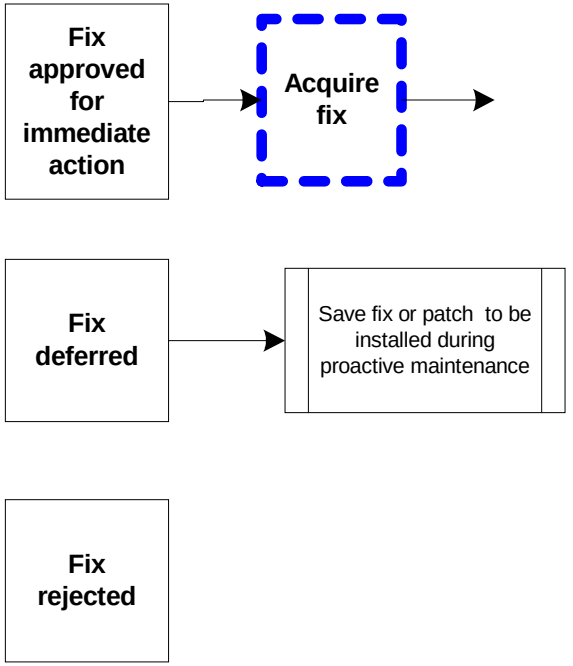
fix approved

fix deferred

fix rejected

reactive patching

-analyze fix for risk, dependencies, and installation issues



planned outages

update high ROI areas while minimizing downtime

updating your system to a new OS

Update

- Preserves non-OS data on root volume group
- Simplified deployment (reduced reboots)

Cold Install

•Will NOT preserve system data on root volume
•Fastest, consistent, most reliable solution
•Best model for distributed replicated sites
•Required for / & /stand size changes
•Only update patch for OS levels at the end of support life

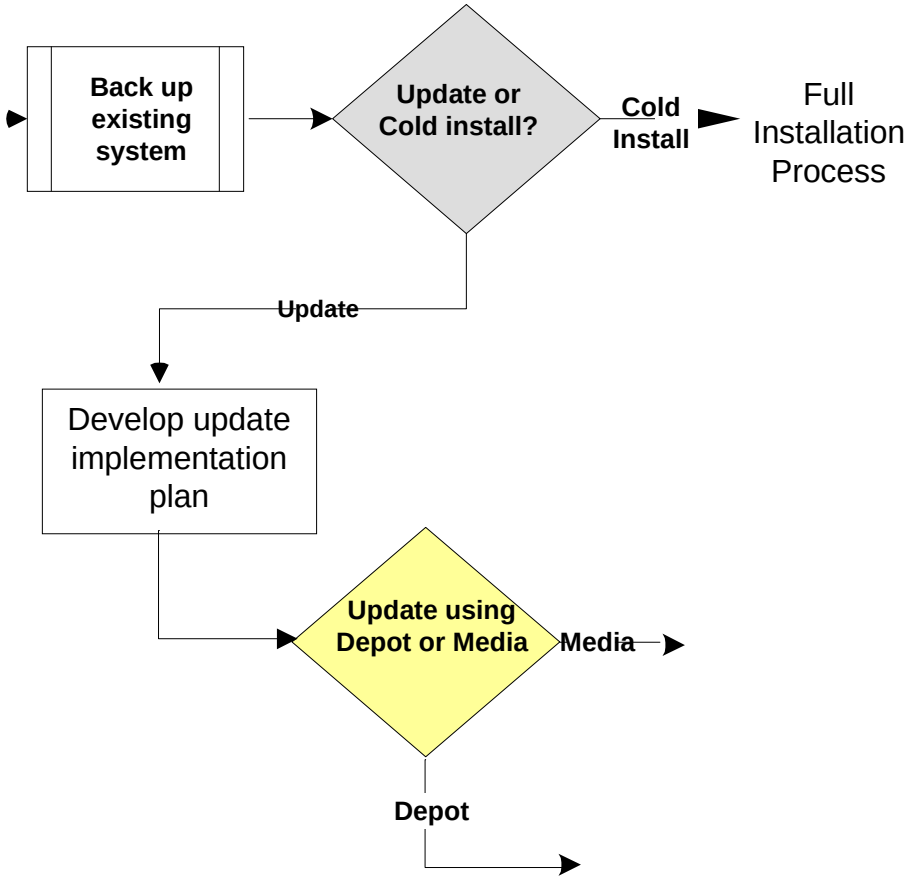
Depot

•Replicated systems
•Simultaneous multiple system deployment

Media

•Deploying to single, or few, systems
•No network connectivity available

Updating your system - step 1



updating your system to a new OS

Updating from a Master Depot

- Fast deployment for replicated systems
- Reduce number of reboots
- Install multiple systems simultaneously
- Provides backup, recovery, and deployment solution

