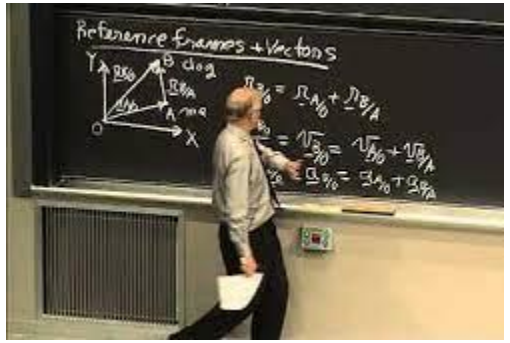
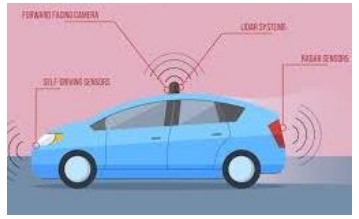
Massachusetts Institute of Technology

STAMP/STPA 2024 Virtual Workshop



Our current safety tools are all 50-75 years old but our technology is very different today



1940 1950 1960 1970 1980 1990 2000 2010 2020

FMEA

FTA HAZOP ETA

STPA

- Introduction of computer control
- Exponential increases in complexity
- New technology
- Changes in human roles

Assume accidents caused by component failures

Causes??

New Causes of Accidents

- No longer just the result of component failures
- More likely to result from requirements and design flaws, unfettered complexity, unknown unknowns.
- Accidents increasingly the result of interactions among components that have not failed or even malfunctioned.

STAMP: Safety Based on System Theory

- Complexity is reaching a new level (tipping point)
  - Old safety approaches becoming less effective
  - New causes of losses appearing (especially related to use of software and autonomy)

- Traditional analysis approaches do not provide the information necessary to prevent losses in these systems

- Need a paradigm change to “Systems Theory”

  Change focus

  ~~Increase component reliability (prevent failures)~~

  Enforce safe system behavior (constraints on system behavior)

STAMP: Safety Based on Systems Theory(2)

- Allows creating new analysis and engineering approaches
  - More powerful and inclusive
  - Orders of magnitude less expensive
  - Work on extremely complex systems (top-down system engineering)

- New paradigm works much better than old techniques:
  - Empirical evaluations and controlled studies show it finds more causal scenarios (the “unknown unknowns”)
  - Can be used before a detailed design exists to design safe and secure systems from the beginning

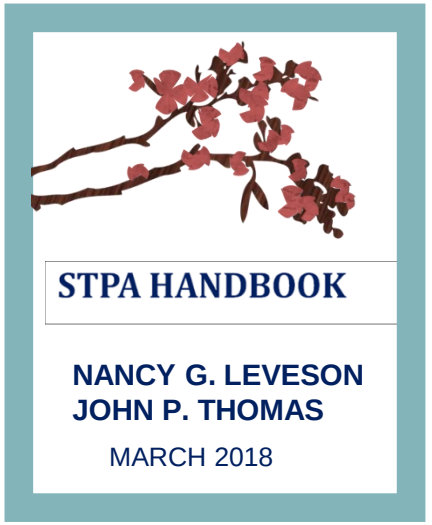
General Definition of “Safety”

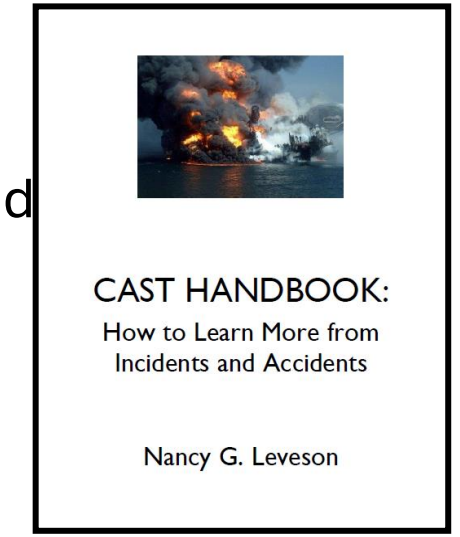
Accident = Mishap = Loss: Any undesired and unplanned event that results in a loss

- Loss of human life or injury
- Property damage,
- Environmental pollution,
- Mission loss,
- Loss of protected information (security),
- Negative business impact (damage to reputation, etc.), etc.

