Reliability, Resiliency and Reparability enhancement in HP’s new zx2-based platforms

White paper

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>2</td>
</tr>
<tr>
<td>CPU subsystem</td>
<td>5</td>
</tr>
<tr>
<td>ECC and parity check with retry in all levels of cache</td>
<td>5</td>
</tr>
<tr>
<td>Intel Cache Safe Technology (Pellston cache self-healing)</td>
<td>6</td>
</tr>
<tr>
<td>Dynamic processor resiliency</td>
<td>6</td>
</tr>
<tr>
<td>Additional HP Integrity processing RAS features</td>
<td>6</td>
</tr>
<tr>
<td>Memory subsystem</td>
<td>6</td>
</tr>
<tr>
<td>Double-chip-spare</td>
<td>7</td>
</tr>
<tr>
<td>Advanced I/O error recovery</td>
<td>7</td>
</tr>
<tr>
<td>DDR2 DIMM enhancements</td>
<td>7</td>
</tr>
<tr>
<td>Page De-allocation</td>
<td>8</td>
</tr>
<tr>
<td>I/O Subsystem</td>
<td>8</td>
</tr>
<tr>
<td>Isolated I/O Paths</td>
<td>8</td>
</tr>
<tr>
<td>Advanced I/O error handling</td>
<td>8</td>
</tr>
<tr>
<td>PCI OL* (Online addition, replacement and deletion)</td>
<td>9</td>
</tr>
<tr>
<td>Chassis infrastructure</td>
<td>9</td>
</tr>
<tr>
<td>Power infrastructure</td>
<td>9</td>
</tr>
<tr>
<td>Cooling Infrastructure</td>
<td>10</td>
</tr>
<tr>
<td>Fault Management</td>
<td>10</td>
</tr>
<tr>
<td>Serviceability</td>
<td>11</td>
</tr>
<tr>
<td>Preventive hardware design</td>
<td>12</td>
</tr>
<tr>
<td>Tool-less design</td>
<td>12</td>
</tr>
<tr>
<td>Customer self-repair</td>
<td>12</td>
</tr>
<tr>
<td>Integrity iLO: The Management Processor</td>
<td>13</td>
</tr>
<tr>
<td>Troubleshooting, diagnosis, and preventative tools</td>
<td>13</td>
</tr>
<tr>
<td>For more information</td>
<td>17</td>
</tr>
</tbody>
</table>
Executive summary

HP’s next generation of entry level Integrity servers offer enterprise level performance with mission critical capabilities at a very competitive price point.

HP’s RAS capabilities on the next generation entry level servers are built upon the framework of the three R’s: reliability, resiliency, and reparability

- **Reliability**: the ability to avoid failures.
- **Recoverability**: the ability to seamlessly work around the failure as if it never happened.
- **Reparability**: the ability to fix a failure fast.

HP makes its servers as reliable as possible by using the highest quality components and qualification procedures. However, each component will have a statistically non-zero predicted failure rate. In addition, there will be some environmentally induced errors such as those caused by cosmic radiation. These errors cannot be completely stopped, even with the best of shielding. Thus, some errors are inevitable, and that is why resiliency and reparability are just as important as reliability.

This paper is dedicated to showing how HP’s next generation of Entry-Level Integrity servers set the standard when it comes to reliability, resiliency, and reparability. These days, nearly every industry available server has the typical baseline RAS (Reliability, Availability, and Serviceability) features such as: redundant, hot-swap power supplies, hard disk drives, and fans; and error correction coding (ECC) on data buses. HP’s innovation goes well beyond this baseline, drawing on over 20 years of research and development experience in this area. HP has been studying availability at customer datacenters and its impact on business, using this data for constructing robust and resilient servers that provide a strong foundation for continuous availability to the customer.

System topology

HP Integrity servers that use the zx1 and the new zx2 chipset are termed entry-level and Integrity blade systems. The entry-level Integrity systems, unlike the rest of the Integrity line, are non-cellular. Integrity entry level servers, in contrast to commodity servers from second-tier vendors, have enterprise level performance and availability designed in.

