UEFI on ThinkSystem V4 servers

New features and enhancements

Lenovo

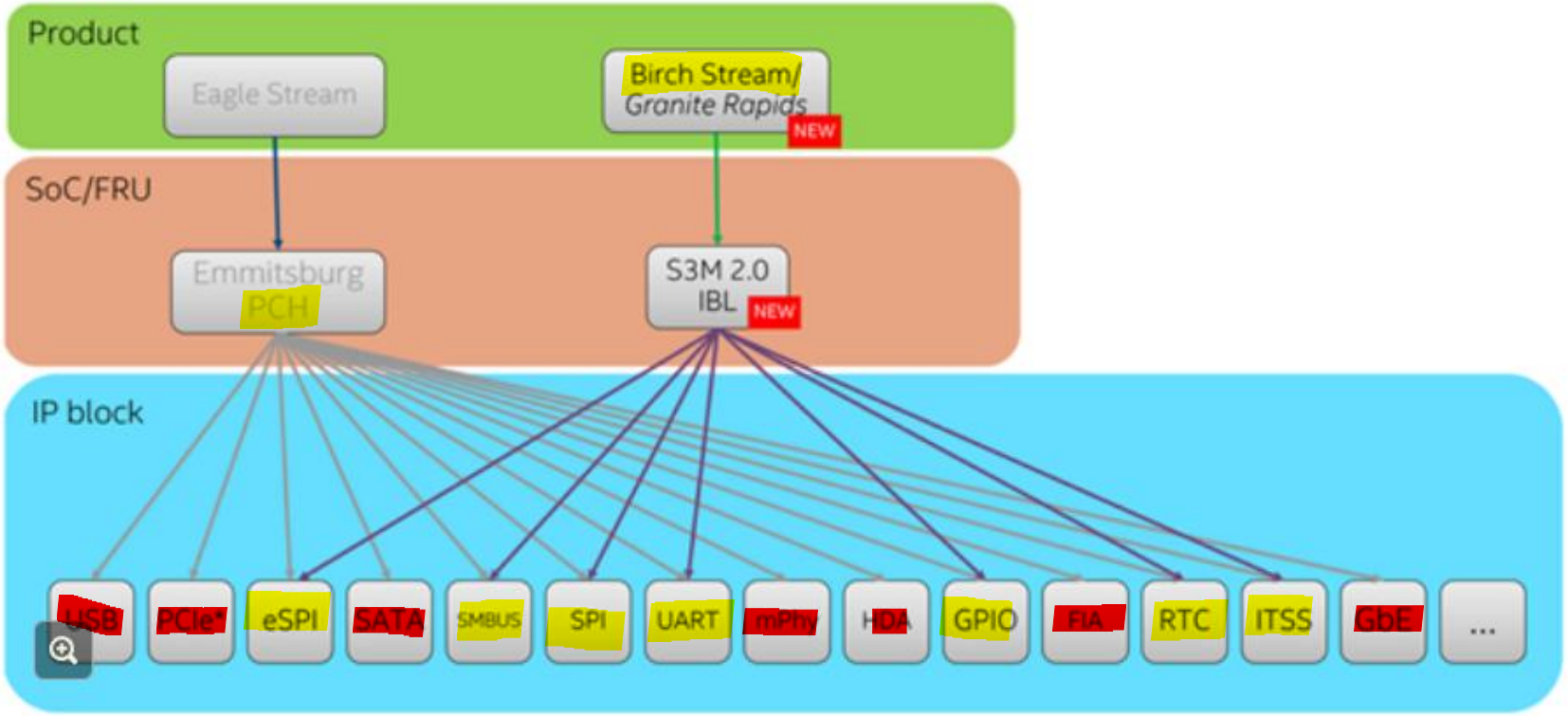
UEFI design change to support Intel Xeon 6 processors

Due to the removal of the Platform Controller Hub (PCH) from the Intel Birch Stream (BHS) platform of processors, there have been some design changes in the version of UEFI used with the ThinkSystem V4 portfolio of Intel® Xeon 6 servers. These design changes will not be introduced in depth in this course. Instead, a service perspective will be taken to highlight the differences between this version and the previous version of UEFI.