Handbook News

- STPA Handbook (Thomas and Leveson)
  - 364,652 downloads
  - Japanese version (24,937 downloads)
  - Chinese version (57,762 downloads)
  - Korean version (number not collected)
- CAST Handbook (Leveson)
  - 95,310
  - Korean and Japanese versions (not collected
- CAST for Healthcare (Leveson) - new



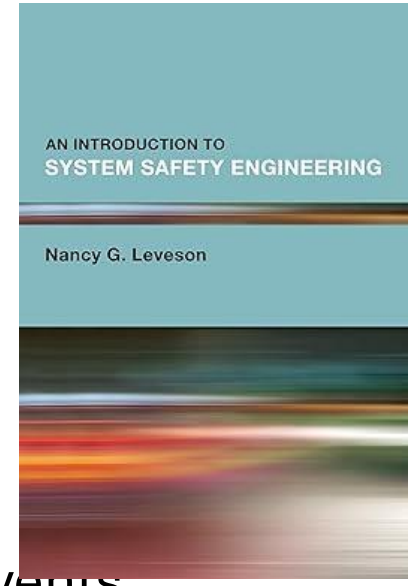


Book News

- Safeware has gone out of print (obsolete anyway)
- New book “Introduction to System Safety Engineering”
  - Published by MIT Press in November, 2023 (second printing)
  - Textbook format (exercises, teaching materials for instructors)
  - General textbook, not a replacement for Engineering a Safer World
  - Being translated by volunteers into Japanese and Chinese (not available for a while)

Contents of New Book

1. Historical and industrial perspectives on safety engineering
2. Risk in modern society
3. Fundamental concepts and definitions
4. Why accidents occur
5. The role of software in safety
6. The role of humans in safety
7. Accident causality models
8. Accident causality analysis and learning from events
9. Hazard Analysis: Basic Concepts
10. Hazard analysis techniques



Contents of New Book (2)

11. Design for safety
12. Human factors in designing for safety
13. Assurance, assessment, and certification
14. Designing a safety management system

Epilogue: Looking forward

Appendix A: Medical Devices: The Therac-25

Appendix B: Space: Challenger and Columbia

Appendix C: Petrochemicals: Flixborough, Seveso, Bhopal, Texas City, Macondo (Deepwater Horizon)

Appendix D: Nuclear Power: Three Mile Island, Chernobyl, Fukushima Daiichi

Recent Student Research

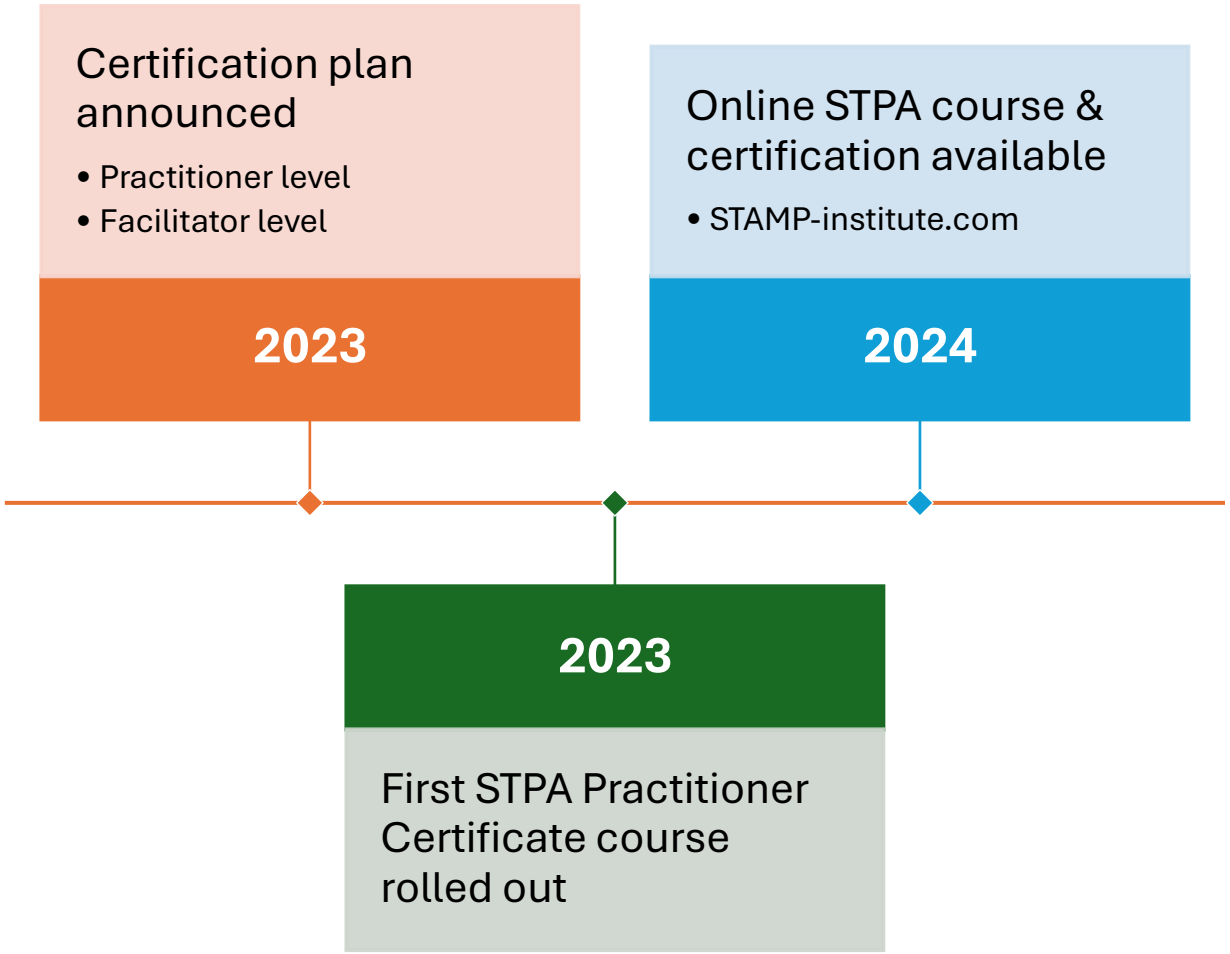
- Andrew Kopeikin, STPA *of Collaborative Multi-Controller Teams*
- John Barstow, *Applying STPA to Work Movement in Production Systems*
- Andrew (Andy) Canady, *Safety in U.S. Navy Navigation: Applying STAMP Processes to Surface Ship Collisions*.
- Brittany Bishop, *STPA of a Novel Airborne Laser Communications System*
- Rodrigo Lopes Rose, *Limitations of Commercial Aviation Safety Assessment Standards in the Wake of the Boeing 737 MAX Accidents*
- Noem Eisen, *STPA as a Practical Tool for Comprehensive Flight Test Analysis*