The new zx2 chipset consists of four VLSI component types: a memory & IO controller (MIO), a scalable memory expander (SME), and PCI-X & PCI-Express IO adapters (IOAs). Figures 1 and 2 are the architecture diagrams of the rx3600 and rx6600 systems respectively (the rx2660 and BL860c have similar architectures based on the zx2 chipset). Numerous RAS features are shown in the diagrams and will be discussed further in this paper.
Figure 1. rx3600 system topology

- 1-bit ECC and 2-bit error detection
- 1-bit ECC on all address/data paths
- Dynamic processor resiliency
- Cache self-healing and Advanced thermal management

- Dynamic memory resiliency
- All memory is parity protected with Advanced ECC
- Double chip spare

- 1+1 redundant hot swap supplies
- 3 pairs of redundant hot swap fans

- Address Parity, Data ECC
- • 1-bit ECC and 2-bit error detection
- • 1-bit ECC on all address/data paths
- • Dynamic processor resiliency
- • Cache self-healing and Advanced thermal management

- Multiple links for redundant, HA I/O
- Out of band management, firmware updates, remote power control, and remote console, Virtual KVM and virtual media

- 4 port (No RAID) or 8 port RAID SAS
- 8 internal hot-swap disks

- Unified Core I/O
- • 10/100/1000bT
- • vKVM & vMedia
- • USB x5
- • SATA/1000bT

- Power Supply
- • 1+1 redundant hot swap supplies

- Fan
- • 3 pairs of redundant hot swap fans
Figure 2. rx6600 system topology

- Address Parity, Data ECC
  - 1-bit ECC and 2-bit error detection L1 & L2 caches
  - 1-bit ECC on all address/data paths
  - Dynamic processor resiliency
  - Cache self-healing and Advanced thermal management

- Dynamic memory resiliency
- All memory is parity protected with Advanced ECC
- Double chip spare

- 1+1 redundant hot swap supplies

- 7 pairs of redundant hot swap fans

- Multiple links for redundant, HA I/O

- Out of band management, firmware updates, remote power control, and remote console, Virtual KVM and virtual media

- Unified Core I/O
  - 10/100/1000bT
  - SAS 133MHz
  - 16 internal SAS hot-swap disks

- 4 port (No RAID) or 8 port RAID SAS

- Power Supply
  - 1+1 redundant hot swap supplies

- Fan
  - 7 pairs of redundant hot swap fans

- Address Parity, Data ECC
  - 1-bit ECC and 2-bit error detection L1 & L2 caches
  - 1-bit ECC on all address/data paths
  - Dynamic processor resiliency
  - Cache self-healing and Advanced thermal management

- Dynamic memory resiliency
- All memory is parity protected with Advanced ECC
- Double chip spare

- 1+1 redundant hot swap supplies

- 7 pairs of redundant hot swap fans

- Multiple links for redundant, HA I/O

- Out of band management, firmware updates, remote power control, and remote console, Virtual KVM and virtual media

- Unified Core I/O
  - 10/100/1000bT
  - SAS 133MHz
  - 16 internal SAS hot-swap disks

- 4 port (No RAID) or 8 port RAID SAS

- Power Supply
  - 1+1 redundant hot swap supplies

- Fan
  - 7 pairs of redundant hot swap fans

- Address Parity, Data ECC
  - 1-bit ECC and 2-bit error detection L1 & L2 caches
  - 1-bit ECC on all address/data paths
  - Dynamic processor resiliency
  - Cache self-healing and Advanced thermal management

- Dynamic memory resiliency
- All memory is parity protected with Advanced ECC
- Double chip spare

- 1+1 redundant hot swap supplies

- 7 pairs of redundant hot swap fans

- Multiple links for redundant, HA I/O

- Out of band management, firmware updates, remote power control, and remote console, Virtual KVM and virtual media

- Unified Core I/O
  - 10/100/1000bT
  - SAS 133MHz
  - 16 internal SAS hot-swap disks

- 4 port (No RAID) or 8 port RAID SAS

- Power Supply
  - 1+1 redundant hot swap supplies

- Fan
  - 7 pairs of redundant hot swap fans

- Address Parity, Data ECC
  - 1-bit ECC and 2-bit error detection L1 & L2 caches
  - 1-bit ECC on all address/data paths
  - Dynamic processor resiliency
  - Cache self-healing and Advanced thermal management

- Dynamic memory resiliency
- All memory is parity protected with Advanced ECC
- Double chip spare

- 1+1 redundant hot swap supplies

- 7 pairs of redundant hot swap fans

- Multiple links for redundant, HA I/O

- Out of band management, firmware updates, remote power control, and remote console, Virtual KVM and virtual media

- Unified Core I/O
  - 10/100/1000bT
  - SAS 133MHz
  - 16 internal SAS hot-swap disks

- 4 port (No RAID) or 8 port RAID SAS
CPU subsystem

These new zx2-based HP Integrity entry-level servers support the new dual-core Intel® Itanium 2 processors (code-name “Montecito”) and provide a foundation for future Itanium 2 processors a.k.a. “Montvale”.