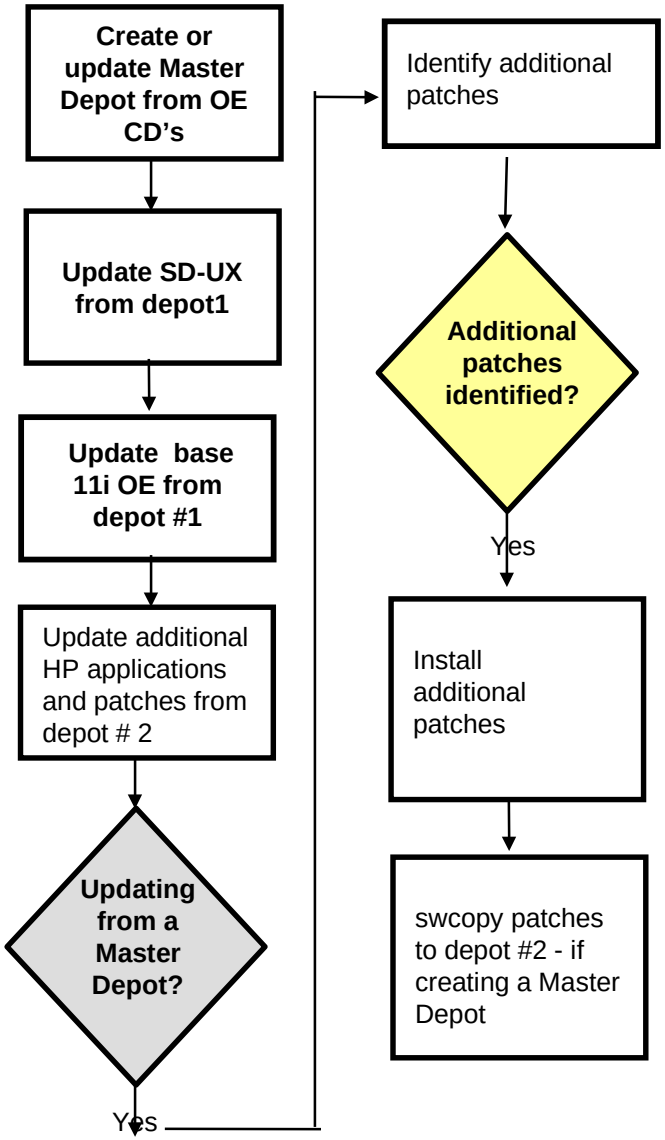
Updating from an Ignite Golden Image

- Fastest deployment method
- Provides backup, recovery, and deployment solution

Additional Patches

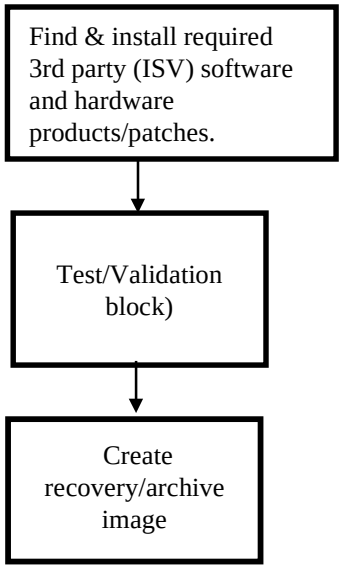
- Need to patch a non-OE applications?
- Need a 'newer' version of an existing patch?

