

How the Erlang Ecosystem is Leaning Into Better Cybersecurity

Kiko Fernandez-Reyes & Alistair Woodman.
Erlang Ecosystem Foundation.
(EEF) (erlef.org)



Agenda

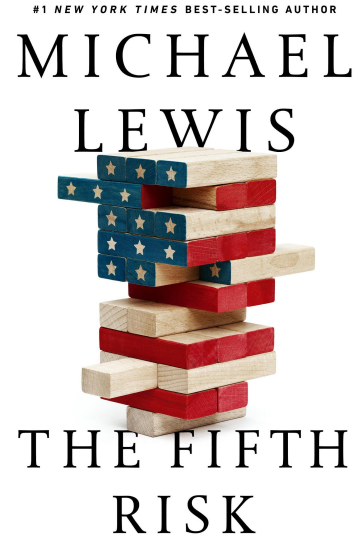
- Indirection #1: Michael Lewis; Renowned Author
- Indirection #2: Christopher Mark;
A Service to America Medals® honoree
- Indirection #3: Coal Mine Safety
- Importance of Erlang & BEAM
- EEF's Plans

The Fifth Risk (2018)

...John MacWilliams, a risk management expert at the United States Department of Energy (DoE) from the Obama Administration, gave Michael Lewis the top five risks he saw for the department:

- 1) Broken arrows (loose nukes and nuclear accidents),
- 2) North Korean nuclear weapons,
- 3) An end to the Iran nuclear deal,
- 4) Protecting the electrical grid from cyberterrorism, and
- 5) ***Internal project management.***

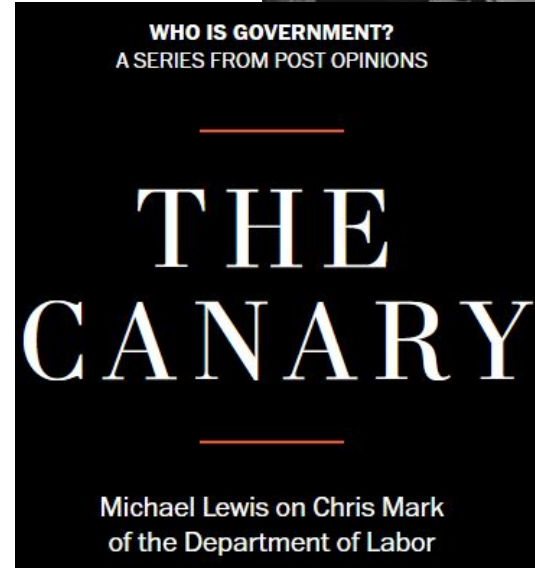
It is this ***fifth*** risk that inspired the title of the book.



Recent Washington Post Opinion Series

- 1) As a result of writing *The Fifth Risk*, Michael Lewis and the Washington Post decided to run a series of articles about “Unsung Heroes” in the Federal Government.
- 2) One of the first, published on September 3rd 2024, covers Chris Mark and his work over the last 50 years to improve mine safety...

<https://www.washingtonpost.com/opinions/interactive/2024/michael-lewis-chris-marks-the-canary-who-is-government/>





The 'Sammie' Awards

- 1) Christopher Mark
- 2) 2024 Lifetime achievement honoree
- 3) ...Over a decades-long career, Mark developed computer software packages that contain guidelines routinely used by mine operators to develop and evaluate mining plans for most underground coal mines in the U.S. A world-renowned expert, he's credited with saving an untold number of miners' lives.