Intel® Itanium® 2 processors have a robust error correction scheme and a world-class Machine Check Architecture specifically designed to enable mainframe-class availability in enterprise environments. Itanium 2 processors, in combination with the advanced RAS capabilities of zx2 based systems, support a level of availability that is only available on high-end proprietary platforms. The reliability features built into the new dual-core Itanium 2 processors are highlighted in Figure 3.

Figure 3. RAS features of dual-core Itanium 2 processors (“Montecito”)

The robustness of the Itanium architecture was demonstrated in a series of tests at Los Alamos National Laboratory (LANL). Using LANL’s neutron beam, Integrity systems were subjected to a particle flux more than 20 million times more intense than would be experienced naturally at sea level. Extrapolating the results to typical datacenter conditions revealed an expected 500+ year mean-time-to-failure for Itanium processors. Furthermore, the Machine Check Architecture successfully contained all fatal errors, something that cannot be done in lower-end processors.

ECC and parity check with retry in all levels of cache

Due to large cache sizes, 95% to 99.99% (depending on the processor type) of all CPU errors will occur in the cache. With the introduction of dual-core Itanium 2 processors, all single-bit cache
errors, in all levels of the cache are automatically corrected. This is the highest level of protection in the industry.

Intel Cache Safe Technology (Pellston cache self-healing)

As cache sizes become larger, the likelihood of cache failures increases. The Itanium processor offsets this increased likelihood of failures using Intel Cache Safe Technology. When there is a correctable error in the L2 cache, Intel Cache Safe Technology tests the cache line and corrects the error with ECC or parity check and retry. If the cache-line is found to be defective, it is disabled. This prevents a permanent defect causing a double-bit uncorrected (but detectable) error. Whenever something is fetched that would be mapped to a disabled cache line, the CPU has to fetch the data from memory. There is no performance penalty incurred since the fault affects only one cache-line. The Intel Cache Safe Technology feature will also keep the CPU from crashing if the cache-line ever fails.

Dynamic processor resiliency

‘Dynamic processor resiliency’ (DPR) is the system’s ability to de-allocate (online) those CPUs that are exhibiting an unacceptable number of correctable errors. CPUs are de-configured if the number of corrected cache errors reaches a specific configurable threshold. DPR is currently available on HP-UX 11i and to a limited extent with the Windows operating system. DPR is only available on HP Integrity servers. No other Itanium systems vendor offers the same level of Mainframe-caliber processor availability.

As the CPU technology advances, Dynamic Processor Resiliency will continue to be enhanced to deal with new recoverable error sources, such as register parity errors. This will further differentiate Integrity servers versus the competition, as it will eliminate about 70% of the remaining CPU error sources.

Additional HP Integrity processing RAS features

Cache error recovery and dynamic processor resiliency allow the system to recover from virtually every error. In addition, the Dual-Core Intel Itanium 2 processor has been error hardened with better VLSI circuitry. The possibility of an error even happening has been substantially reduced through the best designs and manufacturing available in the industry. Furthermore, the error detection capabilities have been extended into the core logic so that non-cache errors will be discovered. A desktop processor, on the other hand, does not detect these errors and enables valuable data to be silently corrupted.

Memory subsystem

The memory system consists of 288-bit memory ECC words with 256 bits of data and 32 ECC check bits. The design of the ECC code is driven by the requirement to support SDRAM two chip spares. In most implementations, words are accessed in 72-bit words with 64 bits used for data and 8 for ECC. However, the ECC algorithm only requires 6-bits and thus 2-bits per every 72-bit word are wasted. With zx2, four classic words are combined into a 288-bit quad-word and use the entire 32 ECC check bits with none wasted. This provides for an increase in the number of failed chips that can be tolerated in a traditional word from one to two. In other words, two complete DRAM chips can fail on a memory DIMM and the error will be recovered, having no impact on system availability. This capability is referred to as double chip sparing.

