ELISA
Enabling Linux in Safety Applications

WORKSHOP

NASA Goddard

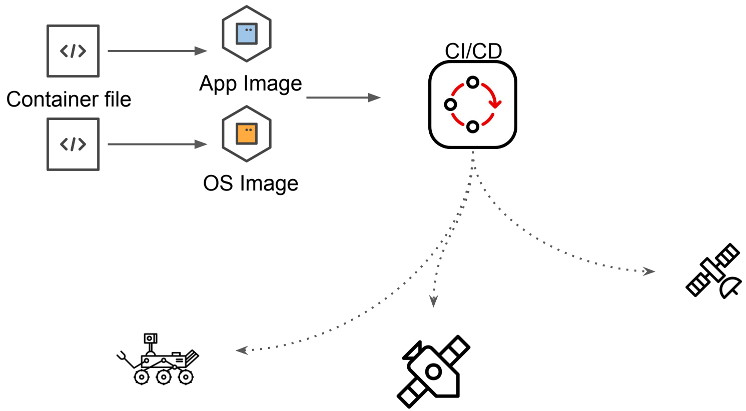
Container and immutable patterns for operating systems and workloads

Michael Epley
Chief Security Strategist

Tony James
Chief Architect, Science and Space

Why containers are the future of modern spaceflight computing

Containers are a packaging system – why not package your operating system in a container just like we package user space applications?

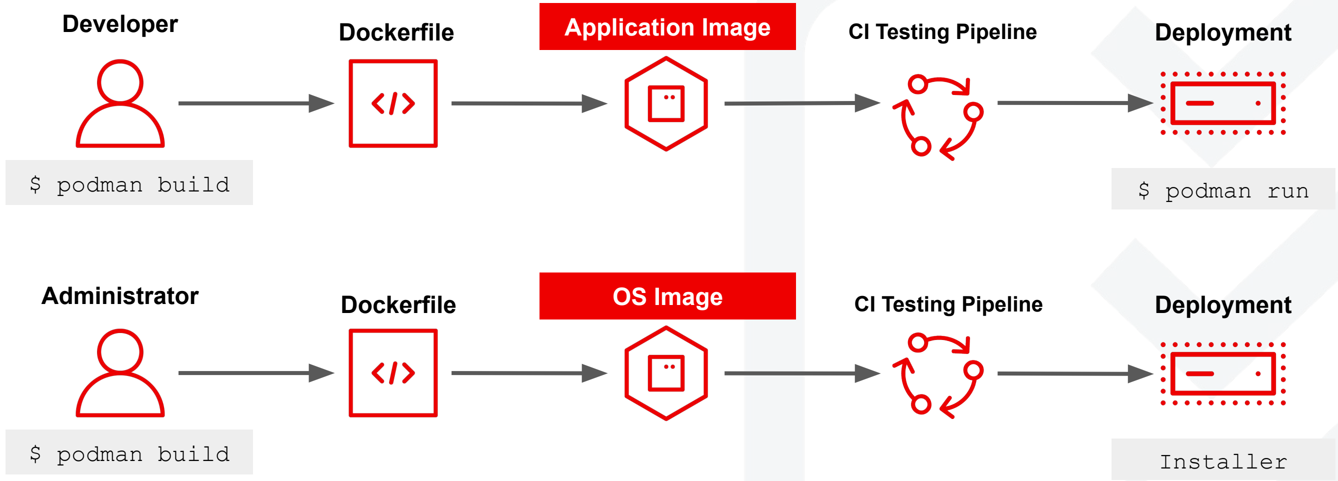


WE CAN!

- 🚀 **Missions** benefit from the simplicity and portability across different platforms and vehicles
- 🚀 **Developers** can use their favorite CI/CD & GitOps workflows
- 🚀 **Security teams** will be delighted by the cryptographic validation, transparent provenance, and tool consolidation
- 🚀 **Organizations** build trusted base operating system and can reliably distribute it

Container workflows now drive the operating system

Now we can promote a single workflow to manage everything from the applications to the underlying operating system. You can build, test, and deploy the operating system as if it was any other container.

