

At the Seams — Why Systems Fail Where They Meet

รอยต่อ — เหตุใดระบบจึงพังตรงที่มันมาบรรจบกัน

Complex systems rarely fail at their centres. They fail at their boundaries, where two correct parts meet under assumptions neither of them wrote down and neither of them owns. Reliability is therefore a property of interfaces, and safety is a control problem rather than a component problem.

A I C E

Contents

- 1 01. The Seam — Why Failure Concentrates Where Parts Meet
- 2 02. Units and Assumptions — The Mismatch Nobody Owns
- 3 03. The Handoff — Where Information Goes to Die
- 4 04. Protocol Drift — When Two Sides Disagree About the Contract
- 5 05. Timeouts and Retries — The Cure That Causes the Disease
- 6 06. The Silent Success — Failure That Reports Everything Is Fine
- 7 07. Latent Conditions — Accidents That Were Already There
- 8 08. The Blame Reflex — Why 'Human Error' Ends the Inquiry
- 9 09. The Postmortem — Turning an Outage Into an Asset
- 10 10. Resilience Engineering — Work as Imagined and Work as Done
- 11 11. Control, Not Components — Leveson's Reframing
- 12 12. Finding Your Own Seams — The Procedure

01. The Seam — Why Failure Concentrates Where Parts Meet

The Anatomy of a Normal Accident

กายวิภาคของอุบัติเหตุปกติ

Sociologist Charles Perrow, working at Yale, proposed that accidents in complex, tightly-coupled systems are an inevitable property of the system structure rather than individual component unreliability. He examined the Three Mile Island Unit 2 disaster of 1979 to demonstrate that four independent, individually minor failures combined to produce a catastrophic system outcome. These failures included stuck feedwater valves left shut after maintenance, a relief valve stuck open, and a control-room indicator that reported the commanded state rather than position. Perrow argued that interactive complexity and tight coupling leave no slack to absorb the interactions, making some accidents structurally unavoidable regardless of the quality of components. This measurement of the 1979 incident suggests that the reliability of a single part provides no predictive power for the overall safety of the entire system.

ในระบบที่ซับซ้อนและผูกกันแน่น อุบัติเหตุเป็นคุณสมบัติของโครงสร้างระบบเอง ไม่ใช่ความไม่น่าเชื่อถือของชิ้นส่วนใดชิ้นหนึ่ง นี่คือข้อเสนอของ Charles Perrow นักสังคมวิทยาแห่ง Yale เขาใช้ภัยพิบัติ Three Mile Island Unit 2 ปี 1979 เป็นหลักฐานความล้มเหลวเล็กน้อย 4 อย่างที่เป็นอิสระต่อกัน รวมกันแล้วพาทั้งระบบไปสู่หายนะ วาล์วน้ำป้อนติดค้างในสถานะปิดหลังซ่อมบำรุง วาล์วระบายแรงดันค้างอยู่ในสถานะเปิด และตัวบ่งชี้ในห้องควบคุมแสดงสถานะที่ส่งไป ไม่ใช่ตำแหน่งจริงของวาล์ว Perrow ให้เหตุผลว่าความซับซ้อนเชิงปฏิสัมพันธ์บวกกับการผูกกันแน่นทำให้ระบบไม่เหลือช่องว่างไว้รองรับปฏิสัมพันธ์เหล่านั้น อุบัติเหตุบางอย่างจึงหลีกเลี่ยงไม่ได้ในเชิงโครงสร้าง ไม่ว่าชิ้นส่วนจะมีคุณภาพดีเพียงใด ผลการวัดเหตุการณ์ปี 1979 นี้บอกว่า ความน่าเชื่อถือของชิ้นส่วนเดียวทำนายความปลอดภัยโดยรวมของทั้งระบบไม่ได้เลย

The Seam as a Unit of Analysis

รอยต่อในฐานะหน่วยของการวิเคราะห์

The seam represents the boundary where two correct parts meet under assumptions neither party wrote down, a concept explored in Perrow's 1984 book, "Normal Accidents: Living with High-Risk Technologies". In the 1979 Three Mile Island Unit 2 case, the failure was not rooted in the core function of any single valve, but in their unexpected, non-linear interactions. By shifting the unit of analysis from the component to the seam, we reframe safety as a control problem rather than a mere exercise in component maintenance. When systems are tightly coupled, the interface becomes the primary site of failure because no individual engineer owns the assumptions governing the interaction of those parts. This perspective, supported by the 2001 analysis by Andrew Hopkins in the Journal of Contingencies and Crisis Management, forces a move away from simple component-level reliability metrics.

รอยต่อคือขอบเขตที่ชิ้นส่วนสองชิ้นซึ่งต่างก็ถูกต้องมาบรรจบกัน ภายใต้ข้อสมมติที่ไม่มีฝ่ายใดเขียนบันทึกไว้ Perrow สำรวจแนวคิดนี้ไว้ในหนังสือปี 1984 เรื่อง "Normal Accidents: Living with High-Risk Technologies" ที่ Three Mile Island Unit 2 ปี 1979 ความล้มเหลวไม่ได้อยู่ในหน้าที่หลักของวาล์วตัวใดตัวหนึ่ง มันอยู่ในปฏิสัมพันธ์ระหว่างวาล์วเหล่านั้น ที่ไม่มีใครคาดคิดและไม่เป็นเส้นตรง ย้ายหน่วยของการวิเคราะห์จากชิ้นส่วนมาที่รอยต่อ ความปลอดภัยก็กลายเป็นปัญหาด้านการควบคุม ไม่ใช่แค่งานซ่อมบำรุงชิ้นส่วน เมื่อระบบผูกกันแน่น จุดเชื่อมต่อจะกลายเป็นตำแหน่งหลักที่ความล้มเหลวเกิด เพราะไม่มีวิศวกรคนใดเป็นเจ้าของข้อสมมติที่กำกับปฏิสัมพันธ์ระหว่างชิ้นส่วนเหล่านั้น มุมมองนี้บีบให้ต้องเลิกวัดความน่าเชื่อถือแบบง่าย ๆ ในระดับชิ้นส่วน การวิเคราะห์ปี 2001 ของ Andrew Hopkins ในวารสาร Journal of Contingencies and Crisis Management สนับสนุนมุมมองเดียวกัน

The Limits of Competitive Theory

ขีดจำกัดของทฤษฎีคู่ขนาน

The validity of Normal Accident Theory is contested by the High-Reliability-Organization camp, led by researchers such as La Porte and Roberts, who argue for different organizational outcomes. Scott D. Sagan, in his 1993 study "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons", competitively tested these theories against Cold War nuclear-command case studies. Sagan found that Perrow's pessimism was largely borne out, citing near-misses during the Cuban Missile Crisis that were attributed more to luck than to rigorous organizational design.

ทฤษฎี Normal Accident Theory ยังถูกโต้แย้ง ฝ่ายที่ได้คือกลุ่ม High-Reliability-Organization นำโดยนักวิจัยอย่าง La Porte และ Roberts ที่ยืนยันว่าองค์กรให้ผลลัพธ์ต่างออกไปได้ Scott D. Sagan นำทฤษฎีสองฝั่งนี้มาทดสอบแข่งกันกับกรณีศึกษาการสั่งการนิวเคลียร์ในช่วงสงครามเย็น ในงานศึกษาปี 1993 เรื่อง "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons" ผลคือมุมมองในแง่ร้ายของ Perrow เป็นจริงเป็นส่วนใหญ่ Sagan ยกเหตุการณ์เฉียดวิกฤตในช่วงวิกฤตการณ์ขีปนาวุธคิวบาเป็นหลักฐาน ครั้งเหล่านี้นรอดมาได้เพราะโชคมากกว่าเพราะการออกแบบเชิงองค์กรที่รัดกุม

Example: A bridge does not collapse because the steel is weak, but because the expansion joint was designed for a temperature range that the climate exceeded.

ตัวอย่าง: สะพานพังไม่ใช่เพราะเหล็กกล้าอ่อน แต่เพราะรอยต่อขยายตัวถูกออกแบบไว้สำหรับช่วงอุณหภูมิหนึ่ง แล้วสภาพภูมิอากาศก็ทะลุช่วงนั้นไป

Verdict. Reliability is a property of the interfaces between components rather than the inherent quality of the individual pieces themselves.

คำตัดสิน. ความน่าเชื่อถือเป็นคุณสมบัติของจุดเชื่อมต่อระหว่างชิ้นส่วน ไม่ใช่คุณภาพในตัวของชิ้นส่วนแต่ละชิ้น

Overtured if: A comprehensive replication of the Cuban Missile Crisis data shows that organizational design, rather than luck, was the primary cause of nuclear safety.

จะพลิกคำตัดสินได้เมื่อ: มีผู้ทำซ้ำข้อมูลวิกฤตการณ์ขีปนาวุธคิวบาอย่างครอบคลุม แล้วพบว่าสาเหตุหลักของความปลอดภัยทางนิวเคลียร์คือการออกแบบเชิงองค์กร ไม่ใช่โชค

Sources. 1984 · Charles Perrow, "Normal Accidents: Living with High-Risk Technologies" — [overview](https://en.wikipedia.org/wiki/Normal_Accidents) · **1993** · Scott D. Sagan, "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons" — [Princeton UP](<https://press.princeton.edu/books/paperback/9780691021010/the-limits-of-safety>)

แหล่งอ้างอิง. 1984 · Charles Perrow, "Normal Accidents: Living with High-Risk Technologies" — [overview](https://en.wikipedia.org/wiki/Normal_Accidents) · **1993** · Scott D. Sagan, "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons" — [Princeton UP](<https://press.princeton.edu/books/paperback/9780691021010/the-limits-of-safety>)

02. Units and Assumptions — The Mismatch Nobody Owns

The Boundary as a Point of Failure

จุดเชื่อมต่อในฐานะจุดบกพร่อง

Complex systems do not fail at their singular, well-defended cores because those areas are subject to rigorous internal verification processes. Instead, these systems collapse at the invisible interface where two distinct, correctly functioning components are forced to exchange critical data. The Mars Climate Orbiter disaster in September 1999 illustrates this, as ground software transmitted thruster impulses using the unit of pound-force-seconds. The navigation system, however, was built to interpret these specific inputs only as Newton-seconds, creating a 4.45x conversion mismatch that remained entirely unobserved. The NASA Mishap Investigation Board confirmed that each subsystem was perfectly valid against its own local specification, yet no entity owned the interface. The lack of a unified authority over the handoff meant the defect existed in the space between the two otherwise functional, compliant engineering teams.