BHS PCH-less vs EGS PCH

This figure shows a comparison of the Birch Stream / Granite Rapids (BHS) PCH-less and Eagle Stream (EGS) PCH products. With the PCH-less setup, you can see that USB, PCIe, SATA, and GbE are no longer controlled by the processor.

- S3M: Secured startup services module
- IBL: Integrated boot logic
- ITSS: Interrupt and timer subsystem (ITSS)
- HDA: High-definition audio
- FIA: Flexible I/O adapter



UEFI Setup – Custom and factory default settings

- UEFI on ThinkSystem V3: There is only one option - select **Load Default Settings**
- UEFI on ThinkSystem V4: Select **Default Options** to open a setup page with two default options:
  - Custom Default
  - Factory Default

Click the buttons to see screenshots.

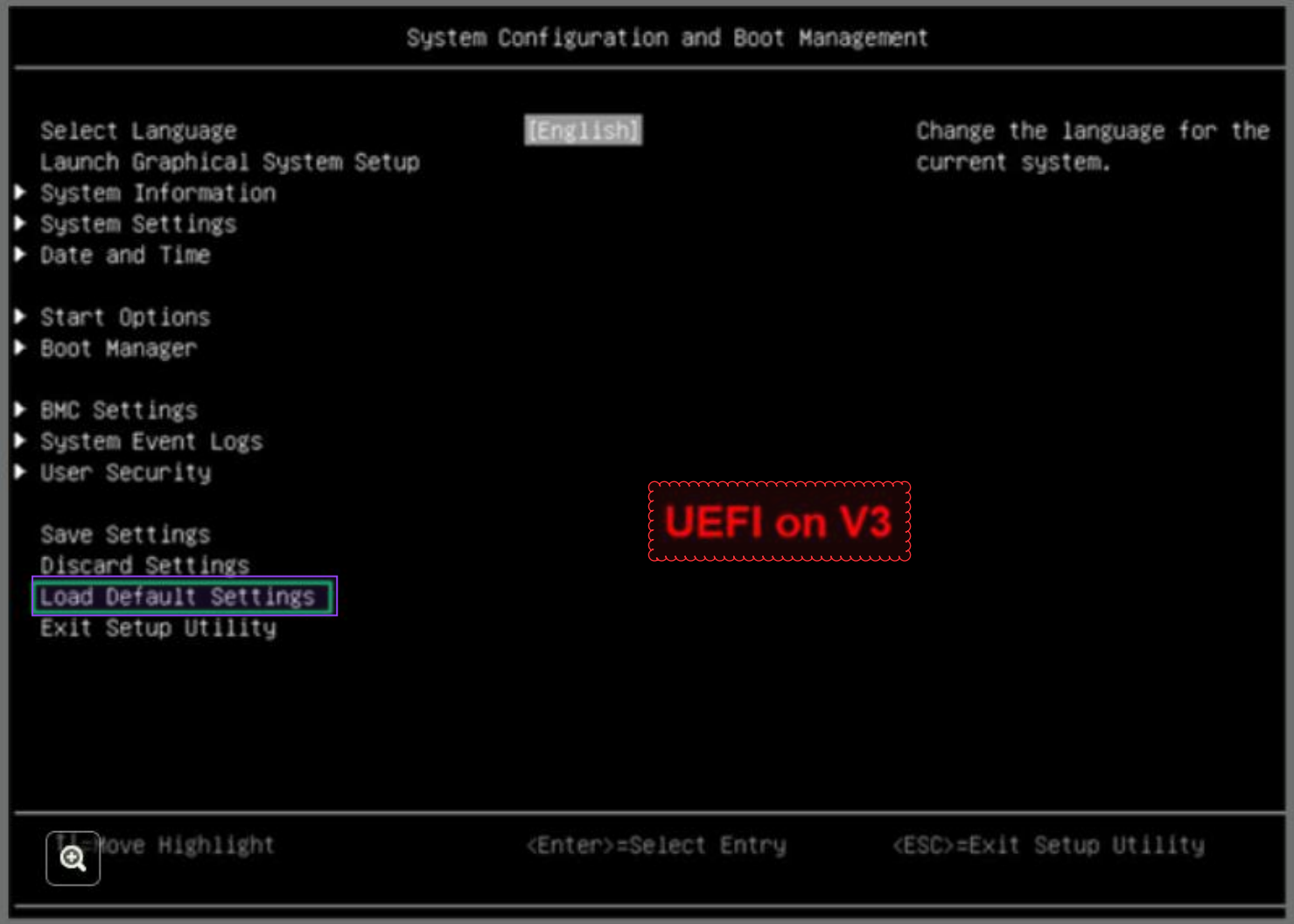
UEFI on ThinkSystem V3

UEFI on ThinkSystem V4

UEFI Setup – Custom and factory default settings

UEFI on V3 – Load Default Settings

There is only one option. Select **Load Default Settings**.

