SEAPATH-Debian or SEAPATH-Yocto

Two versions of LFEnergy SEAPATH could be used, one based on Yocto and one on Debian. They offer the same high level features but differ in their philosophy and implementation.

The Debian version uses prebuilt packages provided by the Debian team, while the Yocto version fetch the sources of all the software and rebuild everything from source.

Here is a comparison of them:

Category	SEAPATH-Debian	SEAPATH-Yocto
Version	• Debian 12 (current) • Debian 11 (legacy)	• Yocto Kirkstone (current LTS) • Yocto Dunfel (previous LTS)
Features	• Host ○ Virtualization (KVM) ○ Containers (Optional with Docker) • Linux-RT • Ceph • Pacemaker/Corosync	• Host ○ Virtualization (KVM) ○ Containers (Optional with Docker) • Linux-RT • Ceph • Pacemaker/Corosync
Build	• Use FAI to create a disk installation with default configuration • No build of packages: use pre-build package from Debian	• Build every software from the source code
Customization	• No ability to customize libraries and binaries ○ Relying on Debian community	• Ability to customize libraries and binaries ○ Customization could be done by Yocto community ○ Customization could be done by SEAPATH community ○ Customization could be done by third-party community
Configuration	• Done by Ansible on run-time	• Done on build-time • Done by Ansible on run-time
Updates	• Uses apt to update packages • Use LVM snapshot for rollback in case of fault ○ Not atomic ○ No recovery possible if the machine doesn't boot • No way to update user applications currently. TODO	• Update the entire operating system ○ A/B update mechanism using SwUpdate ○ Atomic update ○ Automatic rollback mechanism in case of fault
Package management	• Uses APT ○ straightforward but may include extraneous dependencies.	• Every package is built and installed by Yocto • Each package can be modified to remove useless features
Reproductibility	• Available on most packages individually, but not for Debian as a whole (Debian reproducible builds)	• Fully reproducible builds

Cybersecurity	• Compilation flags ○ Debian stock configuration flags • Linux Kernel hardening ○ Debian stock kernel config ○ Designed to work with many kinds of machines and use cases • Minimization of services ○ Partially done: only essential packages are installed, but unnecessary configurations might be set	• Compilation flags ○ Done (TO DETAIL) • Linux Kernel hardening ○ SEAPATH specific kernel configuration with hardening ○ Done (TO DETAIL) • Minimization of services ○ Done
SBOM	• Analyzed / 3rd party SBOM ○ Created on the target without knowing build process ○ Done with heuristics and Debian database ○ Contains less information • Require external tools	• Build and Source SBOM • Generation integrated in the Yocto Project
CVE management	• CVE uploaded on the Debian security tracker • End user cannot patch the CVE itself • Issue is fixed by the Debian community ○ Strong community, but various response time ○ Patch may be applied to the next Debian version and not the current one.	• CVE of each package uploaded to the NIST database • Patch can be provided ○ By package community ○ By Yocto community ○ By SEAPATH user itself • Patch can be applied ○ manually by SEAPATH user ○ by updating the package to the next version
Maintenance	• Ease of use • Require package mirrors to create the disk offline	• steeper learning curve • Require time and strong machine to build ○ (ex: 4h on 32 cores 64G RAM machine) • require mirroring all sources to build offline