ระบบขับเคลื่อนไม่พังที่แกนกลางที่ป้องกันไว้แน่นหนา เพราะส่วนนั้นถูกตรวจสอบภายในอย่างเข้มงวด มันพังที่จุดเชื่อมต่อที่มองไม่เห็น ตรงที่ส่วนประกอบสองส่วนซึ่งต่างก็ทำงานถูกต้องถูกบังคับให้ส่งข้อมูลสำคัญให้กัน กรณี Mars Climate Orbiter เดือนกันยายน 1999 คือตัวอย่าง ซอฟต์แวร์ภาคพื้นดินส่งค่าแรงขับเคลื่อนเป็นหน่วยปอนด์-วินาที ระบบนำทางถูกสร้างมาให้อ่านค่าเหล่านั้นเป็นนิวตัน-วินาทีเท่านั้น ค่าจึงคลาดกันจากการแปลงหน่วย 4.45 เท่า และไม่มีใครสังเกตเห็นเลย NASA Mishap Investigation Board ยืนยันว่าระบบย่อยแต่ละส่วนถูกต้องตามข้อกำหนดของตนเองทุกประการ แต่ไม่มีหน่วยงานใดเป็นเจ้าของจุดเชื่อมต่อ เมื่อไม่มีใครถืออำนาจเหนือจุดส่งต่อ ข้อบกพร่องจึงอยู่ในช่องว่างระหว่างทีมวิศวกรสองทีมที่ต่างก็ทำงานถูกต้องตามมาตรฐาน

The Cost of Implicit Assumptions

ต้นทุนของข้อสมมติฐานโดยนัย

In June 1996, the Ariane 5 Flight 501 failure demonstrated how software reuse can introduce fatal risks when the original context is ignored. The Inquiry Board chaired by Prof. Jacques-Louis Lions discovered that the inertial-alignment software was inherited directly from the previous Ariane 4 rocket design. A 64-bit horizontal-velocity value was passed into a 16-bit integer, causing an unprotected conversion overflow that the system was never designed to handle safely. Similarly, in July 1983, the Gimli Glider incident occurred because the ground crew utilized a fuel-density conversion factor for pounds instead of kilograms. The Board of Inquiry led by George H. Lockwood noted that the crew applied a 1.77 factor instead of the required 0.803 kg/L. This error left the aircraft with under half the required fuel because both sides assumed their unit convention was the universal standard for all calculations.

เดือนมิถุนายน 1996 Ariane 5 Flight 501 ล้มเหลว และแสดงให้เห็นว่าซอฟต์แวร์ที่นำกลับมาใช้ใหม่กลายเป็นความเสี่ยงถึงชีวิตได้เมื่อบริบทเดิมถูกละเลย คณะกรรมการสอบสวนที่มี Prof. Jacques-Louis Lions เป็นประธานพบว่าซอฟต์แวร์จัดแนวแรงเฉื่อยถูกยกมาจากแบบของจรวด Ariane 4 รุ่นก่อนโดยตรง ค่าความเร็วแนวระดับขนาด 64-bit ถูกส่งเข้าตัวแปรจำนวนเต็มขนาด 16-bit ค่าล้นตอนแปลงโดยไม่มีอะไรป้องกัน และระบบไม่เคยถูกออกแบบให้รับมือกรณีนี้อย่างปลอดภัย เหตุการณ์ Gimli Glider เดือนกรกฎาคม 1983 เป็นแบบเดียวกัน เจ้าหน้าที่ภาคพื้นดินใช้ตัวคูณแปลงความหนาแน่นเชื้อเพลิงของหน่วยปอนด์ ไม่ใช่กิโลกรัม คณะกรรมการสอบสวนที่นำโดย George H. Lockwood ระบุว่าทีมงานใช้ตัวคูณ 1.77 แทนที่จะเป็น 0.803 kg/L ตามที่ต้องใช้เครื่องบินจึงมีเชื้อเพลิงไม่ถึงครึ่งของที่ต้องการ เพราะทั้งสองฝ่ายต่างถือว่าหน่วยของตนคือมาตรฐานสากลสำหรับการคำนวณทุกอย่าง

The Consensus of Investigations

ข้อสรุปจากการสอบสวน

There is no serious dispute regarding these findings, as the official investigations agree that the mechanisms of failure were entirely tied to mismatched assumptions. The NASA Mishap Investigation Board, the Inquiry Board led by Prof. Jacques-Louis Lions, and the Board of Inquiry led by George H. Lockwood all concur. Each body confirmed that the technical failure occurred because the interface was not treated as a distinct, owned component of the total system.

ข้อค้นพบเหล่านี้ไม่มีข้อโต้แย้งที่จริงจัง การสอบสวนอย่างเป็นทางการทุกชุดเห็นตรงกันว่ากลไกของความล้มเหลวผูกอยู่กับข้อสมมติที่ไม่ตรงกันทั้งหมด NASA Mishap Investigation Board, คณะกรรมการสอบสวนที่นำโดย Prof. Jacques-Louis Lions และคณะกรรมการสอบสวนที่นำโดย George H. Lockwood ให้ความเห็นเดียวกัน แต่ละคณะยืนยันว่าความล้มเหลวทางเทคนิคเกิดขึ้นเพราะจุดเชื่อมต่อไม่ได้ถูกปฏิบัติเป็นส่วนประกอบหนึ่งของระบบรวมที่แยกออกมาและมีเจ้าของชัดเจน

Example: A bridge fails not because the steel is weak, but because the architect and the engineer used different units for the load.

ตัวอย่าง: สะพานพังไม่ใช่เพราะเหล็กกล้าอ่อน แต่เพราะสถาปนิกกับวิศวกรใช้หน่วยน้ำหนักบรรทุกคนละหน่วย

Verdict. Reliability is a property of the boundary, and a defect that lacks an owner will inevitably remain hidden until the system reaches a failure state.

คำตัดสิน. ความน่าเชื่อถือเป็นคุณสมบัติของจุดเชื่อมต่อ ข้อบกพร่องที่ไม่มีเจ้าของจะซ่อนอยู่จนกว่าระบบจะเข้าสู่สถานะล้มเหลว และนั่นเสี่ยงไม่ได้

Overtaken if: A future analysis demonstrates that the Ariane 5 software overflow was successfully caught by the existing unit testing protocols during the flight preparation phase.

จะพลิกคำตัดสินได้เมื่อ: มีการวิเคราะห์ในอนาคตแสดงว่าค่าล้นในซอฟต์แวร์ Ariane 5 ถูกจับได้จริงโดยโปรโตคอลทดสอบหน่วยย่อยที่มีอยู่แล้ว ระหว่างขั้นเตรียมการบิน

Sources. 1999 · NASA Mishap Investigation Board, "Mars Climate Orbiter Mishap Investigation Board Phase I Report" — [NASA report PDF](https://llis.nasa.gov/llis_lib/pdf/1009464main1_0641-mr.pdf) · **1996** · Inquiry Board (chair J.-L. Lions), "ARIANE 5 Flight 501 Failure — Report by the Inquiry Board" — [ESA](<https://sci.esa.int/web/cluster/-/38889-ariane-501-report-by-board-of-inquiry>)

แหล่งอ้างอิง. 1999 · NASA Mishap Investigation Board, "Mars Climate Orbiter Mishap Investigation Board Phase I Report" — [NASA report PDF](https://llis.nasa.gov/llis_lib/pdf/1009464main1_0641-mr.pdf) · **1996** · Inquiry Board (chair J.-L. Lions), "ARIANE 5 Flight 501 Failure — Report by the Inquiry Board" — [ESA](<https://sci.esa.int/web/cluster/-/38889-ariane-501-report-by-board-of-inquiry>)

03. The Handoff — Where Information Goes to Die

The Fragility of the Boundary

ความเปราะบางของจุดเชื่อมต่อ

Transferring responsibility for a patient is an inherently hazardous operation that frequently produces measurable and preventable harm when the communication process lacks a formal, rigorous structure. The I-PASS Study Group led by Starmer et al. conducted a multicentre implementation involving the Walter Reed National Military Medical Center and nine other partner hospitals. In their 2014 study, they observed that the medical error rate fell from 24.5 to 18.8 per 100 admissions, representing a total decrease of 23 percent. This data demonstrates that the act of handing off information is not a neutral copy operation, but a vulnerable site where errors are manufactured during transmission. Without a standardized bundle, the gaps between the outgoing and incoming clinicians become conduits for the silent degradation of critical clinical information and patient safety protocols.

การส่งมอบผู้ป่วยจากมือหนึ่งไปอีกรมือหนึ่งเป็นงานที่เสี่ยงในตัวเอง เมื่อการสื่อสารไม่มีโครงสร้างที่เป็นทางการและเข้มงวด มันสร้างอันตรายที่วัดได้และป้องกันได้อยู่บ่อยครั้ง กลุ่มการศึกษา I-PASS นำโดย Starmer และคณะ ทดลองใช้จริงพร้อมกันหลายศูนย์การแพทย์ ทั้งที่ Walter Reed National Military Medical Center และโรงพยาบาลพันธมิตรอีกเก้าแห่ง ผลในการศึกษาปี 2014: อัตราความผิดพลาดทางการแพทย์ลดจาก 24.5 เหลือ 18.8 ต่อการรับผู้ป่วย 100 ราย ลดลงรวม 23 เปอร์เซ็นต์ ตัวเลขนี้บอกว่าการส่งต่อข้อมูลไม่ใช้การคัดลอกที่ไม่มีอะไรเปลี่ยน มันคือจุดเปราะบางที่ความผิดพลาดถูกผลิตขึ้นระหว่างทาง เมื่อไม่มีชุดเครื่องมือมาตรฐาน ช่องว่างระหว่างแพทย์ที่ส่งต่อกับแพทย์ที่รับช่วงจะกลายเป็นทางที่ข้อมูลทางคลินิกสำคัญและโปรโตคอลความปลอดภัยของผู้ป่วยเสื่อมหายไปอย่างเงียบๆ

The Architecture of Reliability

สถาปัตยกรรมของความน่าเชื่อถือ

A structured handoff bundle consists of a mnemonic-organized verbal handoff, a standardized written or computerized tool, and formal training paired with ongoing observation of the process. The 2014 I-PASS implementation showed that preventable adverse events decreased from 4.7 to 3.3 per 100 admissions, a significant 30 percent reduction in patient harm. Research published in a 2022/2023 multicentre extension, noted in PubMed 36326255, reported a further 47 percent reduction in handoff-related harm events within these complex clinical systems. These findings confirm that rigorous structure reduces harm without slowing down the workflow of the medical team, transforming the handoff from a hazard into a control. The aviation industry established the sterile cockpit rule under 14 CFR 121.542 in 1981 to restrict non-essential communication during critical phases of flight for similar reasons. This rule was developed by the Federal Aviation Administration following the 1974 Eastern Air Lines 212 crash in Charlotte, which underscored the dangers of crew distraction.