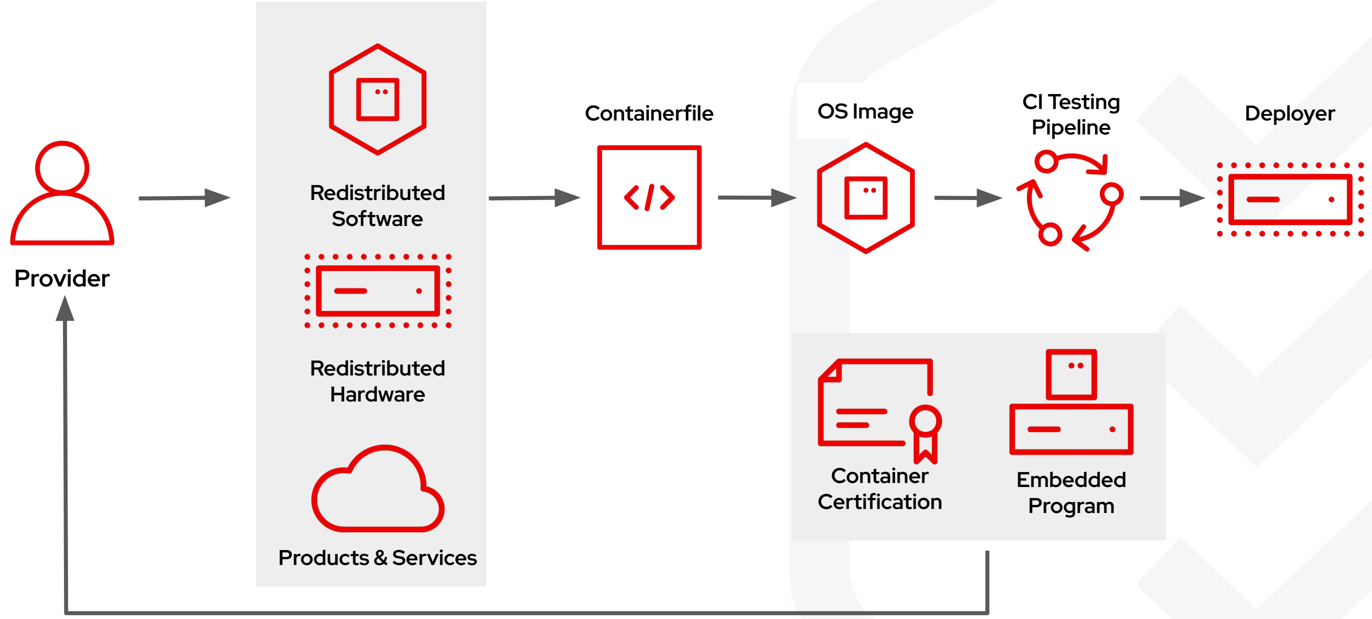


ELISA Enabling Linux in Safety Applications

WORKSHOP

Enabling an commercial space ecosystem

Allows compositional specialization since we have standardized packaging and component metadata



ELISA Enabling Linux in Safety Applications WORKSHOP

Enforcing security and safety through CI

Rich, policy-driven, consistent, reusable testing, validation, attestation in CI

Base
- Application Libraries
- Language Runtime
- Universal Base Image

Provenance, Attestation of Curated Content

▶

Code
- Software Composition Analysis | Digitally Signed & Verified

Dependency Analysis Recommendations

▶

Build
- Image Building | Image Scanning
- Artifact Signining | SLSA Attestation SBOM

▶

Deploy
- YAML Policy | Image Policy
- Signature Checks | Attestation Validation

▶

Monitor
- Profile Risk SBOM | Images Clusters Network

Platform Native Security

Meet Increased regulations, frameworks, directives

SEC Cybersecurity Rule [1] requires more governance and management regarding material cybersecurity risks, incidents.

Government Cybersecurity Regulations

White House Cyber Executive Order 14028

European Union Cyber Resilience Act

Cybersecurity Agency Frameworks and Directives

NSA Cybersecurity Collaboration Center (CCC)

National Institute of Standards and Technology (NIST)

Cybersecurity and Infrastructure Security Agency (CISA)

European Union Agency for Cybersecurity (ENISA)

Demo

WORKSHOP

A container-native workflow for the life cycle of a system

```
FROM rhel9/rhel-bootc:latest

RUN dnf install -y [software]
[dependencies] && dnf clean all

ADD [application]
ADD [configuration files]

RUN [config scripts]
```