HP’s zx2 chipset also provides automatic hardware-based scrubbing of memory single-bit errors. This is offered because software based scrubbing is inherently unreliable on its’ own, as memory locked-down by certain applications can never be accessed by a software scrubber.
Double-chip-spare

An enhanced feature in HP zx2 and sx2000 systems is double-chip-sparing technology. The hardware can permanently detect/correct an error in any given DRAM and also detect/correct an additional memory error in any other memory location in the same codeword. This is done by firmware recognizing when the first DRAM has failed, and “erasing” its bits from the ECC correction calculations. This allows the ECC logic to correct for a second DRAM failure in the same ECC codeword. This feature can be applied to a single DRAM, or all DRAMs sharing a bit of a bus, or all busses of a memory subsystem. This maximizes the coverage of HP’s unique protection mechanism. This enhanced feature is a result of HP’s advance research in memory technology and does not require more DRAM’s per MB than was required for the zx1’s single-chip-sparing support. Compared to single-chip sparing, double-chip sparing reduces the likelihood of a memory induced crashes by 3x. Furthermore, this strategy is far more cost effective than memory mirroring implementations on IA32 servers for protecting memory and yet provides comparable high availability. Unlike memory mirroring and RAID, no extra DIMMs are required for double-chip sparing. Besides the obvious cost benefit, the other major benefit of double-chip sparing is that it nearly eliminates system downtime to replace failed DIMMs. As shown in the below figure, this technology will deliver about a 17x improvement in the number of DIMM replacements vs. those systems that use only single-chip sparing technologies. Furthermore, with repair rates on DIMMs lowered to be on the order of cables, the top four failing FRUs are all hot-swappable (Disks, IO cards, Fans, and power supplies) in a four processor entry-level Integrity rx6600.

Advanced I/O error recovery

The PCI Error Handling feature allows an HP-UX 11i system to avoid a Machine Check Abort (MCA) or a High Priority Machine Check (HPMC) if a PCI error occurs (for example, a parity error). Without the PCI Error Handling feature installed, the PCI slots are set in hard fail mode. If a PCI error occurs when a slot is in hard fail mode, an MCA or HPMC will occur, then the partition will crash.

When the PCI Advanced Error Handling feature is installed, the PCI slots containing I/O cards that support PCI Error Handling will be set to soft fail mode. If a PCI error occurs when a slot is in soft fail mode, the slot will be isolated from further I/O, the corresponding device driver will report the error, and the driver will be suspended. The olrad command and the Attention Button can be used to online recover, restoring the slot, card, and driver to a usable state. PCI advanced error handling, coupled with Multi-pathing, is expected to remove upwards of 90% of IO error causes from system downtime.

DDR2 DIMM enhancements

HP’s stringent High Availability standards require that parity errors on memory addresses and memory control signals be detected by the zx2 chipset. This checking is important because, without parity protection, a ‘bit flip’ on an address / control line may cause the correct data to get written into the wrong location in memory, resulting in data corruption. Furthermore, this type of data corruption is very difficult to detect, since there is no way to determine how a specific memory location got the wrong data. Prior to zx2 and DDR2 memory, you could only get address/control parity protection with HP proprietary DIMMs in the mid-range and high-end cellular Integrity systems. Because HP felt that this was such an important RAS feature, HP worked with the JDEC standards committee to make it a part of the DDR2 specification. Now a single parity error can be detected down to a single DIMM making FRU identification for replacement easy.
Page De-allocation

It is very common to have single bits in a DRAM ‘go bad’ (fail hard) during the life of a computer system. It is advantageous to map these locations out of main memory, as a persistent single bit memory error can be a performance issue.

HP has come up with a unique solution to the single bit hard-fail problem. If a location in memory is ‘bad’, that physical page (4k ‘chunk’) is de-allocated. This physical page de-allocation is persistent across reboots. Over the course of a system’s life, many memory locations can hard-fail, and HP can silently handle hundreds of these faults per system. These de-allocations occur dynamically, without any OS or application interruption. If a location in memory proves to be ‘questionable’ (i.e., exhibits persistent errors), that memory will be de-allocated online, with no customer visible impact. Given the number of spare pages in a system, it is likely that the failed memory will never have to be replaced over the life of the product, resulting in a significant reduction in planned downtime. Furthermore, HP sets a threshold on the total number of tolerated de-allocated pages such that server performance is immeasurably impacted.