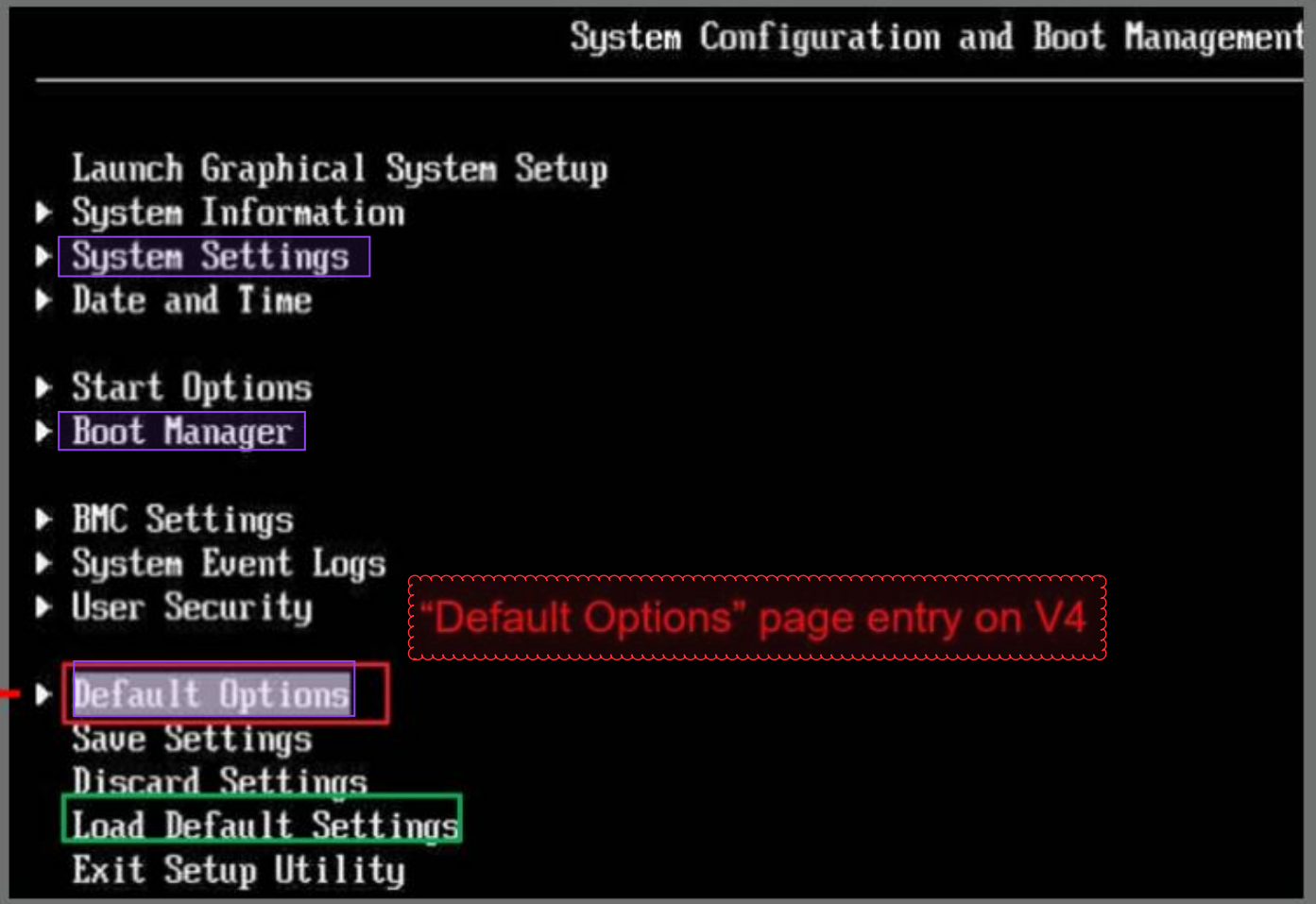


UEFI Setup – Custom and factory default settings

UEFI on V4 – Default Options