urrent Student Research

- Alex Hillman, *The Engineering of Assumptions: A Systems-Theoretic Approach to Design Qualification for Novel, Complex Systems*
- Justin Poh, *Systems-Theoretic Architecture Development Framework (case study: integrating UAM into NAS)*
- Polly Harrington, Applying STPA to Sociotechnical Systems
- Braden Brower, Indicators of Destructive Behavior Onboard Naval Surface Vessels
- Natalie Basnight, STPA in Novel Military Rotorcraft
- Lauren Gutierrez, Systems-Theoretic Organizational Design & Analysis

Online classes and certification

Online STPA Training and Certification



For more info: Email jthomas4@mit.edu

STPA & CAST Handbook Downloads

Handbook Downloads (as of June 2024)

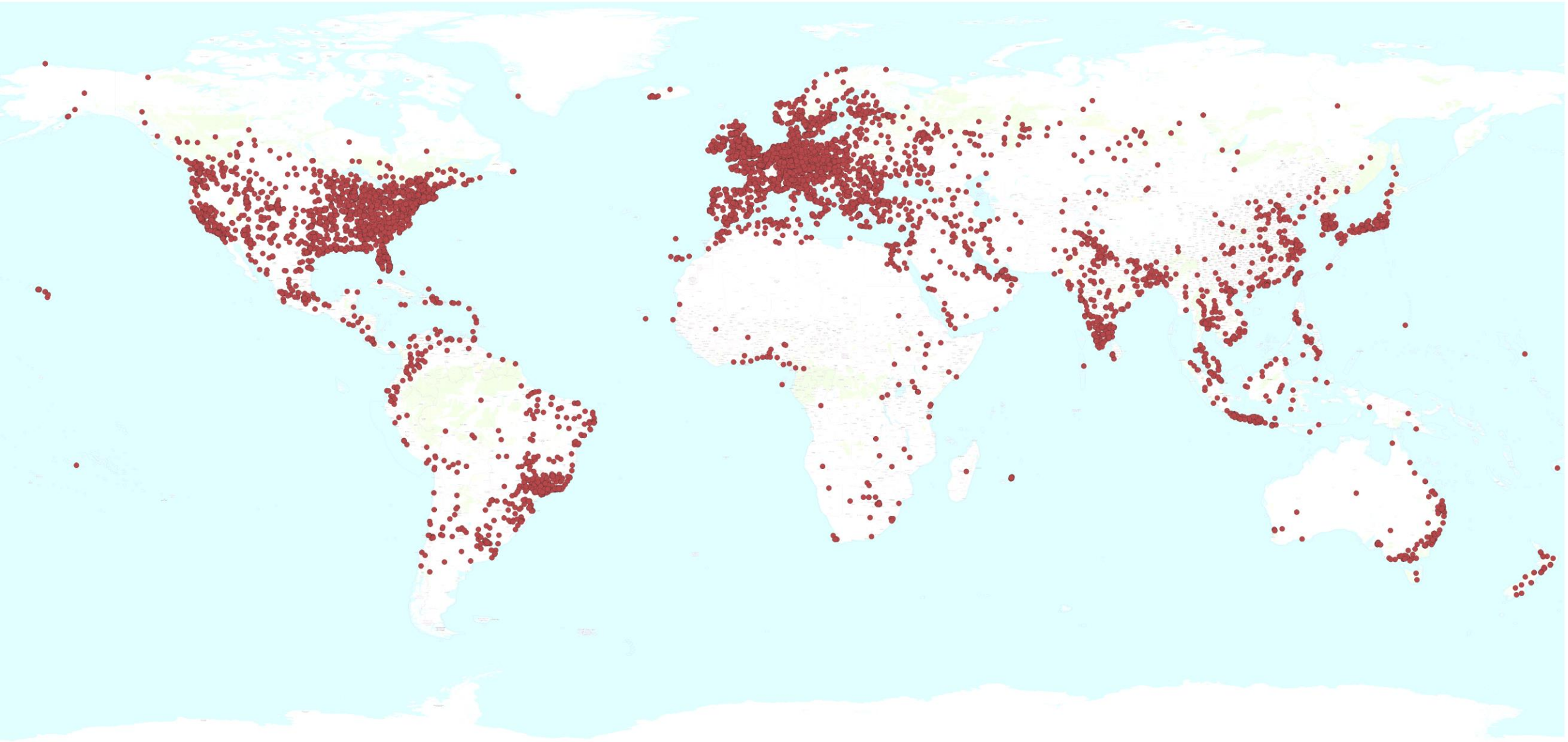
- STPA Handbook
  - English: 348,388
  - Japanese: 23,037
  - Chinese: 56,492
  - Korean: (No Info)
  - English-Korean: (No Info)