ชุดเครื่องมือส่งต่องานที่มีโครงสร้างมีองค์ประกอบดังนี้: ส่งต่อด้วยวาจาโดยเรียงลำดับตามคำช่วยจำ ใช้เครื่องมือที่เป็นลายลักษณ์อักษรหรือระบบคอมพิวเตอร์ที่เป็นมาตรฐาน และฝึกอบรมอย่างเป็นทางการควบคู่กับเฝ้าสังเกตกระบวนการอย่างต่อเนื่อง การนำ I-PASS มาใช้ในปี 2014 ลดเหตุการณ์ไม่พึงประสงค์ที่ป้องกันได้จาก 4.7 เหลือ 3.3 ต่อการรับผู้ป่วย 100 ราย อันตรายต่อผู้ป่วยลดลง 30 เปอร์เซ็นต์อย่างมีนัยสำคัญ งานวิจัยที่ตีพิมพ์ในการขยายผลหลายศูนย์ปี 2022/2023 ระบุไว้ใน PubMed 36326255 รายงานว่าเหตุการณ์อันตรายจากการส่งต่องานลดลงอีก 47 เปอร์เซ็นต์ในระบบทางคลินิกที่ซับซ้อนเหล่านี้ ข้อค้นพบเหล่านี้ยืนยันว่าโครงสร้างที่เข้มงวดลดอันตรายได้โดยไม่ทำให้ทีมแพทย์ทำงานช้าลง การส่งต่องานจึงเปลี่ยนจากภัยอันตรายเป็นกลไกควบคุม อุตสาหกรรมการบินทำแบบเดียวกันด้วยเหตุผลทำนองเดียวกัน: กฎห้องนักบินปลอดสิ่งรบกวน (sterile cockpit rule) ตามข้อบังคับ 14 CFR 121.542 ออกในปี 1981 เพื่อจำกัดการสื่อสารที่ไม่จำเป็นในช่วงวิกฤตของเที่ยวบิน Federal Aviation Administration พัฒนากฎนี้ขึ้นหลังเครื่องบิน Eastern Air Lines เที่ยวบินที่ 212 ตกที่ Charlotte ในปี 1974 อุบัติเหตุครั้งนั้นตอกย้ำอันตรายจากลูกเรือที่เสียสมาธิ

The Consensus on Handoffs

ฉันทามติเรื่องการส่งต่องาน

There is no complicating or null-result evidence found this turn to contest the effectiveness of these structured communication protocols in clinical or aviation environments. The evidence consistently indicates that the boundary where responsibility transfers is the primary location for systemic failure rather than any individual component of the system. The reliability of the system is therefore a property of the interface itself, requiring strict protocols to maintain safety during the transition of information.

รอบนี้ไม่พบหลักฐานที่ซับซ้อนกว่านั้นหรือผลลัพธ์ที่เป็นศูนย์มาโต้แย้งประสิทธิผลของโปรโตคอลการสื่อสารที่มีโครงสร้างเหล่านี้ ทั้งในคลินิกและในการบิน หลักฐานชี้ไปทางเดียวกันตลอด: จุดที่ความรับผิดชอบเปลี่ยนมือคือที่หลักที่ระบบล้มเหลว ไม่ใช่ส่วนประกอบชิ้นใดชิ้นหนึ่งของระบบ ความน่าเชื่อถือของระบบจึงเป็นคุณสมบัติของจุดเชื่อมต่อนั่นเอง และต้องมีโปรโตคอลที่เคร่งครัดคอยรักษาความปลอดภัยระหว่างที่ข้อมูลเปลี่ยนผ่าน

Example: A handoff is not a photocopy of a document but a high-stakes relay race where the baton is most likely to be dropped at the transfer.

ตัวอย่าง: การส่งต่องานไม่ใช่การถ่ายเอกสาร มันคือการวิ่งผลัดที่เดิมพันสูง และไม่ผลัดมีโอกาสตกมากที่สุดตอนส่งมอบ

Verdict. Handoffs are hazardous control problems that require explicit structural intervention to prevent the predictable loss of information and subsequent patient harm.

คำตัดสิน. การส่งต่องานคือปัญหาการควบคุมที่มีความเสี่ยง ต้องแทรกแซงเชิงโครงสร้างอย่างชัดเจน เพื่อกันไม่ให้ข้อมูลสูญหายอย่างที่คาดได้ล่วงหน้า และผู้ป่วยได้รับอันตรายตามมา

Overtuned if: A large-scale replication study fails to produce a reduction in harm or identifies that structural protocols introduce new, higher-frequency failure modes at the interface.

จะพลิกคำตัดสินได้เมื่อ: การศึกษาซ้ำในวงกว้างลดอันตรายไม่ได้ หรือพบว่าโปรโตคอลเชิงโครงสร้างสร้างรูปแบบความล้มเหลวแบบใหม่ที่เกิดถี่กว่าเดิมตรงจุดเชื่อมต่อ

Sources. 2014 · Starmer et al. (I-PASS Study Group), "Changes in Medical Errors after Implementation of a Handoff Program" — [NEJM](<https://www.nejm.org/doi/full/10.1056/NEJMsa1405556>) · **1981** · Federal Aviation Administration, "Sterile Flight Deck Rule (14 CFR 121.542) — origin and scope" — [SKYbrary](<https://skybrary.aero/articles/sterile-flight-deck>)

แหล่งอ้างอิง. 2014 · Starmer et al. (I-PASS Study Group), "Changes in Medical Errors after Implementation of a Handoff Program" — [NEJM](<https://www.nejm.org/doi/full/10.1056/NEJMsa1405556>) · **1981** · Federal Aviation Administration, "Sterile Flight Deck Rule (14 CFR 121.542) — origin and scope" — [SKYbrary](<https://skybrary.aero/articles/sterile-flight-deck>)

Chapter 4

04. Protocol Drift — When Two Sides Disagree About the Contract

The Origins of Liberal Acceptance

ต้นกำเนิดของการยอมรับแบบยืดหยุ่น

In 1989, J. Postel and his colleagues codified a foundational design principle for internet communication within the document formally known as RFC 1122. This guideline, which advised developers to be conservative in what they do but liberal in what they accept, aimed to ensure maximum interoperability between disparate systems. The IETF architects believed that by accepting slightly malformed input, services could survive minor errors without collapsing, thereby keeping the network functional and resilient. However, this design choice quietly shifted the actual maintenance burden onto the side that attempted to remain strictly correct according to the original, intended specification. Because the receiver silently papered over errors, the sender was never alerted that their output had drifted away from the agreed-upon standards of the protocol. Over time, the original contract between these two systems effectively vanished, leaving behind a fragile, undocumented reality that neither party fully owned or understood.

ในปี 1989 J. Postel และคณะเขียนหลักการที่ภายหลังจะทำให้สัญญาระหว่างระบบเลื่อนหายไป ลงในเอกสารที่รู้จักกันในชื่อทางการว่า RFC 1122 หลักการนั้นว่าไว้สั้นๆ ทำในสิ่งที่ตนทำอย่างอนุรักษนิยม ยอมรับสิ่งที่ได้รับอย่างยืดหยุ่น เป้าหมายคือให้ระบบที่ต่างกันทำงานร่วมกันได้มากที่สุด สถาปนิกของ IETF เชื่อว่าถ้ายอมรับอินพุตที่ผิดรูปแบบไปบ้าง บริการต่างๆ จะรอดจากข้อผิดพลาดเล็กน้อยได้โดยไม่ล่ม และเครือข่ายจะยังทำงานได้และทนทาน ทางเลือกนี้กลับผลักภาระบำรุงรักษาจริงไปไว้ที่ฝ่ายที่พยายามทำให้ถูกต้องตามข้อกำหนดดั้งเดิมอย่างเคร่งครัด โดยไม่มีใครรู้ตัว ผู้รับกลบเกลื่อนข้อผิดพลาดไปเงียบๆ ผู้ส่งจึงไม่เคยรู้ว่าเอาต์พุตของตนเบี่ยงเบนไปจากมาตรฐานของโปรโตคอลที่ตกลงกันไว้ เมื่อเวลาผ่านไป สัญญาดั้งเดิมระหว่างระบบทั้งสองก็หายไปทางปฏิบัติ เหลือไว้เพียงความเป็นจริงที่เปราะบาง ไม่มีเอกสารกำกับ และไม่มีฝ่ายใดเป็นเจ้าของหรือเข้าใจอย่างถ่องแท้

The Cost of Silent Tolerance

ต้นทุนของการยอมรับอย่างเงียบเชียบ

By 2023, the Internet Architecture Board, led by authors including Martin Thomson and T. Pauly, published RFC 9413 to formally address the consequences of this drift. The board observed that the long-standing habit of tolerating non-conforming input had inadvertently rewarded senders who failed to adhere to the established, rigorous protocol specifications. This silent tolerance entrenched deep ambiguity and created significant security flaws, as systems began to rely on unpredictable behaviors rather than the formal, explicit interface contract. The conservative sender, who continued to follow the rules, was forced to pay the maintenance cost indefinitely to accommodate the erratic behavior of the liberal peer. The IAB concluded that active protocol maintenance is far superior to the passive acceptance of malformed input, as it forces both sides to remain aligned. Contract testing, such as the use of consumer-driven contracts like Pact, serves as the modern enforcement mechanism that replaces vague assumptions with executable, verifiable interface expectations.