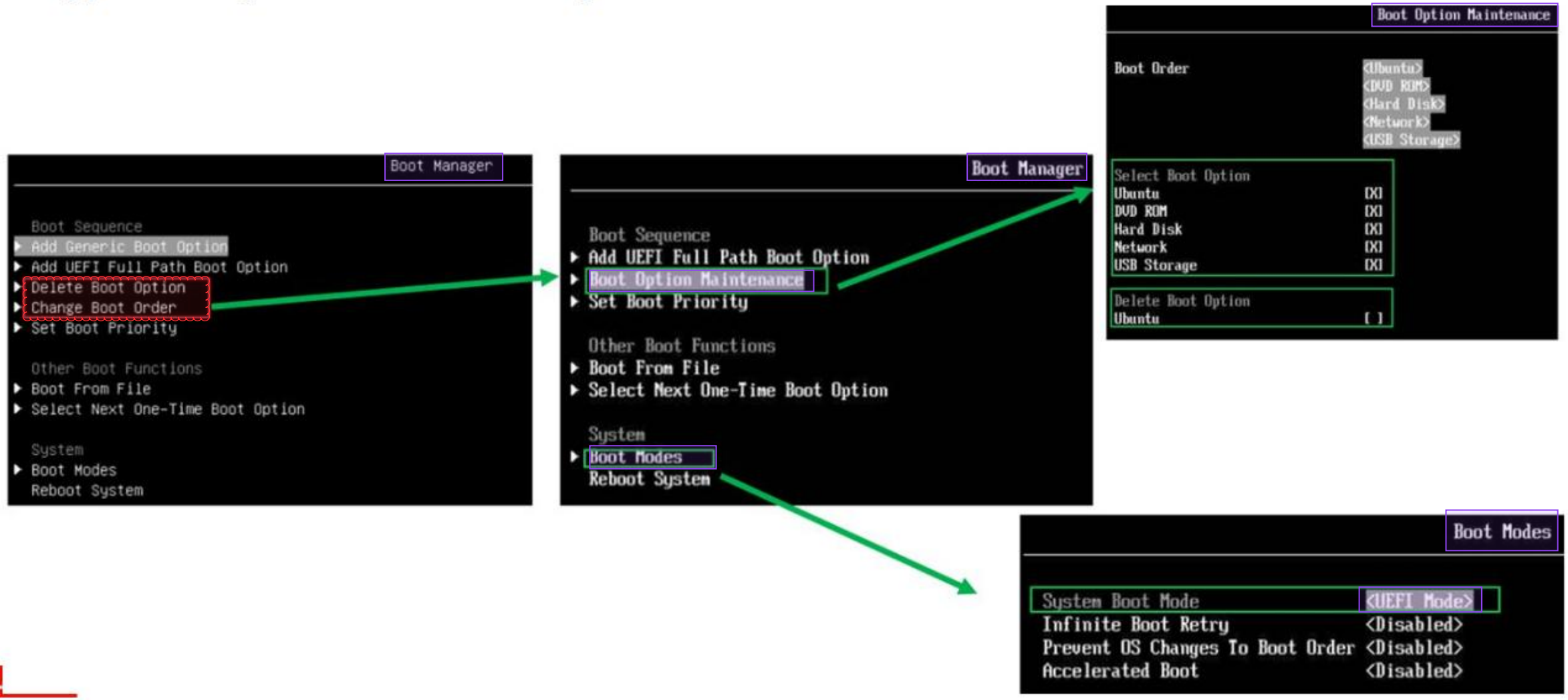
Select **Default Options** to open a setup page with two default options:

- **Custom** Default
- **Factory** Default



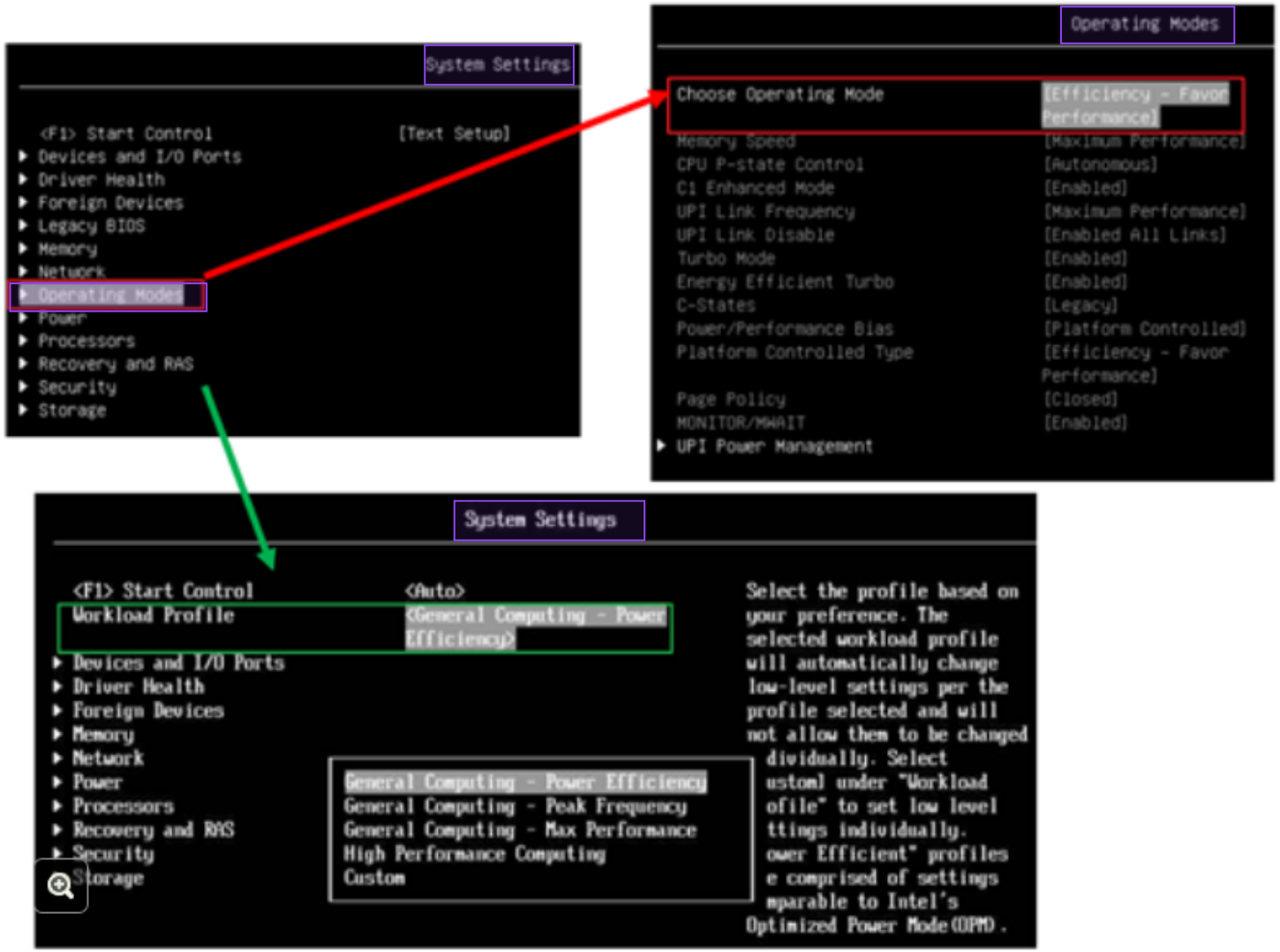
UEFI Setup – Boot manager enhancement

To optimize boot option management in the ThinkSystem V4 UEFI, there is a new setup page to support change and delete boot options.



UEFI Setup – New workload profiles

- Profiles more accurately match customer needs based on workload characteristics
- The workload profile meets the benchmark standard
- The following profiles are already supported:
  - Two general computing workload profiles
  - One HPC workload profile
- The following profiles are due to be supported in wave 2:
  - Two virtualization profiles
  - One database profile
  - One low latency profile



RAS feature enhancement - FQXSFMA0056M

To support SRAR and UCNA, the [arg4] element has been added to the FQXSFMA0056M UEFI event message:

An uncorrected recoverable memory error has been detected on DIMM [arg1] at address [arg2].[arg3] [arg4]

[arg4] values: **–T0** to indicate the error is UCNA

–T1 to indicate the error is SRAR

See the following slide for examples.

To simplify the system error log (SEL):

- Only one uncorrectable error (UE) is reported in the SEL per CPU (UEFI event: FQXSFPU0027N / FQXSFPU0062F)
- Only one UE is reported in the SEL per DIMM (UEFI event: FQXSFMA0056M (with T0 or T1))

Note:

- **SRAR** - **S**oftware **R**ecoverable Error **A**ction **R**equired
- **UCNA** - **UnC**orrected **No** **A**ction (an uncorrectable error logged in MCA Bank)