- CAST Handbook
  - English: 94,084
  - Korean: (No Info)
  - English-Korean: (No Info)
  - Japanese: (No Info)
  - English, for Healthcare: (No Info)

Total: >500,000 (that we know of)

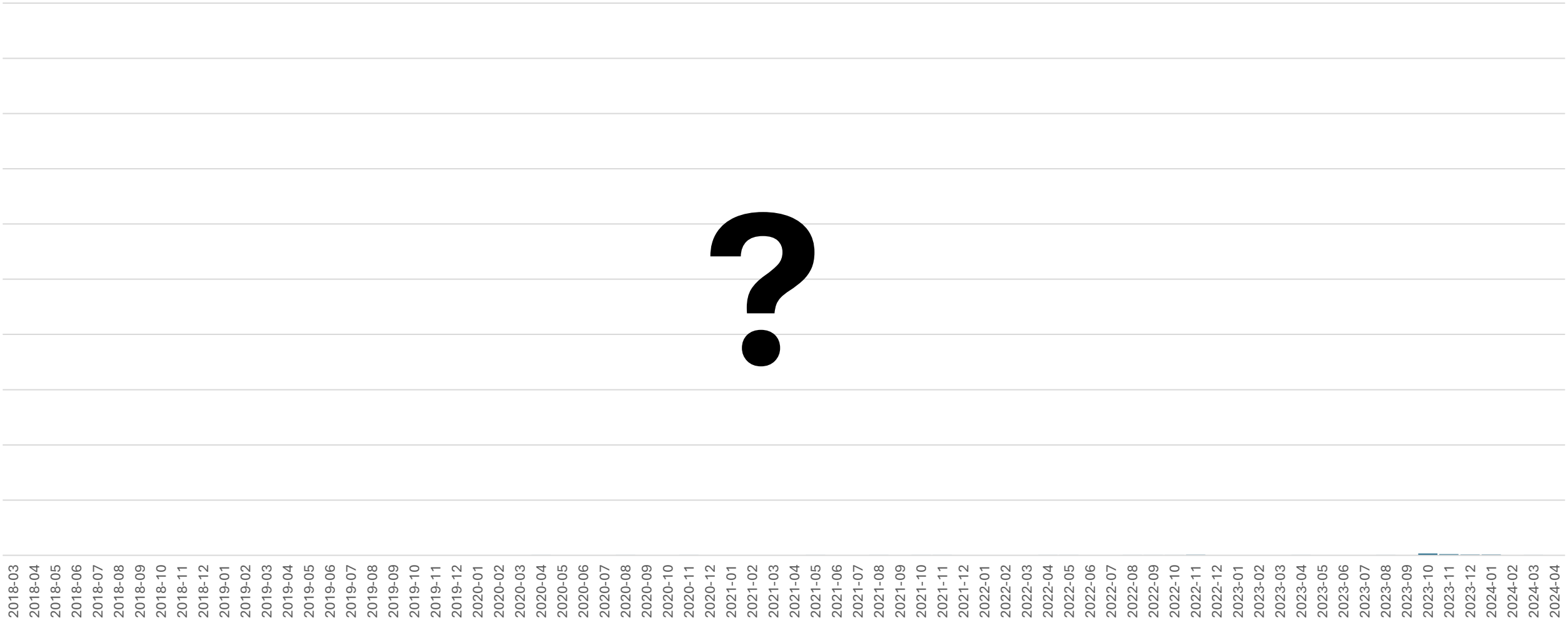
Who is downloading these?