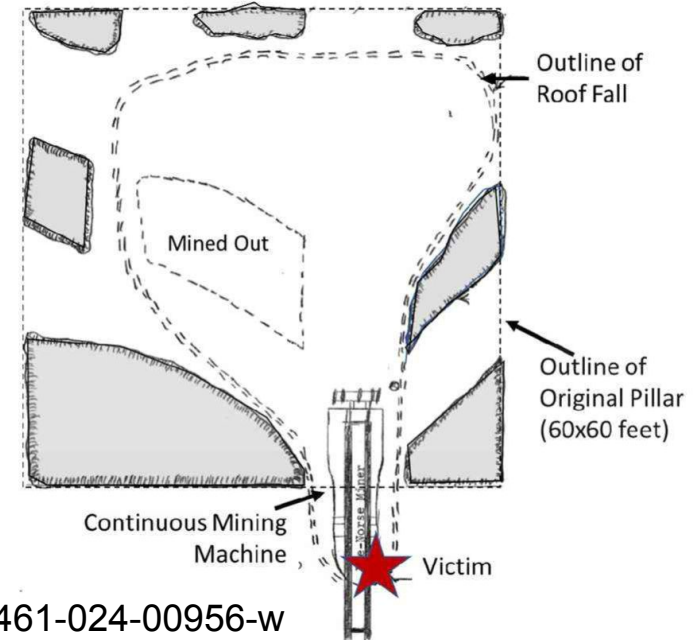
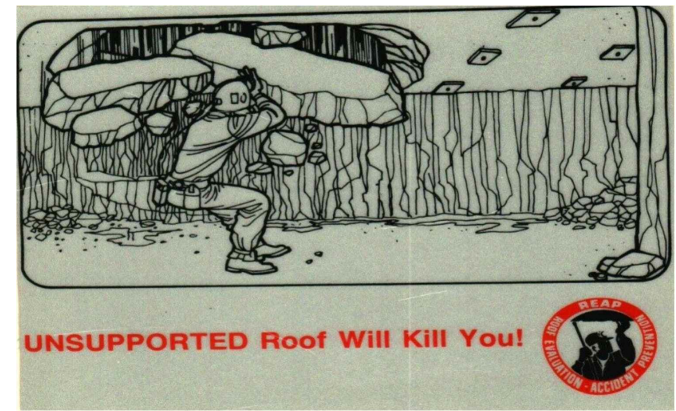


The Road to Zero: The 50-Year Effort to Eliminate Roof Fall Fatalities from US Underground Coal Mines

- Six decades ago, the **most dangerous job in the USA was mining coal underground**. Roof falls were responsible for half of the deaths, killing about 100 miners every year. **Fast forward to 2016 and zero roof fall fatalities**. Just three miners were killed by roof falls during the following 6 years. How did the mining community achieve this historic goal?
- This paper starts by analyzing the roof fall fatalities in 1968, categorizing them by their fundamental cause. Then, it shows how each type of roof fall was reduced over time, using snapshots of the fatalities occurring in subsequent decades. Along the way, it evaluates the influence of the regulatory environment, changing mining methods, and better ground control technology.
- The study found that in 1968 **more than half of roof fall fatalities at large mines were attributable to an inadequate safety culture**. The immediate effect of the 1969 Coal Mine Health and Safety Act was to reduce the riskiest activities, like needlessly going under unsupported roof. Other hazards, like large roof falls, required technological developments before they were brought under control. Roof Control Plans, which the US Bureau of Mines had been advocating since the 1920s, played a significant role throughout the process.

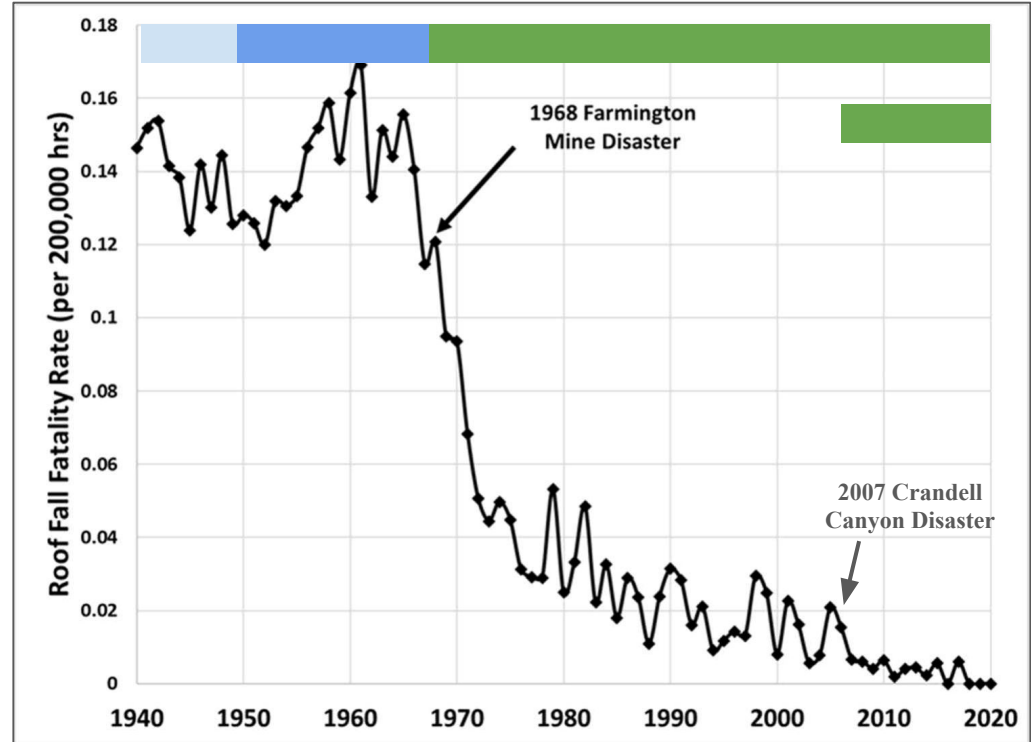
Pictures worth 1K words...