ELISA
Enabling Linux in Safety Applications

WORKSHOP

Encapsulate differences in a sequence of builds

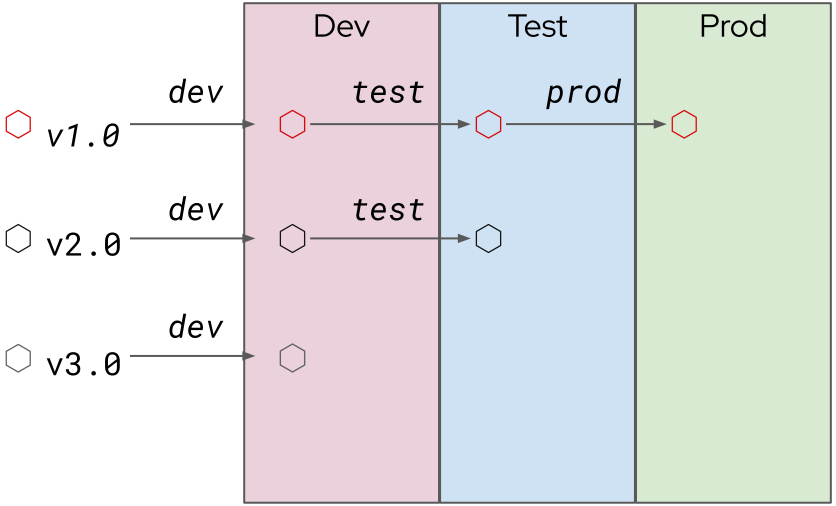
```
# Derive standard operating
environment
FROM rhel9/rhel-bootc:latest

RUN dnf install -y [system
agents] [dependencies]  && dnf
clean all

COPY [unpackaged application]
COPY [configuration files]

RUN [config scripts]
```

```
# Derive database server from SOE
FROM corp-repo/corp-soe:latest

RUN dnf install -y [database]
[dependencies]  && dnf clean all

COPY [configuration files]

RUN [config scripts]
```

OS Updates via Container Registries

Tags for powerful to version & promote updates

Unique Tags		Stable Tags



Tags offer simple versioning and visibility

Tags are simple to automate and use for promotions. Bootc will default to updating from a repository:tag.

Control updates via tagging

Combine tagging with the optional automatic updates to control fleets of systems via registry tags.

Standardized & scaleable infra

Container registries scale very well and any standard registry can be used.

ELISA Enabling Linux in Safety Applications

WORKSHOP

Bootc - A/B booting of container images

bootc upgrade

Download and stage an updated container image

bootc rollback

Rollback to the previous state. Staged updates are discarded

bootc switch

Change to a different reference image

bootc install

Install container image to-disk or to-filesystem

https://github.com/containers/bootc

Composefs - Filesystem layout

Build Time
Everything is writable. e.g. /usr, /etc, /opt, …

Run Time
All image content is read only

/var - RW, Not updated

/etc - RW, Machine local state (hostname, static IP)

Defaults aimed at 80%

Provides a balance of immutable updates w/ persistent config, logs, & container images

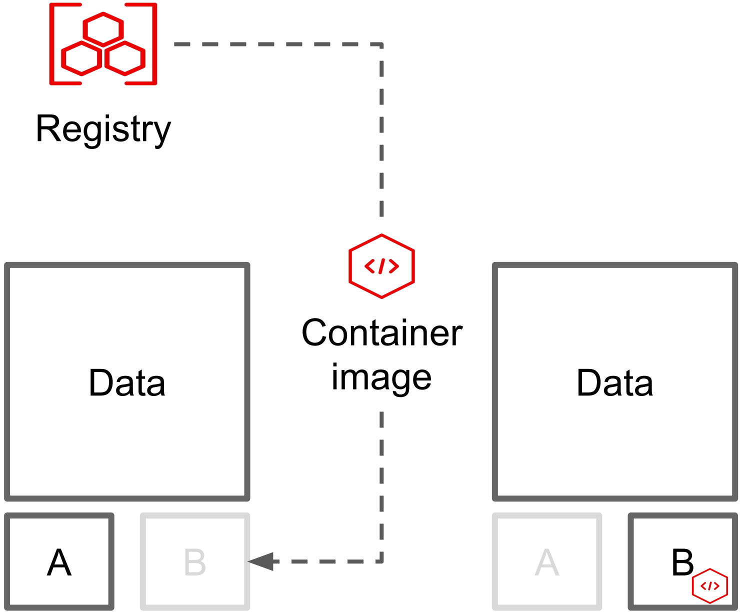
Powerful Configuration for the 20%

Transient / and /etc

RW possible for other directories via bindmounts and symlinks to /var

https://github.com/containers/composefs

Image-based updates



Transactional updates (A → B model)

Bootc uses composefs and ostree to convert the container image into the root filesystem on the host..