STPA Handbook Downloads (English)

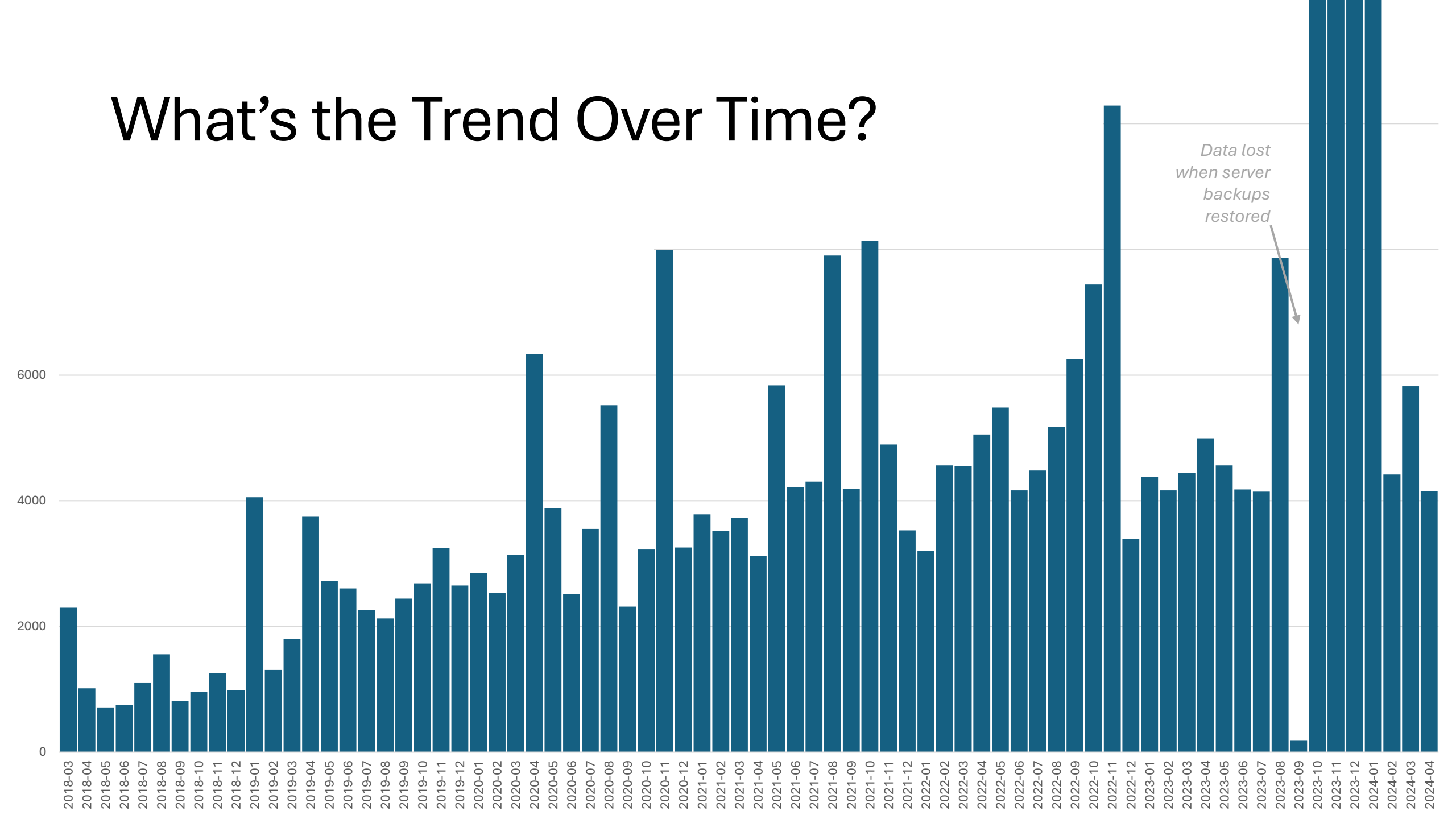