I/O Subsystem

The I/O subsystem connects the processors and memory to the I/O cards. Two types of zx2 chips are used in this process: the memory and IO controller (MIO), and the PCI-X & PCI –Express IO Adapters (IOA).

Each PCI-X or PCI-Express IO adapter derives a bus; with most being dedicated, though some are shared among two slots. This architecture provides greater system availability and flexibility by allowing the user to balance cards so that either failures can be isolated to a single PCI bus, or maximally loaded with critical cards isolated and less critical ones sharing a bus. Since each bus is logically and electrically isolated from all other PCI busses, PCI errors are generally contained to the bus that generated the error, and therefore will not propagate to others in the system. This significantly reduces the system-wide impact of I/O errors. The PCI-X Host Bridge in the zx2 supports PCI-X 2.0 266MHz as well as all previous version of PCI/PCI-X. The new PCI-X 2.0 I/O bus has higher reliability due to the addition of ECC along with the higher bandwidth. The zx2 will enable ECC for any PCI-X card that supports ECC whether it is running at 133 MHz or 266MHz. The PCI-Express option will have full bus error protection as well.

Isolated I/O Paths

This feature allows accessibility to a storage-device/networking-end-node through multiple paths. The access can be simultaneous (in an active-active configuration) or streamlined (in an active-passive configuration). With this feature, points of failure between two end points can be eliminated. The system software can automatically detect network / storage link failures and can failover (online) to a standby link. This feature makes the system fault tolerant to any I/O cable and device-side I/O card errors, which are estimated to be at least 90% of all I/O error sources.

Advanced I/O error handling

The PCI Error Handling feature allows an HP-UX system to avoid a Machine Check Abort (MCA) or a High Priority Machine Check (HPMC), if a PCI error occurs (for example, a parity error). Without the PCI Error Handling feature installed, the PCI slots are set in hard-fail mode. If a PCI error occurs when a slot is in hard-fail mode, an MCA or HPMC will occur, then the system will crash.

When the PCI Advanced Error Handling feature is installed, the PCI slots containing I/O cards that support PCI Error Handling will be set in soft-fail mode. If a PCI error occurs when a slot is in soft-fail
mode, the slot will be isolated from further I/O, the corresponding device driver will report the error, and the driver will be suspended. The olrad command and the Attention Button can be used to online recover, restoring the slot, card, and driver to a usable state. PCI advanced error handling, coupled with Multi-pathing, is expected to remove upwards of 90% of I/O error causes from system downtime.

**PCI OL* (Online addition, replacement and deletion)**

The system hardware uses per-slot power control combined with operating system support for the PCI Card online addition (OLA) feature to allow the addition of a new card without affecting other components or requiring a reboot. This feature enhances the overall high availability solution for customers since the system can remain active while an I/O adapter is being added. All HP supported PCI cards (Gigabit Ethernet, Fiber Channel, SCSI, Term I/O, etc.) and the corresponding drivers have this feature. The new card added can be configured online and quickly made available to the operating environment and applications. PCI OL* is an easy to use feature in HP products, enhanced by the inclusion of doorbells and latches.

Furthermore, I/O cards can fail over time, resulting in an automatic failover to the secondary path, or a loss of a connection to a non-critical device (For those devices that do not warrant dual-path I/O). PCI online replacement (OLR) allows a user to repair a failed I/O card, online, restoring the system to its initial state without incurring any customer visible downtime.

**Chassis infrastructure**

The chassis infrastructure is designed so that the most likely to fail components are all hot-swappable. Easy-to-understand troubleshooting and tool-less repair are emphasized in entry-level Integrity designs.

**Power infrastructure**

HP Integrity zx2 based hardware is capable of receiving AC input from two different AC power sources. The objective is to maintain full equipment functionality when operating from power source A and power source B, or A alone, or B alone. This capability is called “fault-tolerant power compliance”, and it is a requirement for certification earned from the Uptime Institute.

For equipment to qualify as being truly fault-tolerant power compliant by the Uptime Institute, it must meet all of the following criteria as initially installed and as ultimately used in operation:

- If either one of two AC power sources fails or is out-of-tolerance, the equipment must still be able to start up, or continue uninterrupted operation with no loss of data or reduction in hardware functionality, performance, capacity or cooling.