Roll forward or backwards

Updates are staged in the background and applied when the system reboots. The transactional model enables rollbacks for additional assurance

Simplified upgrades

bootc enables moving between major and minor releases

ELISA Enabling Linux in Safety Applications

WORKSHOP

registry.redhat.io/rhel9/rhel-bootc

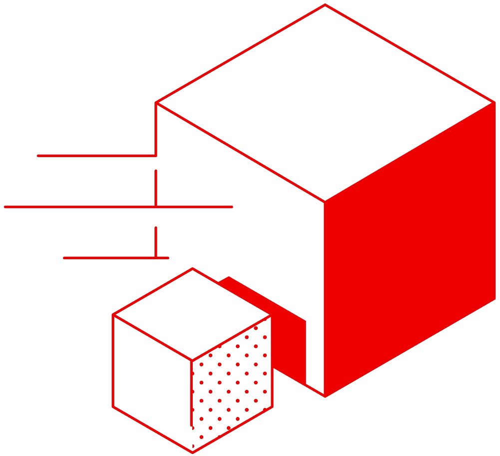


Image Specs:

- 🚀 439 rpms
- 🚀 ~785M compressed
- 🚀 ~2.2G on disk

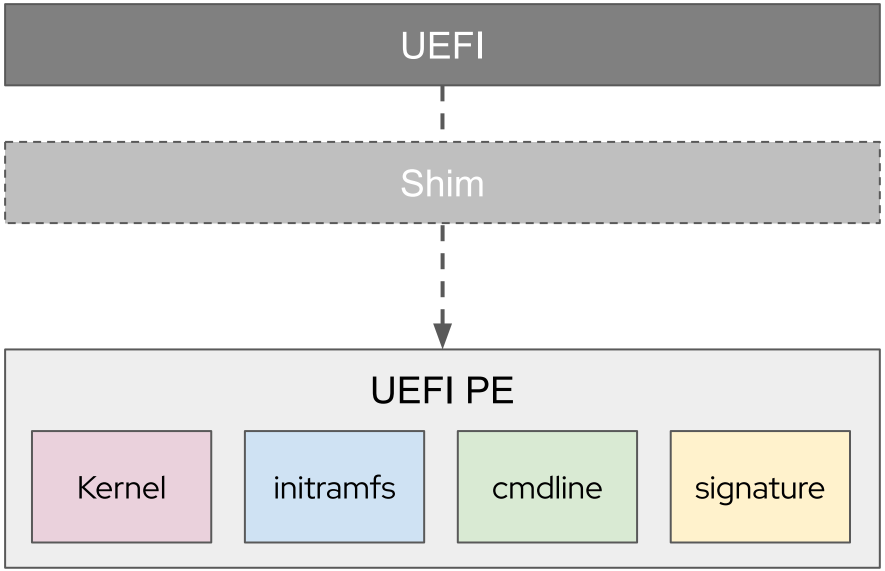
Primary contents:

- 🚀 systemd, kernel, bootc
- 🚀 rpm-ostree[1]
- 🚀 linux-firmware
- 🚀 NetworkManager
- 🚀 podman
- 🚀 python
- 🚀 Misc CLI tools: jq, sos

No cloud-init or virt agents

Unified Kernel Image (UKI)

No more bootloader



Security
A single PE binary (UEFI application) produced and signed in Red Hat build system. Avoids lack of measured boot for initramfs and bootloader passed params.

Tracking & Immutability
Bundled & contains vmlinuz, initramfs, and cmdline as PE sections. Must contain all dracut & kernel modules, and other mods.

Standardized
The base for building UKI is systemd-stub.

Discussion

ELISA Enabling Linux in Safety Applications WORKSHOP

Considerations – and solutions

- 🚀 One off designs
- 🚀 Unreliable Comms
- 🚀 Structured CMD/TLM
- 🚀 Sudden Resets

- ⭐ Containers promote consistency reusability, security
- ⭐ Integrate specialized firmware
- ⭐ Thin, fast images

Question:

Why can’t you just use an off the shelf linux baseline?

ELISA Enabling Linux in Safety Applications WORKSHOP

The End