Updating your system - from a master depot



updating your system to a new OS

Updating your system - complete 11i update



updating your system to a new OS

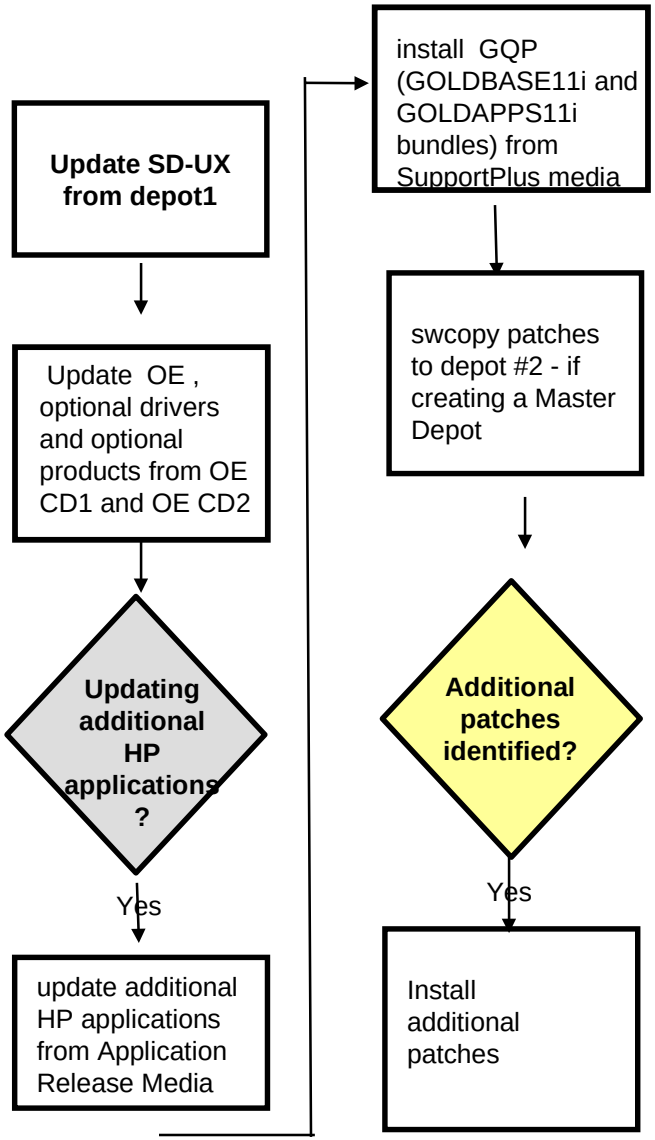
Updating additional HP applications

- Is a non-OE application required?
- Is a newer version of an OE application required?

Additional Patches

•Need to patch a non-OE applications?
•Need a ‘newer’ version of an existing patch?