Roof Falls



Fatality Rates in US Coal Mines

- 1940s Switch to Roof Bolting started
- 1950s Almost full conversion to Roof Bolting
- Late 1950s and early 1960s fatality rates worsen slightly
- 1968 Disaster & Hearing
- 1969 Enforcement allowed
- 2007 Disaster & Oversight
- 2016 first year with no deaths



Summary

- 1) ***Appropriate*** legislation brings benefits that were omitted by the market or present behavior.
- 2) If you are doing things competently, not much need to worry
- 3) If you were not, then start to work towards better cyber security

Importance of Erlang & BEAM VM

Functional programming language

Distributed programming

Concurrent & Parallel

Fault-tolerant

On-the-fly updates

Soft real-time constraints



Importance of Erlang & BEAM

Do you like to do **phone calls**?

Do you like to use **Klarna**?

Do you **receive official mail** via Kivra?

What about **chatting** on WhatsApp?

Do you play **games**?

Do you like the **internet**?



Importance of Erlang & BEAM

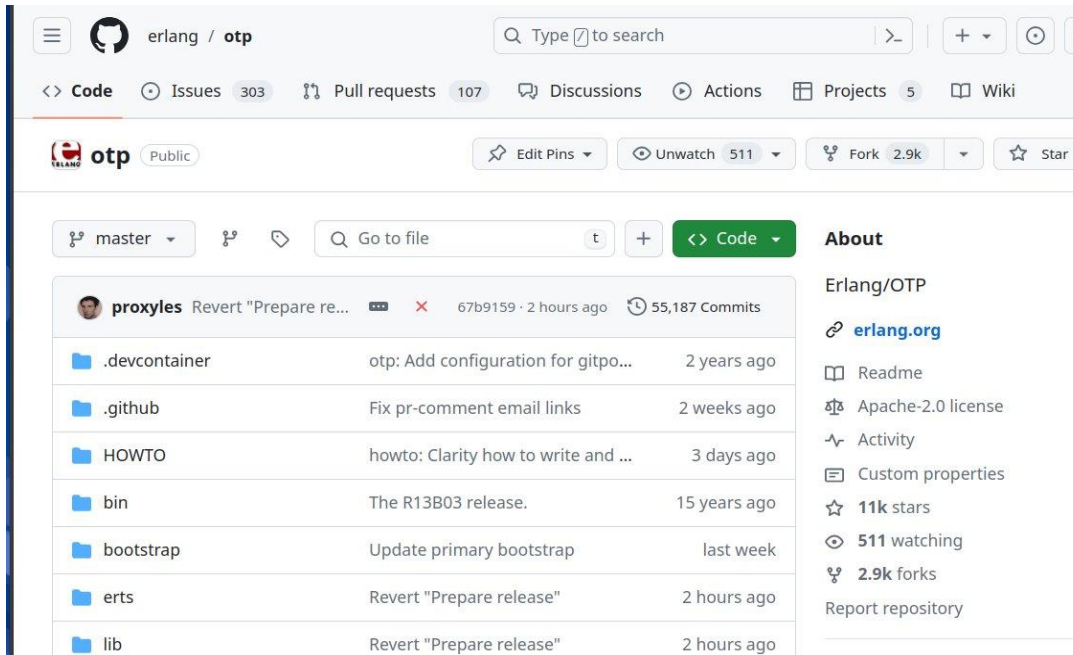
Issues: 2500+

PRs: 3263

Battle-tested by WhatsApp, Klarna, Cisco, Riot Games, Pinterest, etc

Community around Erlang

- Detection of issues
- Contributions with Pull Requests:
 - Documentation fixes
 - Improvements to libraries
 - Bug fixes