N~=350,000

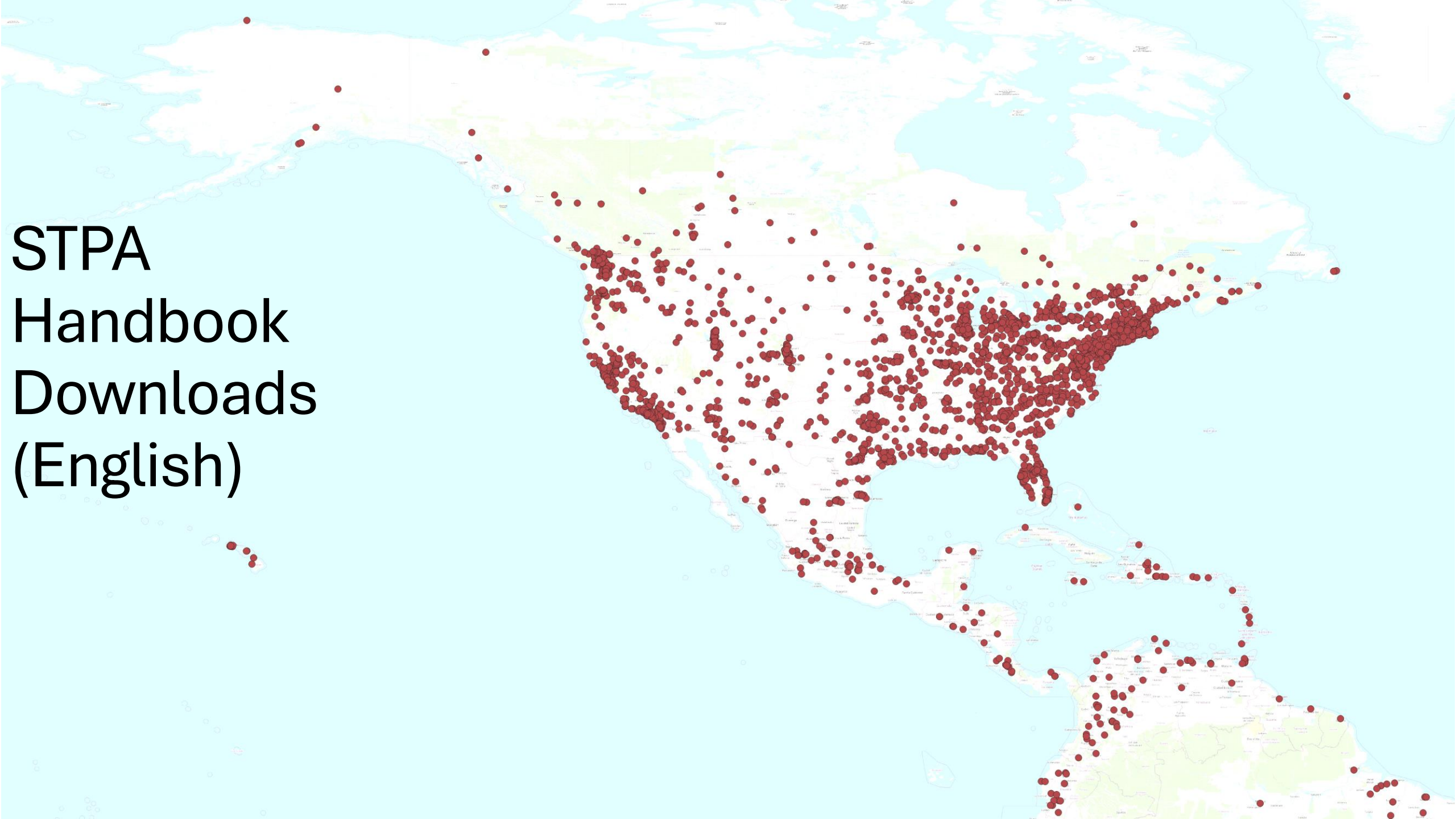
What’s the Trend Over Time?