Updating your system - from media



updating your system to a new OS

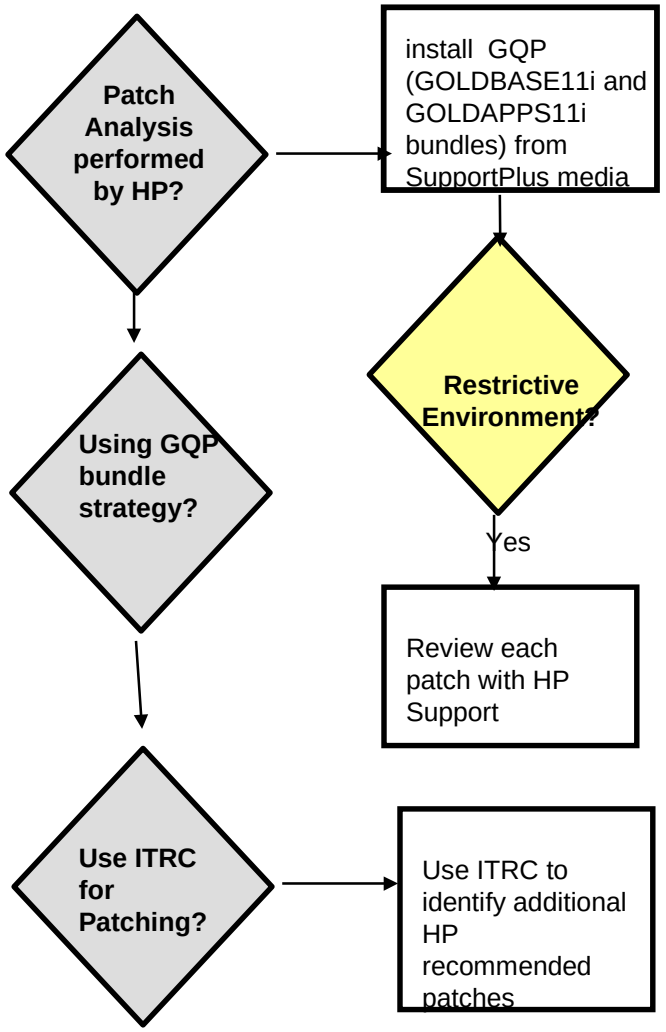
Patch Analysis performed by HP

- Start with the GQP strategy
- HP will value add specifics for your configuration

GQP Bundle Strategy

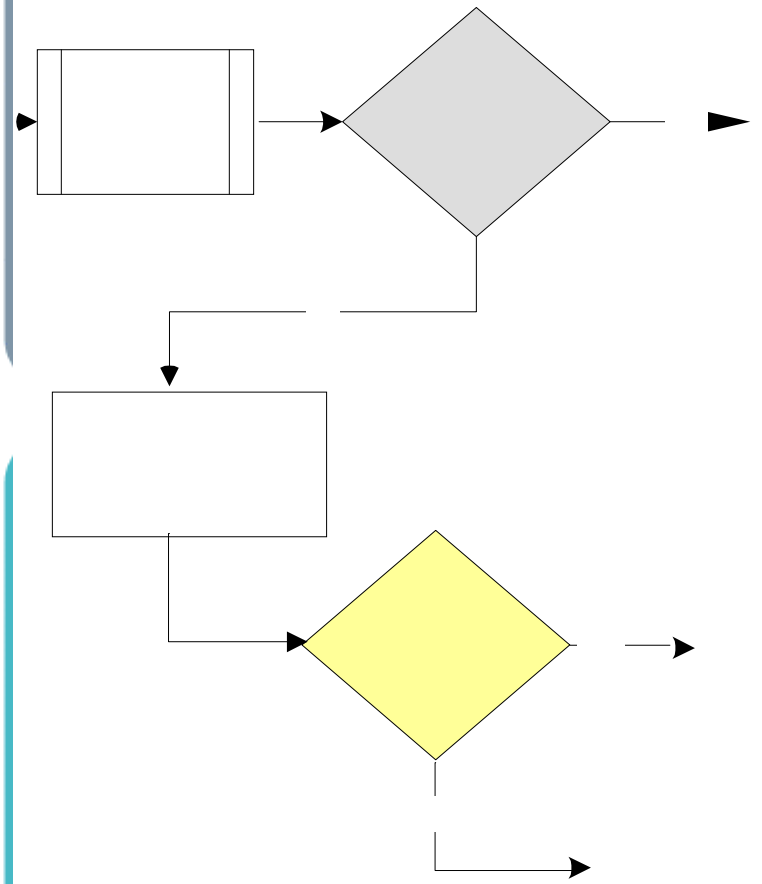
•Recommended base, as a minimum
•Recommended patching strategy supported by ISV's
•Additional patches may be needed for non-OE applications