Importance of Erlang & BEAM

Klarna: EEP and PR for map-comprehension

Klarna: implement Draft-06 of JSON schema validation

99s: HTTP/2 and REST API libraries

AdRoll: Dead-code removal

VMWare: message broker RabbitMQ

WhatsApp: json, eqWAlizer type system, incremental mode to Dialyzer (x7 speedup)

Plataformatec: Elixir language

...

Importance of BEAM

- Erlang Workshop
- Code Europe
- Code AMERICA
- Code BEAM SF



🏠 ICFP 2024 (series) / Erlang 2024 (series) /

Erlang 2024

[About](#)

[Call for Lightning Talks](#)

[Call for Papers](#)

Call for Papers

Overview

The Erlang Workshop aims to bring together the open source, academic, and industrial communities of **Erlang, other BEAM-related languages, actor model programming, distribution, and concurrency** to discuss techniques, technologies, languages and other relevant topics. The Erlang model of concurrent programming has been widely emulated, for example by Akka in Scala. Moreover, several newer programming languages, such as Elixir, have been designed atop Erlang's VM. The workshop is welcoming contributions related to any and all systems like those mentioned above.

The workshop aims to enable participants to learn about recent developments on techniques and tools, novel applications, draw lessons from users' experiences and identify research problems and common areas relevant to the practice of Erlang and other Erlang-like languages, functional programming, actor model programming, distribution, concurrency, etc.

Important Dates

🕒 AoE (UTC)

Thu 30 May 2024
Submission Deadline

Thu 27 Jun 2024
Notification

Thu 18 Jul 2024
Camera Ready

Organizing Committee

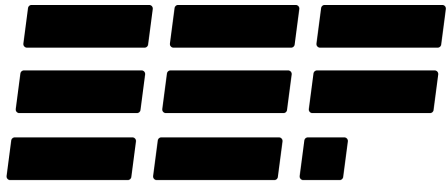
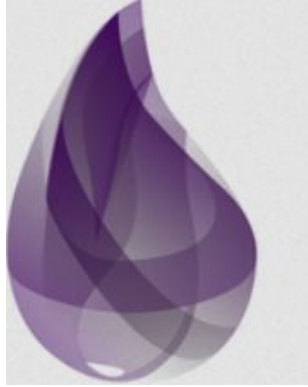


Kiko Fernandez-Reyes
Ericsson, Sweden
Sweden



Adriana Laura Voinea

Who are the Erlang Ecosystem Foundation (EEF) ?



**ERLANG ECOSYSTEM
FOUNDATION**



- 1) California registered 501(c)3 (similar to gGmbH)
- 2) Founded in 2019
- 3) Membership Organization (Nominal yearly dues)
- 4) Funded mostly by Company Sponsors
- 5) The BEAM VM supports:
 - a) Erlang
 - b) Elixir
 - c) Gleam
 - d) Lua
 - e) Lisp

Summary of CRA

1) LFE Broadcasting

2) Yesterday's Presentations

Manufacturers: Software updates, support period

- Manufacturers **must supply vulnerability fixes** throughout the support period
- Products should be **designed to support software updates**, especially for consumer products, ideally automated
- End of support must be communicated on the device without restricting the functionality available to the user
- **Security updates** must be **provided separately** from functionality updates
- Support period should be **no less than 5 years**
- ..., unless the product has a shorter lifetime
- ..., or more if a **longer lifetime** can be reasonably expected

EU Cyber Resilience Act

The EU acts to strengthen the approach to cybersecurity regulation at union level. The CRA aims to achieve 3 policy goals:

- To **reduce vulnerabilities** in digital products,
- To ensure cybersecurity is **maintained** throughout a **product's life cycle** and
- To **enable users** to **make informed decisions** when selecting and operating digital products

The CRA establishes **horizontal mandatory cyber-security requirements** for all digital products, software and/or hardware.

The EU intends to play a **leading international role** in cybersecurity regulation.