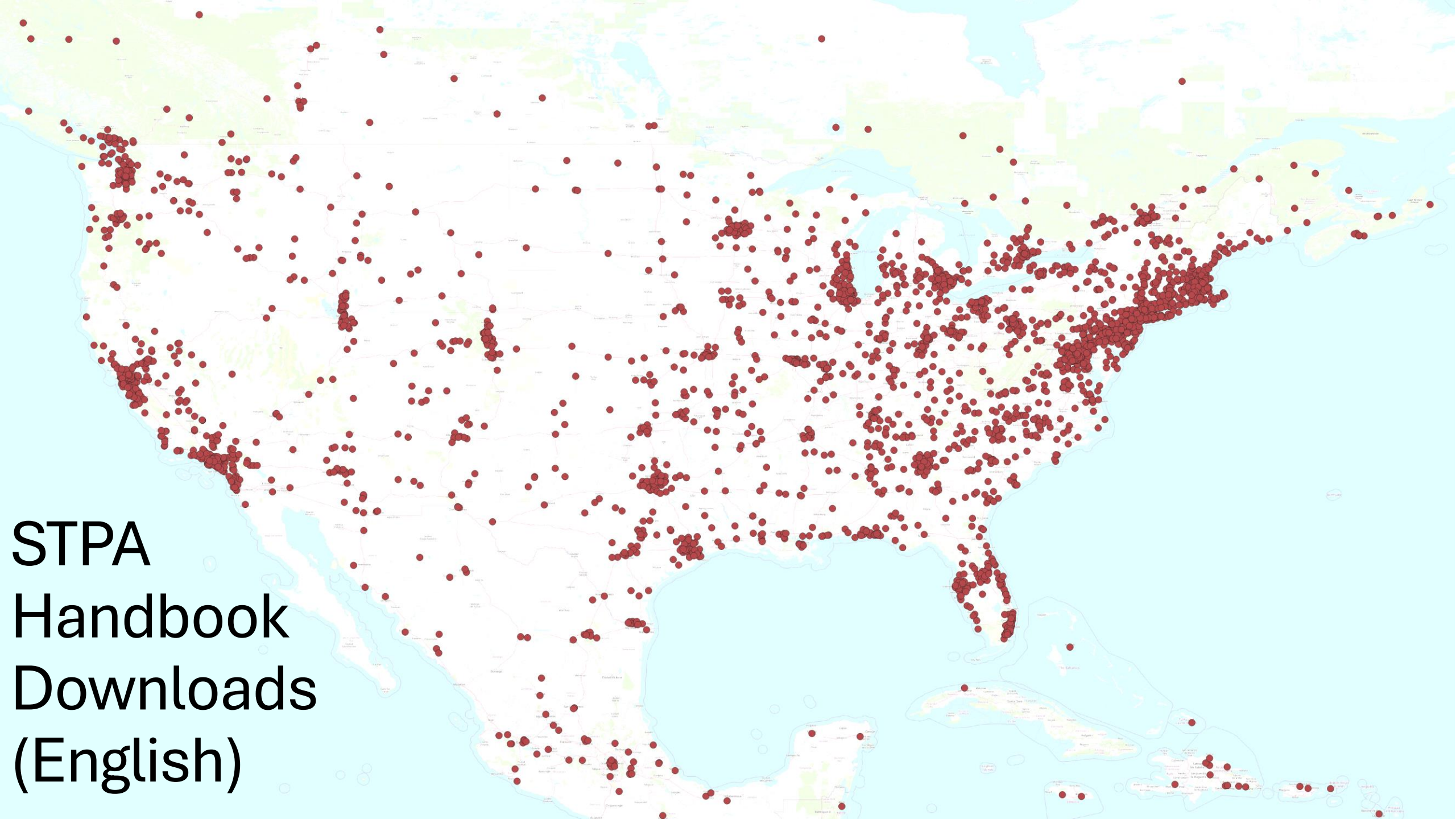


What's the Trend Over Time?



STPA Handbook Downloads (English)