Updating your system - Identify additional patches



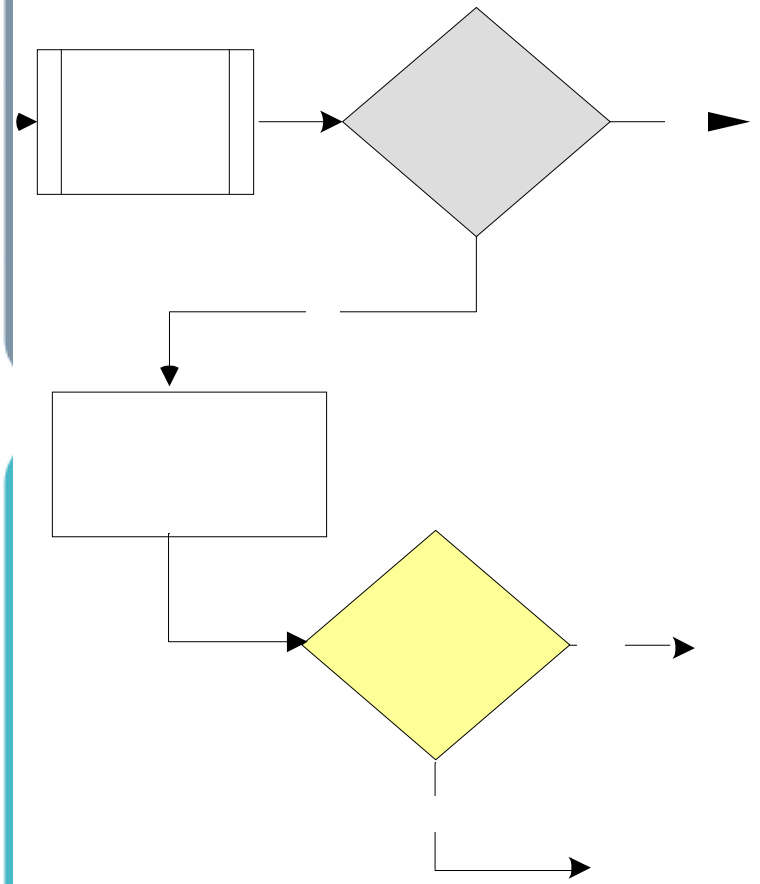
refreshing the current patches on your system OS

Refreshing the current patches on your system



adding a new HW peripheral to your system

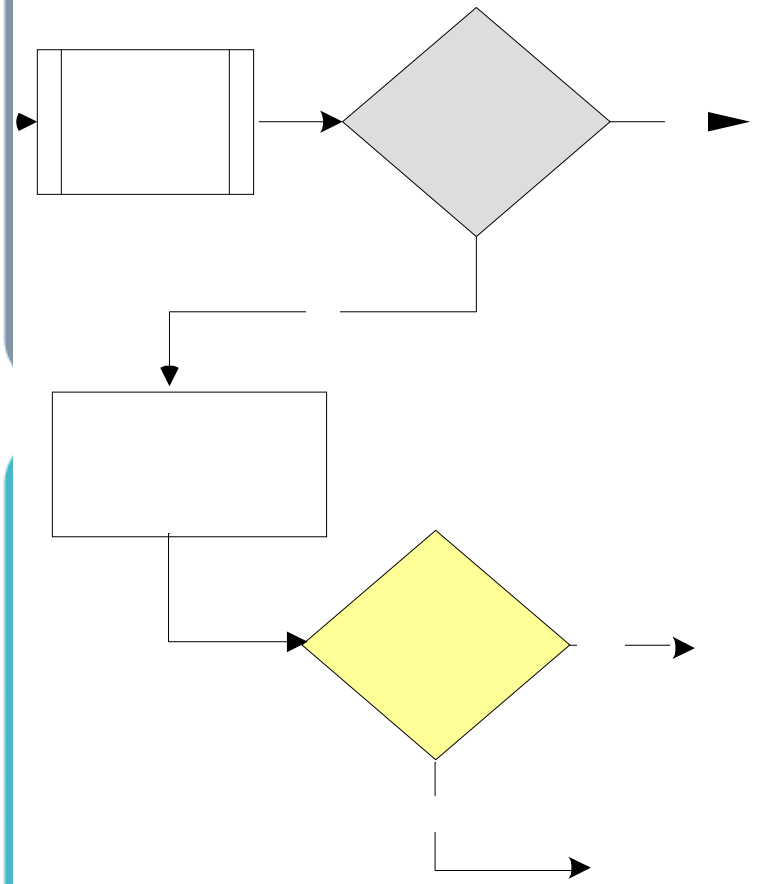
adding a new HW peripheral to your system