UEFI event FQXSFMA0056M – SEL screen capture

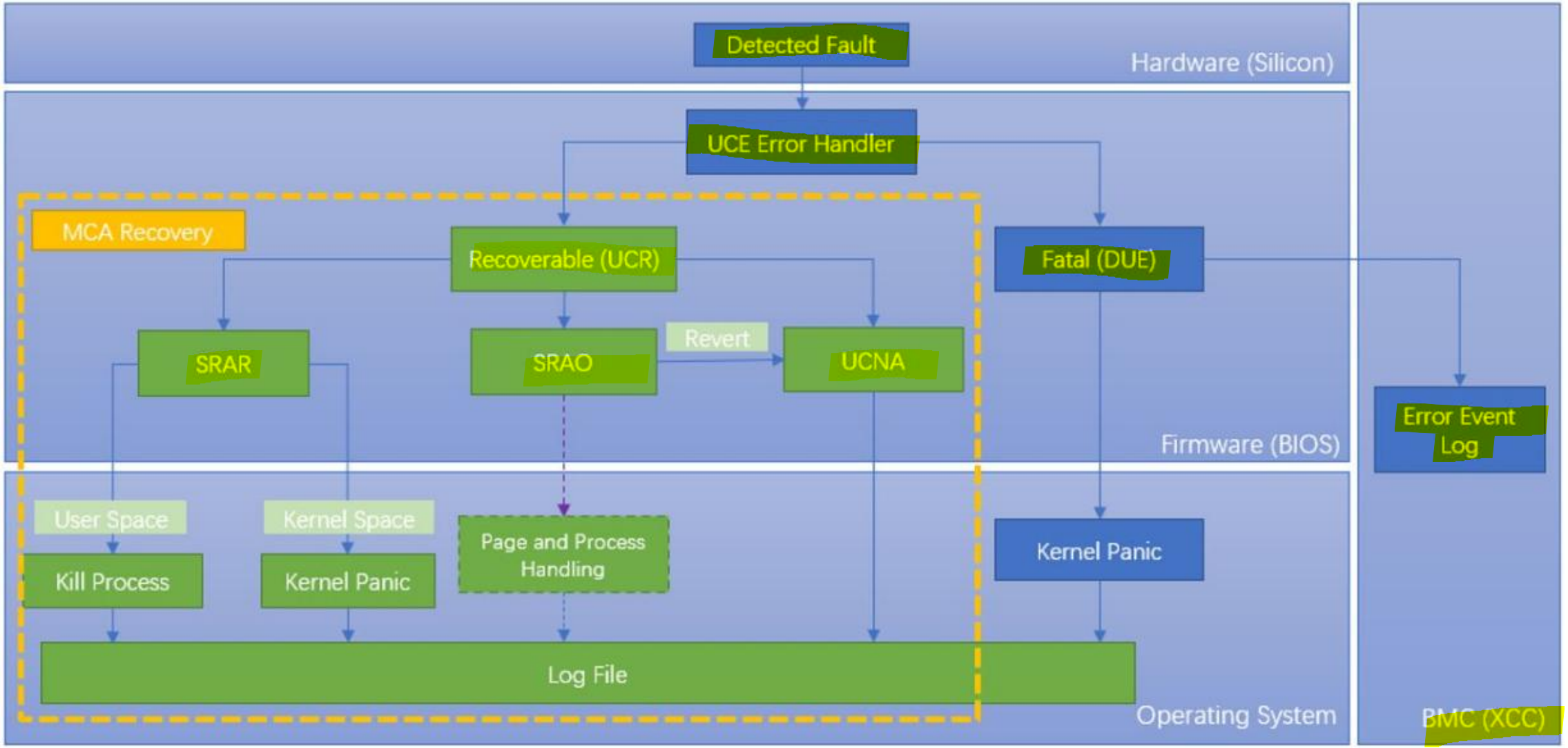
FQXSFMA0056 represents both the UCNA and SRAR memory error types.

- UCNA is indicated by an arg string of -T0
- SRAR is indicated by an arg string of -T1

SEL detail:

4	Memory	FQXSFMA0056M	An uncorrected recoverable memory error has been detected on DIMM 10 at address 0x000000013C2C0400.80AD0121281387AFDB-VC20 -T1	January 8, 2001 5:36:28 AM
5	Memory	FQXSFMA0082M	An uncorrected recoverable memory error has been detected on DIMM 10 and post package repair (PPR) recorded.	January 8, 2001 5:36:27 AM
6	Memory	FQXSFMA0056M	An uncorrected recoverable memory error has been detected on DIMM 10 at address 0x000000013C2C0400.80AD0121281387AFDB-VC20 -T0	January 8, 2001 5:36:27 AM

UEFI SEL flow chart



RAS feature enhancement – runtime sPPR

Runtime PPR (post-package repair) is a new DDR5 feature with the BHS platform. It works by using spare rows to replace a row identified in runtime by UEFI as failing.
Note: Only soft PPR (sPPR) will be supported.

Runtime PPR has been added in ThinkSystem V4 UEFI as a setup item and is disabled by default.
- UEFI setup path: **System Settings** → **Memory** → **Runtime PPR**

Runtime PPR handling

- Report a hiddenlog for runtime PPR success/failure
- Report one related SEL per DIMM
- Remove the pending page retire request on the row if PPR was successful
- Carry out the page retirement for the addresses on the row if PPR failed