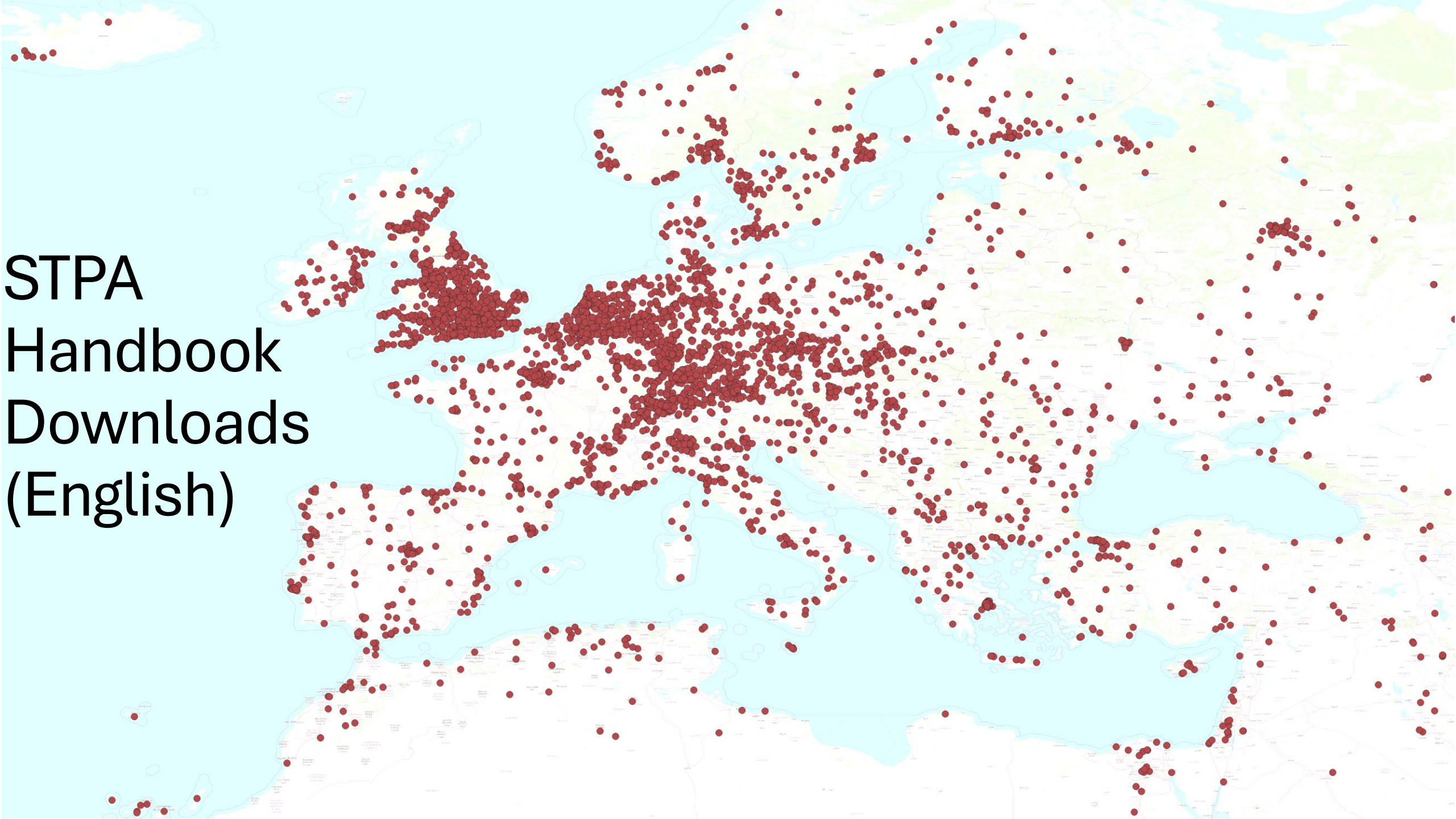


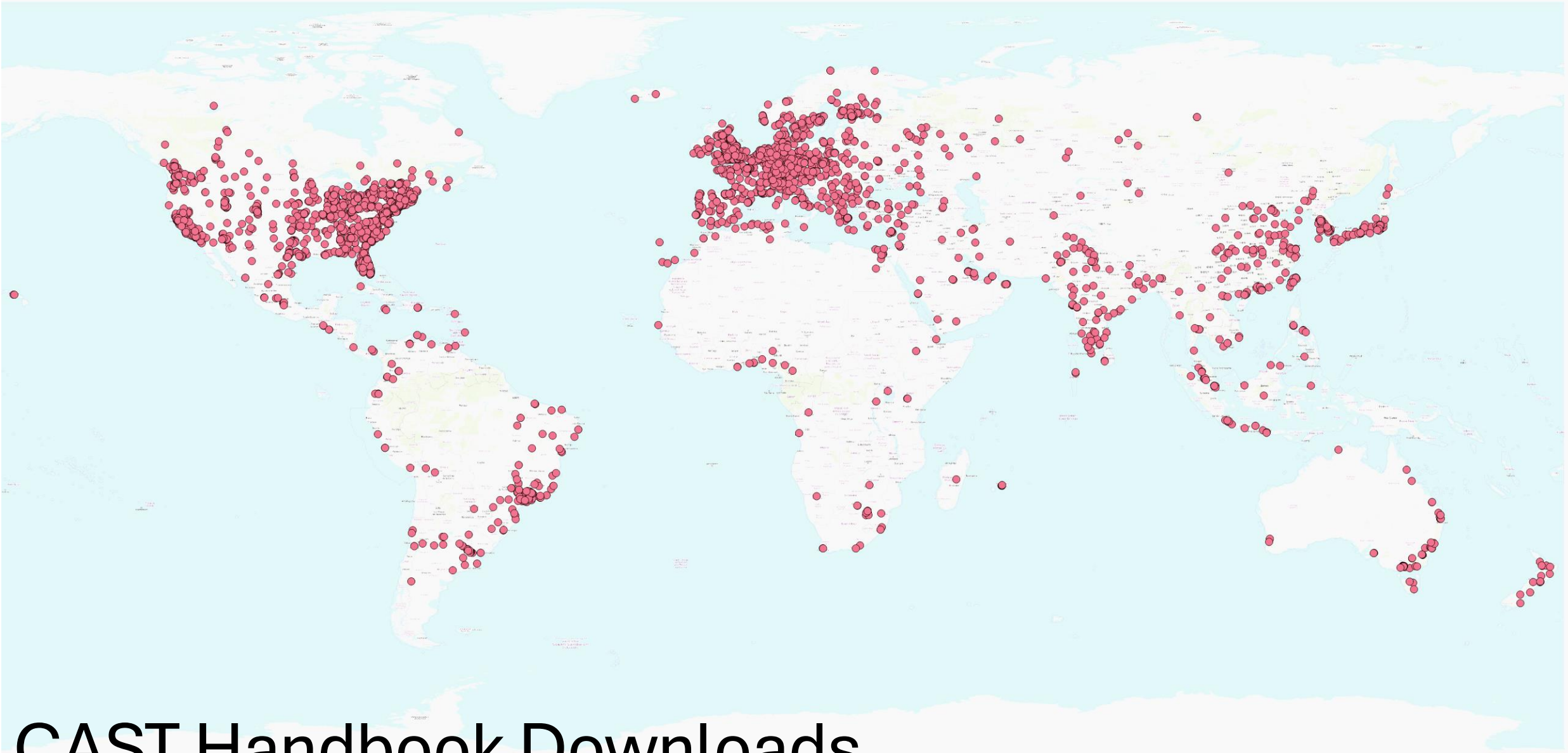

STPA
Handbook
Downloads
(English)

STPA Handbook Downloads (English)

STPA Handbook Downloads (English)

STPA Handbook Downloads (English)





CAST Handbook Downloads