ภายในปี 2023 การเป็ยงเบนนี้ถูกจัดการอย่างเป็นทางการ Internet Architecture Board นำโดยผู้เขียนที่รวมถึง Martin Thomson และ T. Pauly เผยแพร่ RFC 9413 เพื่อรับมือกับผลของมันโดยตรง คณะกรรมการสังเกตว่านิสัยยอมรับอินพุตที่ไม่ตรงมาตรฐานซึ่งมีมานาน ให้รางวัลแก่ผู้ส่งที่ไม่ทำตามข้อกำหนดโปรโตคอลที่เข้มงวดและชัดเจน โดยไม่มีใครตั้งใจ การยอมรับเงียบๆ นี้ฝังความคลุมเครือลงลึก และสร้างข้อบกพร่องด้านความปลอดภัยที่สำคัญ เพราะระบบเริ่มพึ่งพาพฤติกรรมที่คาดเดาไม่ได้ แทนสัญญาจุดเชื่อมต่อที่ชัดเจนและเป็นทางการ ผู้ส่งที่อนุรักษ์นิยมและยังทำตามกฎต้องจ่ายต้นทุนบำรุงรักษาไปไม่มีกำหนด เพื่อรองรับพฤติกรรมที่เอาแน่เอานอนไม่ได้ของคู่สนทนาที่ยืดหยุ่นเกินไป IAB สรุปว่าการบำรุงรักษาโปรโตคอลเชิงรุกเหนือกว่าการรับอินพุตผิดรูปแบบโดยไม่โต้ตอบอยู่มาก เพราะมันบังคับให้ทั้งสองฝ่ายรักษาแนวทางให้ตรงกันอยู่เสมอ การทดสอบสัญญา เช่น สัญญาที่ขับเคลื่อนโดยผู้ใช้งาน (consumer-driven contracts) อย่าง Pact คือกลไกบังคับใช้สมัยใหม่ มันแทนที่ข้อสมมติฐานที่คลุมเครือด้วยความคาดหวังต่อจุดเชื่อมต่อที่รันได้และตรวจสอบได้จริง

The Shift in Standards

การเปลี่ยนแปลงของมาตรฐาน

The dispute regarding the validity of liberal acceptance is now resolved rather than contested, as the Internet Architecture Board has officially adopted the critique. The industry has moved away from the 1989 philosophy of RFC 1122 and toward the 2023 mandate of RFC 9413 for maintaining robust, predictable network protocols. The IETF has essentially reversed its stance, prioritizing explicit enforcement and clear contract adherence over the previous preference for loose, forgiving communication channels.

ข้อพิพาทเรื่องความถูกต้องของการยอมรับแบบยืดหยุ่นจนแล้ว ไม่ใช่ยังถกเถียงกันอยู่ เพราะ Internet Architecture Board รับคำวิจารณ์นั้นไว้อย่างเป็นทางการ uthasathamm ย้ายจากปรัชญาปี 1989 ของ RFC 1122 ไปสู่ข้อบังคับปี 2023 ของ RFC 9413 เพื่อรักษาโปรโตคอลเครือข่ายให้ทนทานและคาดการณ์ได้ IETF กลับจุดยืนโดยพื้นฐาน มันให้น้ำหนักกับการบังคับใช้ที่ชัดเจนและการทำตามสัญญาที่ชัดเจน มากกว่าช่องทางสื่อสารที่หละหลวมและให้อภัยความผิดพลาดอย่างที่เคยเลือกในอดีต

Example: A handshake that ignores a broken finger eventually leads to a grip that cannot hold any weight at all.

ตัวอย่าง: จับมือโดยละเลยนิ้วที่หัก สุดท้ายมือนั้นจะจับอะไรไม่อยู่ ใช้น้ำหนักไม่ได้เลย

Verdict. Systems fail when the interface contract is allowed to decay through the silent, unverified acceptance of inputs that deviate from the agreed specifications.

คำตัดสิน. ระบบล้มเหลวเมื่อสัญญาจุดเชื่อมต่อถูกปล่อยให้เสื่อมถอย ผ่านอินพุตที่เบี่ยงเบนจากข้อกำหนดที่ตกลงกันไว้ แล้วถูกรับเข้ามาเงียบๆ โดยไม่มีการตรวจสอบ

Overtuned if: A large-scale empirical study demonstrates that protocols enforcing strict input validation suffer higher rates of catastrophic failure than those using liberal acceptance policies.

จะพลิกคำตัดสินได้เมื่อ: มีการศึกษาเชิงประจักษ์ขนาดใหญ่แสดงว่าโปรโตคอลที่บังคับตรวจสอบอินพุตอย่างเข้มงวด ล้มเหลวร้ายแรงในอัตราที่สูงกว่าโปรโตคอลที่ใช้นโยบายยอมรับแบบยืดหยุ่น

Sources. 1989 · J. Postel et al., "Requirements for Internet Hosts — Communication Layers" — [IETF Datatracker](<https://datatracker.ietf.org/doc/html/rfc1122>) · **2023** · Internet Architecture Board / M. Thomson, T. Pauly, "Maintaining Robust Protocols" — [RFC Editor](<https://www.rfc-editor.org/info/rfc9413/>)

แหล่งอ้างอิง. 1989 · J. Postel et al., "Requirements for Internet Hosts — Communication Layers" — [IETF Datatracker](<https://datatracker.ietf.org/doc/html/rfc1122>) · **2023** · Internet Architecture Board / M. Thomson, T. Pauly, "Maintaining Robust Protocols" — [RFC Editor](<https://www.rfc-editor.org/info/rfc9413/>)

05. Timeouts and Retries — The Cure That Causes the Disease

The Paradox of Recovery Logic

ปฏิทรรศน์ของตรรกะการกู้คืน

Retry mechanisms are intended to improve reliability by masking transient faults within a distributed system, yet they frequently serve as the primary catalyst for total collapse. In the 2015 DynamoDB US-East disruption, Amazon Web Services documented how automated retry logic inadvertently transformed a localized issue into a sustained, system-wide service failure. When individual storage servers began retrying membership requests against an overloaded metadata service, they created a positive-feedback loop that overwhelmed the already struggling infrastructure components. This specific event showed that the retry logic itself was the mechanism keeping the system in a degraded state, rather than a bridge to recovery. By maintaining a ~55% error rate for customers, the system demonstrated that blindly reapplying requests can exacerbate rather than resolve the underlying resource exhaustion.

การลองใหม่มักกลายเป็นตัวเร่งหลักที่ทำให้ระบบล่มทั้งระบบอยู่บ่อยครั้ง ทั้งที่มันถูกออกแบบมาเพื่อเพิ่มความน่าเชื่อถือ ด้วยการกลบความผิดพลาดชั่วคราวในระบบกระจายศูนย์ไว้ ปี 2015 ระบบ DynamoDB ชัดข้อง และ Amazon Web Services บันทึกไว้เองว่าตรรกะการลองใหม่แบบอัตโนมัติเปลี่ยนปัญหาเฉพาะจุดให้กลายเป็นบริการล้มเหลวทั่วทั้งระบบอย่างยืดเยื้อ โดยไม่มีใครตั้งใจ เซิร์ฟเวอร์จัดเก็บข้อมูลแต่ละเครื่องส่งคำร้องขอสมาชิกภาพซ้ำไปยังบริการเมตาดาตาที่รับภาระเกินกำลังอยู่แล้ว ผลคือวงจรบ้อนกลับเชิงบวก ที่ถ้าโหมใส่ส่วนประกอบของโครงสร้างพื้นฐานที่กำลังแย้อยู่ก่อนแล้ว เหตุการณ์นี้ชี้ว่าตรรกะการลองใหม่นั้นเองคือกลไกที่ตรึงระบบไว้ในสภาวะเสื่อมประสิทธิภาพ ไม่ใช่สะพานไปสู่การกู้คืน อัตราข้อผิดพลาดค้างอยู่ที่ ~55% สำหรับลูกค้าตัวเลขนั้นบอกว่าการส่งคำร้องขอซ้ำโดยไม่ดูสภาพระบบ อาจทำให้ทรัพยากรที่ขาดแคลนอยู่แล้วยิ่งขาดหนักขึ้น แทนที่จะแก้ไขให้หาย

Metastable Failures and Load Shedding

ความล้มเหลวแบบกึ่งเสถียรและการลดภาระงาน

A metastable failure occurs when a system remains stuck in a high-latency or high-error state long after the initial triggering condition has been removed. Nathan Bronson, Abutalib Aghayev, Aleksey Charapko, and Timothy Zhu argued in their 2021 HotOS paper that these retry-driven loops are a defining characteristic of modern distributed systems. The 2015 AWS DynamoDB postmortem provides the definitive case study, illustrating how the metadata service could only recover once the team manually paused all incoming requests. This act of load shedding—deliberately rejecting work to protect the service—proved far more effective than the automated retries that had previously sustained the outage. To prevent the thundering-herd variant of this problem, engineers often implement exponential backoff with full jitter, calculating delay as $\text{random}(0,1)$ multiplied by the $\min(\text{cap}, \text{base} \times 2^{\text{attempt}})$. Marc Brooker, writing for the AWS Architecture Blog in 2015, established this formula as the standard industry mitigation for preventing clients from synchronizing their retry attempts.

ความล้มเหลวแบบกึ่งเสถียรคือระบบที่ยังติดอยู่ในสภาวะหน่วงสูงหรือผิดพลาดสูง ทั้งที่เงื่อนไขที่จุดชนวนถูกกำจัดไปนานแล้ว Nathan Bronson, Abutalib Aghayev, Aleksey Charapko และ Timothy Zhu ได้แย้งไว้ในเอกสาร HotOS ปี 2021 ว่าวงจรที่ซับซ้อนด้วยการลองใหม่นี้คือลักษณะเฉพาะที่นิยามระบบกระจายศูนย์สมัยใหม่ กรณีศึกษาที่ชัดที่สุดคือรายงานขั้นสุดเหตุขัดข้องของ AWS DynamoDB ปี 2015 บริการเมทาดาตาถูกค้นได้ก็ต่อเมื่อทีมงานลงมือระงับคำร้องขอเข้าทั้งหมดด้วยมือเท่านั้น นั่นคือการลดภาระงาน ปฏิเสธงานโดยตั้งใจเพื่อรักษาบริการไว้ และมันได้ผลกว่าการลองใหม่แบบอัตโนมัติที่ต่อลมหายใจให้เหตุขัดข้องมาก่อนหน้านั้นมาก ปัญหาอีกรูปแบบหนึ่งคือฝูงชนแห่เข้ามาพร้อมกัน วิศวกรมักกันไว้ด้วยการถอยเวลาแบบทวีคูณพร้อมการสุ่มเต็มรูปแบบ คือหน่วงเวลาเท่ากับ $\text{random}(0,1)$ คูณด้วย $\min(\text{cap}, \text{base} \times 2^{\text{attempt}})$ Marc Brooker เขียนไว้ใน AWS Architecture Blog ปี 2015 และวางสูตรนี้เป็นมาตรฐานการบรรเทาปัญหาของอุตสาหกรรม เพื่อกันไม่ให้โคลเอนต์ลองใหม่พร้อมกันเป็นจังหวะเดียว

The Consensus on Retry Risks

ฉันทามติเกี่ยวกับความเสี่ยงของการลองใหม่

There is no serious dispute regarding the danger of unconstrained retry loops, as the evidence from both academic research and operational postmortems aligns perfectly. Bronson et al. cite multiple industry incidents that mirror the DynamoDB failure, confirming that the pattern of retry amplification is a systemic, repeatable phenomenon. The field currently accepts that safety is a control problem requiring explicit load management rather than a simple component problem solvable by retrying.