- After the return of either AC power source from a failed or out-of-tolerance condition during which acceptable power was continuously available from the other AC power source, the equipment will not require a power-down, IPL, or human intervention to restore data, hardware functionality, performance or capacity.

- The first or second AC power source may fail one second after the return of the first or second AC power source from a lost or out-of-tolerance condition with no loss of data, hardware functionality, performance, capacity or cooling.

- The two AC power sources can be out of synchronization with each other having different voltages, frequencies, phase rotations, and phase angles as long as the power characteristics for each separate AC source remain within the range of the manufacturer’s published specifications and tolerances.
• Both AC power inputs will terminate within the manufacturer’s equipment. Internal or external active input switching devices (e.g., static transfer switches) are not acceptable.

• A fault inside the manufacturer’s equipment which results in the failure of one AC power source shall not be transferred to the second AC power source causing it to also fail.

• With both AC power inputs available, the power provided by each of the two internal power trains will be 50% ± 10% of the power output for the supply.

• An external software alarm must be provided via the equipment’s software or the host’s operating system when an AC power source is lost or is outside the manufacturer’s published tolerances and when the abnormal condition is corrected.

The design of the individual Bulk Power Supplies and the configuration of the power interconnect in HP Integrity systems meets the conditions listed above for fault-tolerant power compliance. In addition, the BL860c has been certified by the Uptime Institute in meeting these requirements.

Cooling Infrastructure

All fans in zx2 based systems are fully redundant and hot-swappable. These elements can be serviced without affecting uptime of the system.

Fault Management

Fault management is any action taken (preventive, reactive, proactive, or instantaneous) to detect and respond to an unplanned disruption in system availability. As discussed in the previous pages, fault management starts with the quality, the design, and the engineering of every HP server.

Figure 4 Secured Availability of Integrity Servers

In an adaptive enterprise, the built-in product fundamentals are created with fault management in mind. It contributes to continuous and secure operation, dynamic resource optimization, and automated and intelligent management. It is the solution base that enables self-healing and platform
management. It is not a new concept, nor a new initiative; it is simply and will always be fundamental to HP server designs. With the advent of the Intel Itanium Processor Family, HP extends this fundamental design, enabling this offering for Windows and Linux alike. The total fault management offering translates directly into the following four important customer values:

Lower risk of downtime due to faults
- Hardware validation and burn-in tools designed to screen out potential component failures
- Self-healing and highly reliable hardware

Minimized downtime required to recover from faults
- Intuitive tools (iLO2 (Integrated Lights Out, HP ISEE (Instant Support Enterprise Edition), Fault Monitor, System Insight Display, etc.)
- Unsurpassed coverage breadth and depth for problem detection and isolation
- Clear and accurate recommended actions for problem resolution included in reported events so that cross referencing with hardcopy guides is not necessary
- Exercisers for intermittent and performance degradation problems
- Verifiers to ensure repair success
- Ease and speed to physical repair

Problem resolution is easy and low cost; lower TCO
- Better than an easy install, the tools are preinstalled
- Easy to integrate with the existing infrastructure, whether it is HP OpenView, IBM Tivoli, or some other enterprise management application
- In the event that HP completely manages your environment, the fault management tools become the underlying essentials that extend the capabilities of the Instant Support Enterprise Edition (ISEE) support services.
- The fault management applications are designed to be intuitive and effective; the user-friendly event descriptions make the problem determination tools easy to use and comprehend
- The management processor also serves as a remote fault management tool providing an out-of-band method to troubleshoot or manage your HP server
- Service access, fewer steps for hardware replacement or repair
- Fault tolerant and fault containment designs further ease the repair process

Improved total customer experience
- The HP total customer experience is rounded out by making this aspect of the usage phase:
  - Simple
  - A consistent experience, regardless of the operating system residing on the HP Integrity hardware

Serviceability
The days have passed where serviceability was thought of only in the context of part swapping; serviceability is the whole solution that enables effective problem response, recovery, and resolution. Not unlike the other RAS components, serviceability is made of tools, processes, and hardware designs that ultimately contribute to system availability and determine TCO.

Our serviceability strategy is simple: Fix it fast. Problem resolution is made quicker, easier, and more precise. We conscientiously engineer solutions for maximizing uptime when faults occur and even for instances when faults require hardware replacement.