Responsibilities of Open Source Software Stewards*

- The legal entity is the open source software steward
- Stewards should
 - Have a single point of contact for reporting and inquiring about vulnerabilities: <https://www.linuxfoundation.org/security>
 - Implement a cybersecurity policy and communicate it widely
 - Cooperate with market surveillance authorities on their request
 - Notify widely about reported vulnerabilities
- Governance reports should document the non-profit character of the organization

* tentative, preliminary, not final

<https://www.youtube.com/watch?v=uOk4WIFddsc>

Possible outcomes of the CRA...

- 1) The EU CRA standards & policies will be too harsh and the law becomes a dead letter.
- 2) The costs for many of the small O/S players become too large and the O/S big players take over.
- 3) Somehow the supply chain and open-source projects adjusts to support CE marks. Commercial Open-Source projects will need better mechanisms of capturing funding for the value they create... Any Suggestions ?

What the EEF plans to do

- 1) Increase engagement with Civil Society organizations
- 2) Increase engagement with Vertical and Horizontal Industry organizations
- 3) Provide educational outreach inside our own community
- 4) Raise funding
- 5) Develop compliance processes and tools to pass the new EU and US standards



Standards and Processes we will focus on

- 1) OpenChain Project Compliance
- 2) NIST's SSDF
- 3) SBOM support
 - 1) SPDX and
 - 2) CycloneDX
- 4) Static tooling of known BEAM vulnerabilities
(automated checking of EEF Security group guidelines)
- 5) CI/CD tooling, monitoring CVEs and vulnerabilities

OpenChain Project Compliance

- OpenChain ISO/IEC 5230:2020 helps organizations manage open source licensing requirements for past, current and future products or services

Q: How do I trust my open source supply chain?

- OpenChain Security Assurance Specification (ISO/IEC DIS 18974:2023)

OpenChain Project Compliance (ISO/IEC DIS 18974)

4.1.5 Standard practice implementation

The program shall demonstrate sound and robust handling procedures of supplied software;
Method to identify structural and technical threats to the supplied software;
Methods for detecting existence of known vulnerabilities in supplied software;
following procedures:
Method for following up on identified known vulnerabilities;

- Method for **analyzing supplied software** for newly published known vulnerabilities post release of the supplied software;

OpenSSF Scorecard:

Assesses open source projects for security risks through a series of automated checks

WIP Static detection of known vulnerabilities
per EEF security group guidelines

OpenChain Project Compliance (ISO/IEC DIS 18974)

4.1.5 Standard practice implementation

- Method for **continuous and repeated security testing** to be applied for all supplied software before release;
- Method to **verify that identified risks will have been addressed** before release of supplied software;
- Method to **export information about identified risks** to third parties as appropriate.

Erlang Ecosystem Foundation will focus on:

- CI/CD tooling, monitoring CVEs, and vulnerabilities

OSV: A distributed vulnerability
database for Open Source

OpenChain Project Compliance (ISO/IEC DIS 18974)

4.3 Open source software content review and approval

4.3.1 Software bill of materials

A process shall exist for **creating and maintaining a bill of materials** that includes each open source software component from which the supplied software is comprised.

Erlang Ecosystem Foundation will focus on:

- Automatic Creation of SBOM (Soft. Bill of Materials)



ERLANG ECOSYSTEM
FOUNDATION

Develop compliance processes and tools

- 1) C/C++ Compiler options
- 2) Safe Erlang/Elixir/BEAM compiler and security defaults

We cannot forbid all unsafe behaviour,
but you can opt-in to unsafe behaviour

- 3) Existing NIFs may remain in C/C++, new NIFs should be written in memory safe languages (e.g., Rust, Ada, etc)

Long-term Plans & Academic Collaborations

- 1) Improving static tooling to detect more typing errors
Erlang/OTP team interacts with developers of type systems to improve the number of tools that work on Erlang (eqWAlizer, etylizer, gradualizer)
- 2) Compiler Verification Efforts to verify that compilation optimisations are semantics preserving
- 3) Security and energy efficiency

Closing Remarks

- Erlang Ecosystem Foundation as open source steward
- Erlang (BEAM) is:
 - EU language, created in Sweden,
 - Open source,
 - Ericsson has a team that maintains it
 - Critical to the Swedish infrastructure
 - Banking (Klarna)
 - Telecommunications (Ericsson, CISCO, Telia, etc)
 - Message industry (WhatsApp, Kivra, etc)
- EEF will guide efforts to be CRA compliant