อันตรายของวงจรลองใหม่ที่ไร้การควบคุมไม่มีข้อโต้แย้งที่สำคัญเหลืออยู่ หลักฐานจากงานวิจัยทางวิชาการและรายงานชั้นสูงเหตุขัดข้องจากหน้างานตรงกันทั้งหมด Bronson และคณะ อ้างถึงเหตุการณ์ในอุตสาหกรรมหลายครั้งที่ซ้ำรอยความล้มเหลวของ DynamoDB และยืนยันว่าการขยายตัวของการลองใหม่เป็นปรากฏการณ์เชิงระบบที่เกิดขึ้นได้ ปัจจุบันสาขานี้ยอมรับแล้วว่าความปลอดภัยเป็นปัญหาเชิงควบคุม ต้องจัดการภาระงานอย่างชัดเจน ไม่ใช่ปัญหาของส่วนประกอบขึ้นเดียวที่ลองใหม่แล้วจบ

Example: Retrying a failed request in an overloaded system is like pouring more water into a clogged drain, hoping the pressure will clear the pipe.

ตัวอย่าง: ส่งคำร้องขอที่ล้มเหลวซ้ำในระบบที่ภาระงานล้นมือ ก็เหมือนเทน้ำเพิ่มลงท่อระบายน้ำที่ตัน แล้วหวังว่าแรงดันจะดันสิ่งอุดตันให้หลุด

Verdict. Aggressive retry logic is a leading cause of large-scale, self-sustaining outages and should be replaced by load shedding during periods of high contention.

คำตัดสิน. ตรรกะการลองใหม่ที่ก้าวร้าวเกินไปคือสาเหตุอันดับต้นของเหตุขัดข้องขนาดใหญ่ที่หล่อเลี้ยงตัวเองได้ และควรถูกแทนที่ด้วยการลดภาระงานในช่วงที่แย่งชิงทรัพยากรกันสูง

Overtuned if: A large-scale system demonstrates that unconstrained retries under extreme load consistently lead to faster recovery times than load shedding or backoff strategies.

จะพลิกคำตัดสินได้เมื่อ: มีระบบขนาดใหญ่แสดงให้เห็นว่าการลองใหม่โดยไม่ได้รับการควบคุมภายใต้ภาระงานสุดขีด คุ้มกันได้เร็วกว่าการลดภาระงานหรือกลยุทธ์การถอยเวลาอย่างสม่ำเสมอ

Sources. 2021 · Nathan Bronson, Abutalib Aghayev, Aleksey Charapko, Timothy Zhu, "Metastable Failures in Distributed Systems" — [paper PDF] (<https://sigops.org/s/conferences/hotos/2021/papers/hotos21-s11-bronson.pdf>) · **2015** · Amazon Web Services, "Summary of the Amazon DynamoDB Service Disruption and Related Impacts in the US-East Region" — [AWS postmortem](<https://aws.amazon.com/message/5467D2/>)

แหล่งอ้างอิง. 2021 · Nathan Bronson, Abutalib Aghayev, Aleksey Charapko, Timothy Zhu, "Metastable Failures in Distributed Systems" — [paper PDF] (<https://sigops.org/s/conferences/hotos/2021/papers/hotos21-s11-bronson.pdf>) · **2015** · Amazon Web Services, "Summary of the Amazon DynamoDB Service Disruption and Related Impacts in the US-East Region" — [AWS postmortem](<https://aws.amazon.com/message/5467D2/>)

06. The Silent Success — Failure That Reports Everything Is Fine

The Illusion of Operational Certainty

ภาพลวงตาของความแน่นอนในการปฏิบัติงาน

The most dangerous failure mode is not the crash, but the silent return of corrupted data that masquerades as a valid success. When a storage stack confirms a write, the application assumes the data is safely committed, yet that confirmation often hides physical instability underneath. In a study of 1.53 million disk drives conducted over 32 months, researchers at NetApp and the University of Wisconsin found that 9.5% of nearline SATA drives developed at least one latent sector error per year. This high incidence rate demonstrates that physical components frequently degrade without triggering the error reporting mechanisms that engineers rely upon to maintain system health and data integrity. Such failures remain hidden from the monitoring layers because the hardware itself provides no indication that the underlying bit-level representation has drifted away from the original input.

ความล้มเหลวที่อันตรายที่สุดไม่ใช่เครื่องหยุดทำงาน แต่คือข้อมูลเสียหายที่ถูกส่งกลับมาเงียบๆ ในคราวของความสำเร็จที่ถูกต้อง สแต็กจัดเก็บข้อมูลยืนยันว่าเขียนแล้ว แอปพลิเคชันจึงถือว่าข้อมูลถูกบันทึกไว้ปลอดภัย แต่คำยืนยันนั้นมักซ่อนความไม่เสถียรทางกายภาพที่อยู่ข้างใต้เอาไว้ นักวิจัยที่ NetApp และ University of Wisconsin ศึกษาฮาร์ดไดรฟ์ 1.53 ล้านตัวเป็นเวลา 32 เดือน และพบว่าไดรฟ์ SATA แบบ nearline 9.5% เกิดข้อผิดพลาดในเซกเตอร์แบบแฝงอย่างน้อยหนึ่งครั้งต่อปี อัตราที่สูงขนาดนี้บอกว่าชิ้นส่วนทางกายภาพเสื่อมสภาพอยู่บ่อยครั้งโดยไม่ไปกระตุ้นกลไกรายงานข้อผิดพลาดที่วิศวกรใช้ดูแลความสมบูรณ์ของระบบและความถูกต้องของข้อมูล ความล้มเหลวแบบนี้จึงซ่อนตัวพ้นชั้นตรวจสอบ เพราะฮาร์ดแวร์เองไม่ส่งสัญญาณใดเลยว่าบิตที่เก็บอยู่ข้างล่างเบี่ยงไปจากอินพุตต้นฉบับแล้ว

The Scale of Mercurial Hardware

ขนาดของฮาร์ดแวร์ที่ไม่แน่นอน

Data integrity cannot be assumed at the interface layer because corruption occurs at rates high enough to matter fundamentally whenever systems operate at modern, massive fleet scales. A companion study of the same drive population over 41 months identified more than 400,000 instances of silent checksum mismatches, proving that standard reporting often fails to catch significant corruption. At Meta, engineers report that roughly 1-in-1,000 CPU cores exhibit defects capable of inducing silent data corruption, a phenomenon that forces a reassessment of reliability at the instruction level. Similarly, Google's "Cores that don't count" study coined the term "mercurial cores" to describe processors that silently miscompute results while continuing to report normal operational status to the kernel. These findings illustrate that absence of an alert is not evidence of system health, as the hardware layer may be actively producing errors while claiming to function perfectly.

ความสมบูรณ์ของข้อมูลเป็นสิ่งที่อนุমানเอาที่ชั้นจุดเชื่อมต่อไม่ได้ เพราะเมื่อระบบทำงานในระดับกลุ่มเครื่องขนาดใหญ่อย่างทุกวันนี้ ความเสียหายเกิดขึ้นในอัตราที่สูงพอจะมีความหมายในเชิงพื้นฐาน การศึกษาคู่ขนานบนประชากรโดรฟักกลุ่มเดียวกันเป็นเวลา 41 เดือน พบ checksum ไม่ตรงกันแบบเจียบมากกว่า 400,000 ครั้ง นี่คือหลักฐานว่าการรายงานตามมาตรฐานมักจับความเสียหายที่มีนัยสำคัญไม่ได้ ที่ Meta วิศวกรรายงานว่ CPU cores รว 1-in-1,000 มีข้อบกพร่องที่ทำให้ข้อมูลเสียหายแบบเจียบได้ ปรากฏการณ์นี้บิให้ต้องประเมินความน่าเชื่อถือกันใหม่ในระดับคำสั่ง การศึกษา "Cores that don't count" ของ Google ไปในทางเดียวกัน และบัญญัติคำว่า "mercurial cores" ให้โปรเซสเซอร์ที่คำนวณผลผิดแบบเจียบ ขณะยังรายงานสถานะปกติไปยังเคอร์เนล ข้อค้นพบเหล่านี้ชี้ว่าการไม่มีคำเตือนไม่ใช่หลักฐานว่ระบบสมบูรณ์ ชั้นฮาร์ดแวร์อาจกำลังผลิตข้อผิดพลาดอยู่ในขณะที่อ้างว่ตัวเองทำงานได้ไม่มีที่ติ

The End-to-End Necessity

ความจำเป็นแบบต้นทางถึงปลายทาง

Because intermediate layers cannot be trusted to report their own internal failures, Saltzer, Reed, and Clark argued in 1984 that integrity checks must reside at the system endpoints. This end-to-end argument remains the standard for robust design, as it avoids the fallacy of trusting individual components to identify and report every possible internal state of corruption. No consensus exists to reject this core argument, which has instead generated over 40 years of refinement literature regarding where checksums should be placed in evolving network stacks.

การตรวจสอบความสมบูรณ์ต้องอยู่ที่จุดสิ้นสุดของระบบ Saltzer, Reed และ Clark โต้แย้งไว้เช่นนั้นในปี 1984 เพราะชั้นกลางเชื่อใจให้รายงานความล้มเหลวภายในของตัวเองไม่ได้ ข้อโต้แย้งแบบต้นทางถึงปลายทางนี้ยังเป็นมาตรฐานของการออกแบบที่แข็งแกร่ง มันสร้างความเข้าใจผิดที่ว่าส่วนประกอบแต่ละชิ้นจะระบุและรายงานสถานะความเสียหายภายในได้ครบทุกแบบ ไม่มีฉันทามติใดปฏิบัติข้อโต้แย้งหลักนี้ สิ่งที่น่าทึ่งทำให้เกิดคือวรรณกรรมปรับปรุงต่อยอดยาวกว่า 40 ปี ว่าด้วยตำแหน่งที่ควรวาง checksum ในสแต็กเครือข่ายที่เปลี่ยนไปเรื่อยๆ

Example: A digital photograph arriving with a single corrupted pixel is a system success that hides a failure of the underlying storage medium.