Figure 5 below shows serviceability in its reactive fault recovery space of fault management. However, we will review some of the proactive “keep it running” aspects, providing more detail about the proactive tools themselves.
Preventive hardware design

Fault management starts by working with hardware and OS designers to create hardware and software capabilities and instrumentation points that provide the ability to detect and isolate system anomalies at both the manufacturing level and the end-user production environment. HP Integrity Servers embody the latest and foremost of HP fault management to ensure maximum uptime in your high-availability environment. Much of this fault-avoidance design has already been described in the reliability and availability sections. The following sections discuss some additional capabilities involving the serviceability and fault recovery of Integrity.

Tool-less design

One of the areas where better serviceability is designed in is with the goal of tool-less design. With all FRUs, other than the processor, no tools are required. For the processor, the one tool that is required is attached to the system for easy access. All of this translates to fast repair and consequentially more system uptime.

Customer self-repair

With repair of zx2 systems so easy and fast, the customer can replace and upgrade certain hardware components themselves. For example, even though HP has the fastest response times in the industry, customers can choose to swap in a new disk drive rather than wait a few hours for an HP representative to come on site. HP gives its entry-level Integrity customers choices, so the IT operator can choose the repair method that works best for them.
Integrity iLO: The Management Processor

The HP Integrity entry-level servers have upgraded the Integrity iLO (Integrated Lights Out), sometimes known as the management processor (MP), to iLO2 with its zx2 systems. It is one of the interfaces used for service and for the console. The iLO2 also is used for monitoring the health of the system. HP customers can choose between a menu-driven or command line interface for iLO2. The menu-driven interface is identical to that used in HP ProLiant servers, while the command line interface is common with HP 9000 systems.

One clear advantage of iLO and iLO2 is its out-of-band access, acting independently of both the operating system and the payload LAN. Sometimes referred to as “extended fault management,” the iLO2 is capable of remote power control and environmental monitoring of the fans, temperature, and power supplies, display of system configuration, and configuration of the MP itself. Users can connect to partition consoles, display server and partition state, view archived and live logs, and (with over 40 available commands) perform many other platform management capabilities. iLO2 protects the system from unauthorized use of these functions by authenticating users, assigning them role-based capabilities, and by offering secure (SSL-based) access using secure Embedded Web Console.

The Integrity iLO also provides a Virtual Front Panel (VFP), a real-time display of the system’s boot status and activity. The VFP provides the following types of information: progress status of the system through boot sequence, the operating state of the system, and any errors detected and flagged during boot process.

The iLO was designed to monitor and control system availability. Therefore, iLO is designed in such a way that a failure of the iLO will not cause the system to crash nor prevent the system from booting. New to the zx2 designs is iLO2 which provides even more capabilities with remote graphics console (sometimes known as virtual KVM) and remote media (virtual media).

Troubleshooting, diagnosis, and preventative tools

Besides the out-of-band iLO, there are several in-band tools that further enrich the serviceability of Integrity servers. Run on the operating system, prevention and health monitoring are the emphasis of these tools. Though HP provides tools for all operating systems that Integrity supports (Windows, Linux, OpenVMS, HP-UX 11i), the most comprehensive set run on HP-UX 11i and are further detailed below.

HP-UX 11i proactive tools

While much of the proactive fault management space is gracefully handled by the preventive hardware designs, there are also the tools that monitor, detect, and report ensuing faults. The monitoring tools also have the ability to take corrective action before an unplanned downtime event occurs. These monitoring tools are part of HP-UX EMS.

HP-UX 11i EMS

The Event Monitoring Service (EMS) is made up of three primary components: the target and client applications, the resource monitors, and the Event Monitoring Service framework itself. Client applications are the applications used to configure the monitors. Target applications are the end-user interfaces where notifications are sent. The EMS framework contains the APIs, registrar, and resource dictionary.
Resource monitors

Resource monitors include hardware monitors, software monitors, and optional high-availability monitors. Monitors can also be referred to as agents or providers. Resource monitors are responsible for the detection, isolation, and reporting of system faults or impending failures. Notification is available to the system console, e-mail, pager, logs (text log and/or syslog), HP Support Services, and enterprise management platforms.

