Our Cyber-physical Future

A wave of connectivity, advanced software, analytics, and AI is transforming the world of industry, transportation, and energy. Smart, software defined machines are emerging with promises of major improvements in efficiency, flexibility, and sustainability, but these innovations also expose a vast new surface area for cyberattacks.

Within today's digital landscape lurks an alarming prevalence of cyber threats, along with the inherent consequences of attacks on our critical infrastructure. In a rapidly evolving technological landscape, the need for secure, resilient, cyber-physical systems has never been more urgent.

Legacy systems weren't built for the future

Legacy software platforms were designed before the emergence of cloud computing, and are not ready for a world of distributed, intelligent, software defined machines. Designed to automate office work, communications, and information access, they never anticipated the needs or risks presented by billions of connected, autonomous smart machines providing vital services and infrastructure. They were designed for different needs, different hardware profiles, different use cases, and greater human involvement in their operation. While they have adapted and morphed since their inception in the 70s, dredging a moat around weak castles will never keep the attackers at bay.

Mission critical systems are falling behind

Fearing this minefield of risk, our most vital systems have sidestepped the benefits and efficiencies of modernization and today face a different problem. Their aging tech stacks are weak, and their cost-to-serve is falling out of line with their markets.

No-one wants to imagine a future where our factories, infrastructure, farms, and transportation do not modernize and enhance the intelligence and security of their machinery. These sectors have fallen behind, not due to a lack of ambition or imagination or because they misunderstand what is at stake, but because they have been underserved.

The quest for a Secure OS

When you consider the incredible investment and advancement of AI happening today and the inevitable outcomes over the next several years, there is no doubt there will be incredible breakthroughs in the intelligence and capability of machines to assist us. For these new capabilities to reach their potential in tomorrow's devices, they demand a robust platform from which to operate.

Several years ago, Kry10 recognized the limitations of existing operating systems in addressing the unique risks faced by mission-critical connected machines and embarked on a quest to build a novel forward-looking

solution for a connected world. That solution is now ready for today's software-defined machines, and for secure infrastructure solutions for decades to come.

Matched both to today’s customer needs and hardware capability, as well as providing secure infrastructure solutions for decades to come, the Kry10 OS, anchored by the formally verified seL4 microkernel, offers a compelling solution to both mitigate the increasing risks and take advantage of the coming innovations as they develop.

There is a reason why national cyber defense organizations such as DARPA, NCSC and Cyber Agentur are investing heavily in this space.

The Kry10 Solution

Kry10 is building the world’s first "formally proven" operating system and commercializing it globally to build a more secure and interconnected future. The Kry10 solution revolutionizes how machines are safeguarded against cyberattacks. The Kry10 solution comprises several interlocking components to deliver the highest levels of security with unparalleled ease of development and adaptability:

- Kry10 Operating System
- Remote Management Services
- Developer Tools and Support
- Libraries

These components are described in more detail in the following sections.

Kry10 Operating System (KOS)

The Kry10 Operating System is built directly on the seL4 Microkernel. Any system that is not backed by formal methods, as seL4 is, cannot, fundamentally, be considered secure. The KOS leverages and builds on the security of the kernel to deliver a robust OS for todays connected machines:

- Manipulates the capabilities and policies provided by the kernel.
- Loads, recovers, updates, and facilitates communications between the rest of the applications on a machine.
- Uses signed manifests to describe all software, hardware resources used, and communication channels between applications.

Flexibility and Security

Although KOS systems are strongly defined and constrained by rules backed by formally proven policies, these rules are not rigid and brittle like static systems. The built-in management services allow the rules to be updated within the framework of formal policies. Applications cannot take down KOS even in the event of a hard fault. With updates to manifests, however, you can reconfigure a machine while it is running.

Kry10 has patents pending on these techniques. We are now working with governments around the world to extend the proofs to cover the user-mode parts of the operating system.

Familiar Development Tools

New machines and software need to be easy and familiar to build. The Kry10 OS currently supports several application environments, including C, RUST, and Erlang BEAM, and more will be added as needed.

Remote Management Services

With the Kry10 Management Services, you can create resilient systems that can recover from errors and be remotely updated. Devices can communicate in the cloud, be updated, and have remote UI – all within the formally proven framework provided by KOS.

You can run the Kry10 Management Services as a Kry10 cloud hosted multi-tenant SaaS. The services have Azure/AWS marketplace integration for single-tenant clusters or can be delivered as on-prem servers for air-gapped facilities. The combined KOS and management services are built with zero-trust security principles. Updates are only accepted when they are properly signed with cryptographic keys. Even a fully compromised server cannot update machines without proper signatures.

Developer Tools and Support

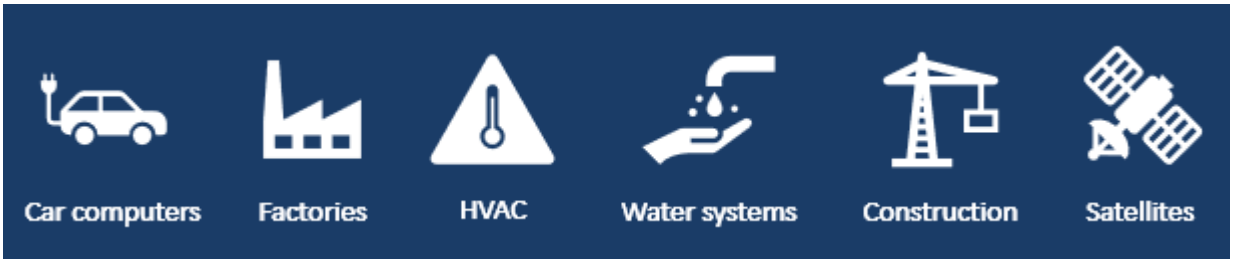
Kry10 provides familiar application runtime environments with great library support. Today that includes musl, RUST, BEAM, partial POSIX, and Linux VMs, with more coming every quarter as we expand our footprint. To bring formal methods into common use, Kry10 believes machines must be easy to build and easy to maintain, and not require deep engineering knowledge.

Libraries

Kry10 has built many drivers for common hardware that can stand up new builds in minutes. This year we are extending this into an app store with reusable libraries of code and source attestation.

Who is it for?

Kry10 was built for organizations developing and maintaining mission critical devices, where trust and security are paramount. It was built to allow you to develop solutions that can adapt and scale without sacrificing security. Solutions that can leverage the innovations that are happening now, and those to come. The Kry10 solution was made for industries such as automotive, aviation, autonomous and semi-autonomous vehicles, energy grids, telecommunications infrastructure, medical devices, industrial control systems, and more.



Work with Kry10

After 5 years of development, Kry10 has a working 1.0 version of these products, including extensive developer documentation. Kry10 remains in technical stealth working largely with national cyber agencies in the US, UK, Germany, and Australia/New Zealand to build evidence for the industry and work on certification. Kry10 software and developer documentation is available to early partners based on an NDA. Please reach out for a meeting if you want to partner with us on building a resilient and secure future.

Ngā mihi (Thank you!)

Boyd Multerer - CEO Kry10