ตัวอย่าง: ภาพถ่ายดิจิทัลที่มาถึงโดยมีพิกเซลเสียหนึ่งพิกเซลคือความสำเร็จของระบบ และมันปิดบังความล้มเหลวของสื่อจัดเก็บข้อมูลที่อยู่เบื้องล่าง

Verdict. Reliability is a property of interfaces, and safety must be managed through end-to-end verification rather than relying on the reported status of internal components.

คำตัดสิน. ความน่าเชื่อถือเป็นคุณสมบัติของจุดเชื่อมต่อ ความปลอดภัยจึงต้องจัดการด้วยการตรวจสอบแบบต้นทางถึงปลายทาง ไม่ใช่พึ่งสถานะที่ส่วนประกอบภายในรายงานมา

Overtaken if: A comprehensive longitudinal study demonstrates that modern storage and compute hardware achieves a zero-error rate, rendering end-to-end checksums redundant and computationally unnecessary.

จะพลิกคำตัดสินได้เมื่อ: มีการศึกษาเชิงยาวที่ครอบคลุมแสดงว่าฮาร์ดแวร์จัดเก็บข้อมูลและประมวลผลสมัยใหม่มีอัตราข้อผิดพลาดเป็นศูนย์ จน checksum แบบต้นทางถึงปลายทางกลายเป็นของซ้ำซ้อนและไม่จำเป็นในเชิงการคำนวณ

Sources. 2007 · L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, J. Schindler, "An Analysis of Latent Sector Errors in Disk Drives" — [ACM DL] (<https://dl.acm.org/doi/10.1145/1269899.1254917>) · **2008** · L. N. Bairavasundaram, G. R. Goodson, B. Schroeder, A. C. Arpaci-Dusseau, R. H. Arpaci-Dusseau, "An Analysis of Data Corruption in the Storage Stack" — [USENIX PDF](https://www.usenix.org/legacy/event/fast08/tech/full_papers/bairavasundaram/bairavasundaram.pdf)

แหล่งอ้างอิง. 2007 · L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, J. Schindler, "An Analysis of Latent Sector Errors in Disk Drives" — [ACM DL] (<https://dl.acm.org/doi/10.1145/1269899.1254917>) · **2008** · L. N. Bairavasundaram, G. R. Goodson, B. Schroeder, A. C. Arpaci-Dusseau, R. H. Arpaci-Dusseau, "An Analysis of Data Corruption in the Storage Stack" — [USENIX PDF](https://www.usenix.org/legacy/event/fast08/tech/full_papers/bairavasundaram/bairavasundaram.pdf)

07. Latent Conditions — Accidents That Were Already There

The Architecture of Latent Failure

สถาปัตยกรรมของความล้มเหลวที่แฝงอยู่

James Reason proposed the Swiss cheese model to illustrate how accidents occur through the alignment of latent conditions rather than a single catastrophic failure point. These latent conditions remain hidden within an organization for long periods, effectively waiting for a specific set of circumstances to bridge the gaps in safety defenses. In his 2000 publication, Reason argued that the final action taken by an operator is rarely the true cause of a complex system failure event. By examining these underlying systemic weaknesses, researchers shift their focus from the immediate human error to the broader environmental and organizational factors that permit accidents. This conceptual framework encourages professionals to view safety as a persistent management challenge rather than merely an exercise in eliminating individual component-level mistakes or errors.

อุบัติเหตุเกิดเมื่อเงื่อนไขแฝงหลายข้อเรียงตัวตรงกัน ไม่ใช่เมื่อจุดใดจุดหนึ่งพังลงอย่างร้ายแรงเพียงจุดเดียว นี่คือนี่ที่ James Reason เสนอไว้ในแบบจำลอง Swiss cheese เงื่อนไขแฝงพวกนี้ซ่อนอยู่ในองค์กรได้เป็นเวลานาน มันรอ รอให้สถานการณ์ชุดหนึ่งมาถึงพอดี แล้วเชื่อมช่องโหว่ในแนวป้องกันความปลอดภัยให้ทะลุถึงกัน ในงานตีพิมพ์ปี 2000 Reason ได้แย้งว่าการกระทำสุดท้ายของผู้ควบคุมแทบไม่เคยเป็นสาเหตุจริงของความล้มเหลวในระบบที่ซับซ้อน เมื่อผู้วิจัยไล่ดูจุดอ่อนเชิงระบบที่ซ่อนอยู่เหล่านี้ จุดเน้นจึงย้ายจากความผิดพลาดของมนุษย์ที่อยู่ตรงหน้า ไปยังปัจจัยด้านสิ่งแวดล้อมและองค์กรในวงกว้างที่ปล่อยให้อุบัติเหตุเกิดขึ้นได้ กรอบคิดนี้ให้ผู้เชี่ยวชาญมองความปลอดภัยเป็นงานบริหารที่ต้องทำต่อเนื่องไม่มีวันจบ ไม่ใช่แค่ไล่กำจัดความผิดพลาดหรือข้อผิดพลาดทีละชิ้นส่วน

The Incubation of Disaster

ระยะฟักตัวของหายนะ

Barry Turner developed the concept of the incubation period by coding 84 official British accident and disaster inquiry reports published by the year 1978. His research demonstrated that the preconditions for a disaster accumulate over a long, socially normal period before the triggering event finally makes the danger visible. Turner noted that he stopped his analysis at 84 reports because the final 71 documents failed to produce any new categories for his incubation-period model. Sidney Dekker expanded on this theme in 2011 by describing how organizations drift into failure through a series of small, locally rational adaptations over time. The "cause" identified in a typical inquiry is often simply the point where the long-term accumulation of latent conditions finally manifested in an observable way.

ระยะฟักตัวเป็นแนวคิดที่ Barry Turner สร้างขึ้นจากการอ่านและลงรหัสรายงานสอบสวนอุบัติเหตุและหายนะอย่างเป็นทางการของอังกฤษ 84 ฉบับ ที่ตีพิมพ์ภายในปี 1978 งานของเขาชี้ว่าเงื่อนไขเบื้องต้นของหายนะสะสมตัวมานาน ในช่วงที่ทุกอย่างดูปกติในสายตาสังคม จนกว่าเหตุการณ์กระตุ้นจะทำให้ภัยนั้นปรากฏชัดในท้ายที่สุด Turner ระบุว่าเขาหยุดวิเคราะห์ที่ 84 ฉบับ เพราะเอกสาร 71 ฉบับสุดท้ายไม่ให้หมวดหมู่ใหม่แก่แบบจำลองระยะฟักตัวของเขาอีกเลย Sidney Dekker ต่อยอดเรื่องนี้ในปี 2011 เขาอธิบายว่าองค์กรไหลเข้าสู่ความล้มเหลวได้อย่างไร ผ่านการปรับตัวเล็กๆ น้อยๆ ที่แต่ละครั้งดูสมเหตุสมผลในบริบทของมันเอง สะสมไปเรื่อยๆ ตามเวลา "สาเหตุ" ที่การสอบสวนทั่วไประบุ จึงมักเป็นแค่จุดที่เงื่อนไขแฝงซึ่งสะสมมานานโผล่ออกมาให้สังเกตเห็นได้เท่านั้น

The Limits of the Model

ข้อจำกัดของแบบจำลอง

The Swiss cheese model is contested by researchers like Larouzeé and Le Coze, who argue in their 2020 paper that the theory is often too vague. Critics suggest the model is effectively untestable or unfalsifiable as a causal theory, prone to being applied dogmatically as if layered defenses guarantee absolute safety. They also highlight that James Reason himself later qualified the model, acknowledging the limitations inherent in using such a simplified representation for complex organizational systems.

แบบจำลอง Swiss cheese ถูกโต้แย้ง นักวิจัยอย่าง Larouzeé และ Le Coze เขียนไว้ในบทความปี 2020 ว่าทฤษฎีนี้มักคลุมเครือเกินไป นักวิจารณ์กลุ่มนี้เห็นว่า ในฐานะทฤษฎีเชิงสาเหตุ แบบจำลองนี้แทบทดสอบไม่ได้และพิสูจน์ว่าเป็นเท็จไม่ได้ ทั้งยังถูกนำไปใช้อย่างตายตัว ราวกับว่าวางแนวป้องกันซ้อนกันเป็นชั้นๆ แล้วจะปลอดภัยโดยสมบูรณ์ พวกเขาชี้ด้วยว่าตัว James Reason เองก็ปรับเงื่อนไขของแบบจำลองนี้ในภายหลัง โดยยอมรับข้อจำกัดที่ติดมากับการใช้ภาพแทนอย่างง่ายเช่นนี้กับระบบองค์กรที่ซับซ้อน

Example: Like a slow-growing rust that weakens a bridge until the final car crosses it, the failure existed long before the collapse occurred.

ตัวอย่าง: ความล้มเหลวอยู่ตรงนั้นก่อนสะพานพังลงมานานแล้ว เหมือนสนิมที่ค่อยๆ กัดสะพานให้อ่อนลง จนรถคันสุดท้ายแล่นข้ามไป

Verdict. Accidents are systemic outcomes that incubate through latent conditions rather than being the direct result of the final action taken by an operator.

คำตัดสิน. อุบัติเหตุเป็นผลลัพธ์ของระบบ มันฟักตัวผ่านเงื่อนไขแฝง ไม่ใช่ผลโดยตรงจากการกระทำสุดท้ายของผู้ควบคุม

Overtured if: A rigorous replication of the 84 original inquiry reports reveals that the majority of disasters arise from sudden, isolated events without prior systemic accumulation.