Hardware monitors are installed with the base operating system and cover both core system components and peripheral devices. These are native EMS monitors and they include CPU, memory, chassis, fans, system bus, temperature, disk arrays, SCSI devices and enclosures, Fibre Channel devices, and power supplies. The monitors perform subsystem log tracking, event correlation to the most suspect FRU, predictive analysis to determine likelihood of impending failure, and reporting with failure cause-action statements. In addition, the monitors extend their value by providing isolation and correction capabilities, also referred to in the industry as self-healing. These include online and persistent de-allocation of failed processors (DPR), de-allocation of memory pages, graceful system shutdown upon power failover to UPS, and automatic system restart upon system hang.

Software and high-availability monitors provide even more extensive monitoring capabilities. These monitors cover kernel resources, network, LAN aggregate and failover, database, clusters, etc.

HP-UX 11i RAS feature highlights

In addition to the features already mentioned – PCI I/O error Handling, PCI online addition, PCI online replacement, EMS – HP-UX 11i v2 has even more capabilities in the areas of reliability, resiliency and reparability. These capabilities include vPars, HP Integrity Virtual Machines (Integrity VM), dynamic tunables and security containment. vPars provides operating system and application isolation across soft partitions, and allows for individual reconfiguration and reboot. Integrity VM is a soft
partitioning and virtualization technology that provides operating system isolation, shared processor (with sub-processor granularity), shared I/O and automatic dynamic resource allocation built in. With HP-UX 11i v2, additional dynamic tunables have been identified which further minimize planned downtime by eliminating reboots needed to change certain kernel parameters. HP-UX 11i Security Containment is comprised of three core technologies – compartments, fine-grained privileges and role-based access control. HP-UX Security Containment makes several trusted mode security features available on standard mode HP-UX 11i systems.
### Summary

<table>
<thead>
<tr>
<th>Location</th>
<th>Features</th>
<th>Customer experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory system</td>
<td>Error detection / correction</td>
<td>17x fewer DIMM replacements than with traditional chip-spare</td>
</tr>
<tr>
<td></td>
<td>DIMM address parity protection</td>
<td>Extreme levels of availability with no compromise of system performance or any added hardware cost</td>
</tr>
<tr>
<td></td>
<td>hardened proprietary DIMM</td>
<td>Risk of memory data corruption is drastically reduced to near zero with HP’s DIMM enhancements</td>
</tr>
<tr>
<td></td>
<td>Double-chip sparing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power redundancy</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>Cache error detection / correction</td>
<td>Covers all cache errors and the majority (70%) of the CPU core errors resulting in much better error coverage and data integrity than can be expected with x86 CPUs: Enterprise-class reliability for Enterprise customers.</td>
</tr>
<tr>
<td></td>
<td>Cache Safe Technology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Core logic parity protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic Processor Resiliency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processor Bus ECC</td>
<td></td>
</tr>
<tr>
<td>I/O slots</td>
<td>Error detection / correction</td>
<td>Moves I/O errors from one of the major contributors of system downtime (~2 years MTBF) down to only a minor nuisance (~50 years MTBF). The ability to online repair further enhances the fault avoidance capabilities.</td>
</tr>
<tr>
<td></td>
<td>PCI failure isolation to a single slot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enhanced I/O error recovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multi-pathing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PCI card OLARD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power redundancy</td>
<td></td>
</tr>
<tr>
<td>Chipset</td>
<td>Internal data path error detection / correction</td>
<td>HP’s value added chip-set puts performance and availability above all else.</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Machine Check Architecture (MCA) and event monitoring.</td>
<td>Itanium processor MCA handling allows processes to attempt to recover without crashing the system. In addition, Enhanced MCA combined with event monitoring provides comprehensive diagnostic information to help root cause issues to drivers, the OS, firmware, or hardware so that errors can be eliminated and corrected quickly.</td>
</tr>
</tbody>
</table>
For more information

HP Integrity servers:  [www.hp.com/products1/servers/integrity/index.html](http://www.hp.com/products1/servers/integrity/index.html)

HP-UX 11i:  [www.hp.com/go/hpux11i](http://www.hp.com/go/hpux11i)

HP Virtual Server Environment:  [www.hp.com/go/vse](http://www.hp.com/go/vse)


For more information on EMS monitors, go to  [www.docs.hp.com/hpux/ha/index.html](http://www.docs.hp.com/hpux/ha/index.html).