updating to a new version of 3rd party software

Update

Updating to a new version of 3rd party software

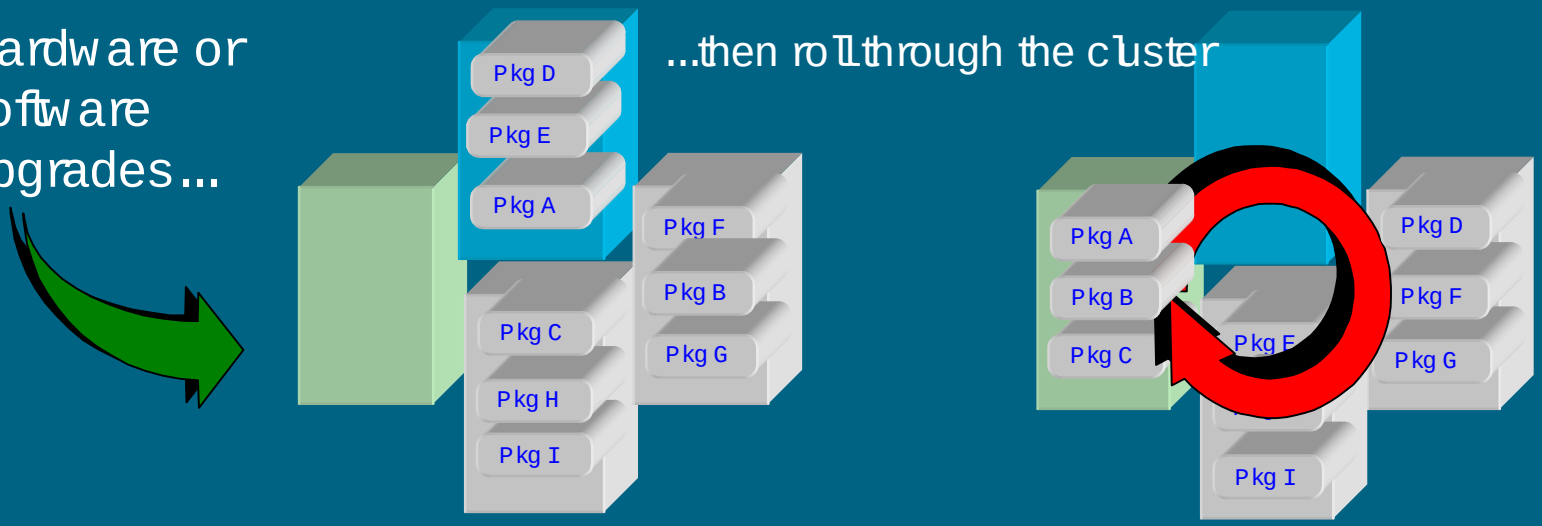


mc/serviceguard: rolling upgrade

- Rolling upgrade: minimize planned downtime
- Maximize application uptime
- Cluster remains up

Backward compatbility:
- Operating system
- MC/ServiceGuard

Hardware or software upgrades...



ARD - Alternate Root Disk

- “near” dynamic patching
  - system available throughout maintenance process – until actual reboot
  - timing of reboot controlled
  - unattended reboot
  - available much sooner than true dynamic system management
- initial features
  - cloning from active system
  - creation of bootable recovery image
  - cloning from Ignite Recovery image
  - modify new alternate image
  - command line interface
- initial requirements
  - disk capacity for duplicate root volume group
  - special release product

for more information…

See the Patch SIG page at:
http://www.interex.org/advocacy/mcgs/index.html#sigs

Appendix

use model decision helper
use model flow charts
use model glossary

Keep It Running
Targeted recommendations

	O/S, Products, Applications	Proactive Patching	Reactive Patching	Software Change Management	Test Environment
Restrictive	Stable release Available for 1+ years	▪ Use only thoroughly-tested patches with the highest level of field experience	▪ Make fewest changes possible to restore function ▪ Perform full diagnostic analysis before attempting a solution	▪ Formal plan with explicit roles & responsibilities ▪ Documented back-out plan for changes, if necessary ▪ Documented DRP that is updated & tested at least yearly	▪ Dedicated equipment ▪ Matches production environment ▪ Testing includes simulated loads
Conservative	Stable release Available for 6+ months	▪ Use only thoroughly-tested patches with substantial field experience	▪ Make fewest changes possible to restore function ▪ Perform full diagnostic analysis before attempting a solution	▪ Formal plan with explicit roles & responsibilities ▪ Documented back-out plan for changes, if necessary	▪ Dedicated equipment that matches production environment
Innovative	Stable release Available for 2+ months	▪ Patches should be carefully reviewed for risks and benefits	▪ Focus on restoration of function ▪ Limit number of concurrent changes	▪ Established roles & responsibilities	Test on development equipment or off-hours on production environment

hp's full-range disaster tolerant solutions