จะพลิกคำตัดสินได้เมื่อ: มีใครทำซ้ำการศึกษาจากรายงานสอบสวนต้นฉบับ 84 ฉบับอย่างเคร่งครัด แล้วพบว่าหายนะส่วนใหญ่เกิดจากเหตุการณ์ฉับพลันที่แยกขาดจากกัน โดยไม่มีเงื่อนไขเชิงระบบสะสมมาก่อน

Sources. 2000 · Reason, J., "Human error: models and management" — [PubMed/BMJ 320:768–770](<https://pubmed.ncbi.nlm.nih.gov/10720363/>) · **2020** · Larouzeé, J. & Le Coze, J.-C., "Good and bad reasons: The Swiss cheese model and its critics" — [ScienceDirect, Safety Science](<https://www.sciencedirect.com/science/article/pii/S0925753520300576>)

แหล่งอ้างอิง. 2000 · Reason, J., "Human error: models and management" — [PubMed/BMJ 320:768–770](<https://pubmed.ncbi.nlm.nih.gov/10720363/>) · **2020** · Larouzeé, J. & Le Coze, J.-C., "Good and bad reasons: The Swiss cheese model and its critics" — [ScienceDirect, Safety Science](<https://www.sciencedirect.com/science/article/pii/S0925753520300576>)

08. The Blame Reflex — Why 'Human Error' Ends the Inquiry

The First Story and the Stopping Point

เรื่องเล่าชุดแรกและจุดหยุดชะงัก

When an accident occurs, organizations frequently default to the "first story," which centers on identifying who performed the action that led to the system failure. Sidney Dekker, in his 2014 work "The Field Guide to Understanding 'Human Error'," argues that this focus on the individual effectively terminates the investigation process. By naming a person as the primary cause, the inquiry stops exactly where a deeper technical or procedural investigation should ideally begin for the organization. This reflexive search for a culprit ignores the systemic conditions that influenced the human actor, leaving the underlying boundary vulnerabilities entirely unaddressed for the future. The "second story," by contrast, seeks to understand why the action made sense to the operator at the time, revealing the real causes within the system.

เมื่อเกิดอุบัติเหตุ องค์กรมักหยิบ "เรื่องเล่าชุดแรก" ขึ้นมาก่อน คือถามว่าใครเป็นคนทำสิ่งที่พาระบบไปสู่ความล้มเหลว Sidney Dekker ได้แย้งไว้ในงานเขียนปี 2014 เรื่อง "The Field Guide to Understanding 'Human Error'" ว่าการจับจ้องที่ตัวบุคคลแบบนี้ปิดกระบวนการสืบสวนลงทั้งหมด พอระบุชื่อคนว่าเป็นสาเหตุหลัก การสืบสวนก็หยุดตรงจุดที่องค์กรควรเริ่มสืบลึกลงไปในเชิงเทคนิคหรือเชิงกระบวนการพอดี การไล่หาผู้กระทำผิดตามสัญญาตณูณแบบนี้มองข้ามเงื่อนไขเชิงระบบที่กดดันผู้ปฏิบัติงานอยู่ ช่องโหว่บริเวณรอยต่อที่ซ่อนอยู่จึงยังอยู่ครบ ไม่มีใครแก้ไขสำหรับอนาคต "เรื่องเล่าชุดที่สอง" เดินคนละทาง มันถามว่าเหตุใดการกระทำนั้นจึงสมเหตุสมผลในสายตาผู้ปฏิบัติงานในขณะนั้น และคำตอบนั้นเองที่เผยสาเหตุที่แท้จริงภายในระบบ

The Distortion of Hindsight

การบิดเบือนจากอคติเมื่อรู้ผลแล้ว

The human tendency to view past events as inevitable is reinforced by the cognitive phenomenon known as hindsight bias, which was famously analyzed by Baruch Fischhoff. In their 1975 experiment involving 172 students at an Israeli university, Fischhoff and Beyth demonstrated that knowing an outcome significantly distorts one's memory of past uncertainty. The students who were told a historical outcome assigned that outcome a substantially higher retrospective probability than the control group that received no such information. This finding shows that the belief that an error "should have been obvious" is a psychological construct rather than a reliable assessment of the prior situation. Because investigators are aware of the outcome, they suffer from this bias, which makes their retrospective judgment of human performance inherently unreliable and prone to error.

คนที่รู้ผลแล้วจำความไม่แน่นอนในอดีตไม่ได้ตามจริง นี่คือนอกคติเมื่อรู้ผลแล้ว
ปรากฏการณ์ทางสถิติปัญหาที่ Baruch Fischhoff วิเคราะห์ไว้จนเป็นที่รู้จัก และมัน
ตอกย้ำแนวโน้มของมนุษย์ที่มองเหตุการณ์ในอดีตว่าหลีกเลี่ยงไม่ได้ Fischhoff และ
Beyth แสดงให้เห็นในการทดลองปี 1975 กับนักศึกษา 172 คนในมหาวิทยาลัยแห่งหนึ่ง
ของอิสราเอล ว่าการทราบผลลัพธ์ล่วงหน้าบิดเบือนความทรงจำเรื่องความไม่แน่นอนใน
อดีตอย่างมีนัยสำคัญ นักศึกษาที่ถูกบอกผลลัพธ์ทางประวัติศาสตร์ให้ความน่าจะเป็น
ย้อนหลังแก่ผลลัพธ์นั้นสูงกว่ากลุ่มควบคุมที่ไม่ได้รับข้อมูลนั้นมาก ความเชื่อว่าข้อ
ผิดพลาดนั้น "ควรจะเป็นสิ่งที่เห็นได้ชัดเจน" จึงเป็นสิ่งที่จิตใจสร้างขึ้นภายหลัง ไม่ใช่การ
ประเมินสถานการณ์ก่อนหน้านี้ที่เชื่อถือได้ ผู้สืบสวนรู้ผลลัพธ์อยู่แล้ว จึงตกอยู่ใต้อคตินี้
การตัดสินใจการปฏิบัติงานของมนุษย์ย้อนหลังจึงไม่น่าเชื่อถือและผิดพลาดง่ายโดยเนื้อแท้

The Responsibility Counterargument

ข้อโต้แย้งเรื่องความรับผิดชอบ

This focus on systemic causes is contested by Parker and Davies in their 2020 paper, which critiques the common industry shift toward a "no blame" culture. They argue for a "responsibility culture" in medicine, suggesting that individuals should still be held accountable for errors that are genuinely foreseeable and avoidable. If blamelessness is taken too far, the authors contend that the organization risks letting genuine negligence escape the necessary scrutiny required for professional accountability.

Parker และ Davies โต้แย้งการมุ่งเน้นสาเหตุเชิงระบบนี้ในบทความปี 2020 ของพวกเขา บทความนั้นวิพากษ์การที่อุตสาหกรรมโดยทั่วไปหันไปหาวัฒนธรรมแบบไม่กล่าวโทษบุคคล ทั้งสองเสนอ "วัฒนธรรมแห่งความรับผิดชอบ" สำหรับทางการแพทย์ บุคคลยังต้องรับผิดชอบต่อความผิดพลาดที่มองเห็นล่วงหน้าได้จริงและหลีกเลี่ยงได้จริง ผู้เขียนยืนยันว่าถ้าดันแนวคิดเรื่องการไม่กล่าวโทษไปไกลเกิน องค์กรจะเสี่ยงปล่อยให้ความประมาทเลินเล่อที่แท้จริงหลุดจากการตรวจสอบที่ความรับผิดชอบในวิชาชีพต้องการ

Example: Blaming a pilot for a crash is like blaming the map for a road that was missing a warning sign at a dangerous intersection.

ตัวอย่าง: โทษนักบินเมื่อเครื่องบินตก ก็เหมือนโทษแผนที่เมื่อถนนขาดป้ายเตือนตรงทางแยกอันตราย

Verdict. Naming an individual as the cause of a complex system failure is a cognitive shortcut that prevents the discovery of systemic safety risks.

คำตัดสิน. การชี้ชื่อบุคคลว่าเป็นสาเหตุของความล้มเหลวในระบบที่ซับซ้อนคือทางลัดทางความคิด และทางลัดนั้นปิดทางค้นพบความเสี่ยงด้านความปลอดภัยเชิงระบบ

Overtuned if: A replication of the 1975 Fischhoff and Beyth study fails to show that knowledge of an outcome inflates the perceived probability of its occurrence.

จะพลิกคำตัดสินได้เมื่อ: มีผู้ทำซ้ำการศึกษาของ Fischhoff และ Beyth ปี 1975 แล้วไม่พบว่าการทราบผลลัพธ์ล่วงหน้าทำให้การรับรู้ความน่าจะเป็นของเหตุการณ์นั้นสูงขึ้น

Sources. 2014 · Dekker, S., "The Field Guide to Understanding 'Human Error'" — [Routledge](<https://www.routledge.com/The-Field-Guide-to-Understanding-Human-Error/Dekker/p/book/9781472439055>) · **1975** · Fischhoff, B. & Beyth, R., "I Knew It Would Happen: Remembered Probabilities of Once-Future Things" — [ResearchGate](https://www.researchgate.net/publication/223213727_I_Knew_It_Would_Happen_Remembered_Probabilities_of_Once-Future_Things)

แหล่งอ้างอิง. 2014 · Dekker, S., "The Field Guide to Understanding 'Human Error'" — [Routledge](<https://www.routledge.com/The-Field-Guide-to-Understanding-Human-Error/Dekker/p/book/9781472439055>) · **1975** · Fischhoff, B. & Beyth, R., "I Knew It Would Happen: Remembered Probabilities of Once-Future Things" — [ResearchGate](https://www.researchgate.net/publication/223213727_I_Knew_It_Would_Happen_Remembered_Probabilities_of_Once-Future_Things)

09. The Postmortem — Turning an Outage Into an Asset

The Institutional Shift of Blameless Review

การเปลี่ยนผ่านเชิงสถาบันสู่การไม่กล่าวโทษบุคคล

The practice of the blameless postmortem emerged as a structural method to pivot from individual blame toward organizational learning by removing the fear of punishment. John Allspaw of Etsy pioneered this approach in his 2012 article "Blameless PostMortems and a Just Culture" to redefine how engineers interact with complex system failures. Google SRE has further institutionalized this methodology within their internal processes, as detailed in their workbook chapter on postmortem culture, to ensure systemic improvement occurs. The primary goal is to treat an outage as an asset for knowledge, rather than a point of failure that requires the termination of personnel. By 2012, this cultural shift began to define the standard for how technology firms process complex incidents without resorting to the destructive cycle of blame.

การชันสูตรเหตุขัดข้องแบบไม่กล่าวโทษบุคคลเกิดขึ้นเพื่อย้ายจุดเน้นจากตัวคนผิดไปที่การเรียนรู้ขององค์กร วิธีของมันคือตัดความกลัวว่าจะถูกลงโทษออกไป และทำเป็นโครงสร้าง ไม่ใช่ทำเป็นครั้งคราว คนบุกเบิกคือ John Allspaw จาก Etsy ในบทความปี 2012 เรื่อง "Blameless PostMortems and a Just Culture" เขาเขียนขึ้นเพื่อนิยามใหม่ ว่าวิศวกรควรรับมือกับความล้มเหลวของระบบซับซ้อนอย่างไร Google SRE ระเบียบวิธีนี้เข้าเป็นมาตรฐานในกระบวนการภายในของตน และเขียนไว้เป็นบทหนึ่งว่าด้วยวัฒนธรรมการชันสูตรเหตุขัดข้องในหนังสือคู่มือ จุดประสงค์คือให้การปรับปรุงเชิงระบบเกิดขึ้นจริง เป้าหมายหลักของทั้งหมดนี้คือปฏิบัติต่อเหตุระบบหยุดชะงักในฐานะสินทรัพย์ความรู้ ไม่ใช่จุดล้มเหลวที่ต้องจบด้วยการเลิกจ้างใครสักคน ภายในปี 2012 การเปลี่ยนแปลงทางวัฒนธรรมนี้เริ่มกลายเป็นมาตรฐานว่าบริษัทเทคโนโลยีจัดการเหตุการณ์ซับซ้อนอย่างไร โดยไม่ตกลงไปในวงจรกล่าวโทษที่ทำลายล้าง

Measuring the Artifacts of Failure

การวัดผลจากร่องรอยของความล้มเหลว

The Verica Open Incident Database, known as the VOID 2022 report, analyzed nearly 10,000 incident reports from just under 600 companies to understand industry trends. This massive empirical survey, published in 2022, serves as the largest existing dataset regarding how organizations document the boundaries where their complex systems fail. The data revealed that postmortem practice remains wildly inconsistent across the industry, with most public incident reports failing to identify any clear root cause. Near-miss analysis is almost nonexistent in these documents, leaving a significant gap in how companies learn from events that did not result in total collapse. While these artifacts are collected, the VOID report measures the documentation itself rather than whether these reviews actually reduce the rate of future system incidents.

ชุดข้อมูลใหญ่ที่สุดที่มีอยู่ในเรื่องนี้คือ Verica Open Incident Database หรือรายงาน VOID 2022 ตีพิมพ์ปี 2022 มันวิเคราะห์รายงานเหตุการณ์เกือบ 10,000 ฉบับจากบริษัทไม่ถึง 600 แห่ง เพื่อหาแนวโน้มของอุตสาหกรรม สิ่งที่มีนัยสำคัญคือวิธีที่องค์กรเขียนเอกสารถึงขอบเขตที่ระบบซับซ้อนของตนล้มเหลว ผลที่ออกมาชัด การชันสูตรเหตุขัดข้องในอุตสาหกรรมนี้ไม่สม่ำเสมออย่างมาก รายงานเหตุการณ์สาธารณะส่วนใหญ่ระบุสาเหตุรากเหง้าที่ชัดเจนไม่ได้เลย การวิเคราะห์เหตุการณ์เกือบพลาดแทบไม่ปรากฏในเอกสารเหล่านี้ จึงเหลือช่องว่างใหญ่ในวิธีที่บริษัทเรียนรู้จากเหตุการณ์ที่ไม่ได้จบด้วยการล่มทั้งระบบ ข้อจำกัดต้องพูดให้ชัด รายงาน VOID วัดตัวเอกสาร ไม่ได้วัดว่าการทบทวนเหล่านี้ลดอัตราเหตุการณ์ในระบบในอนาคตได้จริงหรือไม่ แม้ร่องรอยเหล่านี้จะถูกเก็บรวบรวมไว้ก็ตาม

The Gap in Causal Evidence

ช่องว่างในหลักฐานเชิงสาเหตุ

There is no independent, reliable dataset that allows researchers to confirm whether postmortem learning causally reduces future incident rates, a limitation noted in academic literature. A 2024 ACM workshop paper on postmortem action items explicitly documents that these items routinely go unimplemented, which undercuts the assumption that review produces change. This absence of evidence is not a minor detail but a fundamental ambiguity regarding the efficacy of the postmortem as an institutional tool for reliability.

ไม่มีชุดข้อมูลอิสระที่เชื่อถือได้ชุดใดให้นักวิจัยยืนยันได้ว่าการเรียนรู้จากการชันสูตรเหตุขัดข้องเป็นเหตุให้อัตราเหตุการณ์ในอนาคตลดลง วรรณกรรมทางวิชาการเองก็ระบุข้อจำกัดนี้ไว้ บทความจากเวิร์กช็อปของ ACM ปี 2024 ว่าด้วยข้อปฏิบัติหลังการชันสูตรเหตุขัดข้องเขียนไว้ตรงๆ ว่าข้อเหล่านี้มักไม่ถูกนำไปทำจริง สมมติฐานที่ว่าทบทวนแล้วจะเกิดการเปลี่ยนแปลงจึงถูกบั่นทอนตรงจุดนี้ หลักฐานที่หายไปไม่ใช่รายละเอียดปลีกย่อย มันคือความคลุมเครือขั้นพื้นฐานว่าการชันสูตรเหตุขัดข้องใช้ได้ผลแค่ไหนในฐานะเครื่องมือเชิงสถาบันเพื่อความน่าเชื่อถือ

Example: A postmortem is a map of a territory that has already shifted, which is only useful if the organization actually builds the roads.

ตัวอย่าง: การชันสูตรเหตุขัดข้องคือแผนที่ของดินแดนที่ขยับไปแล้ว มันมีประโยชน์ก็ต่อเมื่อองค์กรลงมือสร้างถนนบนดินแดนนั้นจริง

Verdict. The postmortem is an essential ritual for internal communication, but its capacity to prevent future failure remains an unproven hypothesis without causal data.

คำตัดสิน. การชันสูตรเหตุขัดข้องเป็นพิธีกรรมที่ขาดไม่ได้สำหรับการสื่อสารภายใน แต่จะกันความล้มเหลวในอนาคตได้หรือไม่ยังเป็นสมมติฐานที่ไม่ได้พิสูจน์ トラバที่ไม่มีข้อมูลเชิงสาเหตุ

Overtured if: A longitudinal study succeeds in establishing a statistical link between the rigor of specific postmortem action items and a measurable decline in incident frequency.

จะพลิกคำตัดสินได้เมื่อ: มีการศึกษาติดตามผลระยะยาวที่พิสูจน์ความเชื่อมโยงทางสถิติได้ ระหว่างความเข้มงวดของข้อปฏิบัติแต่ละข้อจากการชันสูตรเหตุขัดข้อง กับความถี่ของเหตุการณ์ที่ลดลงอย่างวัดผลได้

Sources. 2012 · Allspaw, J., "Blameless PostMortems and a Just Culture" — [Etsy Code as Craft](<https://codeascraft.com/2012/05/22/blameless-postmortems/>) · **2022** · Verica / Nash, C., "The VOID Report 2022" — [Verica](<https://www.verica.io/blog/void-2022-report-now-available/>)

แหล่งอ้างอิง. 2012 · Allspaw, J., "Blameless PostMortems and a Just Culture" — [Etsy Code as Craft](<https://codeascraft.com/2012/05/22/blameless-postmortems/>) · **2022** · Verica / Nash, C., "The VOID Report 2022" — [Verica](<https://www.verica.io/blog/void-2022-report-now-available/>)

10. Resilience Engineering — Work as Imagined and Work as Done

The divergence of procedure and practice

ความแตกต่างระหว่างขั้นตอนปฏิบัติและแนวทางปฏิบัติจริง

David Woods established the fundamental distinction between work-as-imagined, which represents the formal written procedure, and work-as-done, which describes the actual performance of complex tasks. In 2012, Alper et al. measured this gap within two pediatric hospitals by surveying 199 nurses regarding their adherence to medication administration protocols during daily operations. The data revealed that self-reported protocol violations occurred in 8%–30% of routine situations, demonstrating that workers frequently adapt their methods to meet system demands. These findings suggest that the gap is not a sign of individual deviance, but rather a systematic feature of how people navigate real-world constraints. When the formal procedure fails to align with operational reality, staff members must improvise to ensure that the work actually reaches its intended conclusion. By documenting these departures, researchers have shown that systems rely on these informal, unwritten adaptations to maintain performance levels under varying environmental pressures.

ช่องว่างระหว่างงานอย่างที่คิดว่าทำกับงานอย่างที่แท้จริงวัดออกมาเป็นตัวเลขได้ ในปี 2012 Alper และคณะสำรวจพยาบาล 199 คนในโรงพยาบาลเด็กสองแห่ง ถามว่าในงานประจำวันพวกเขาทำตามระเบียบการจ่ายยาแค่ไหน พยาบาลรายงานเองว่าละเมิดระเบียบใน 8%–30% ของสถานการณ์ทั่วไป คู่ความแตกต่างนี้ David Woods เป็นผู้วางรากฐานไว้ งานอย่างที่คิดว่าทำคือขั้นตอนที่เขียนไว้เป็นลายลักษณ์อักษรอย่างเป็นทางการ งานอย่างที่แท้จริงคือสิ่งที่เกิดขึ้นเมื่อคนลงมือทำงานที่ซับซ้อนในสถานการณ์จริง ตัวเลขนั้นบอกว่าผู้ปฏิบัติงานปรับวิธีทำงานอยู่บ่อยครั้งเพื่อให้ทันความต้องการของระบบ ช่องว่างจึงไม่ใช่สัญญาณว่าใครคนหนึ่งเปี่ยงเบน มันเป็นลักษณะเชิงระบบของวิธีที่คนรับมือกับข้อจำกัดในโลกจริง เมื่อขั้นตอนทางการไม่ตรงกับหน้างาน พนักงานต้องค้นสดเพื่อให้งานไปถึงปลายทางที่ตั้งใจไว้ นักวิจัยบันทึกการเปี่ยงเบนเหล่านี้ไว้ และแสดงให้เห็นว่าระบบพึงพาการปรับตัวที่ไม่เป็นทางการและไม่ได้เขียนไว้เหล่านี้เอง เพื่อรักษาระดับผลงานภายใต้แรงกดดันจากสภาพแวดล้อมที่เปลี่ยนไป

The ETTO principle and adaptive safety

หลักการ ETTO และความปลอดภัยเชิงปรับตัว

Erik Hollnagel introduced the ETTO principle, or efficiency-thoroughness trade-off, to explain how practitioners constantly balance these competing pressures to remain effective in their roles. The research by Alper et al. in 2012 further confirmed this, showing that in emergency situations, self-reported violations rose significantly to between 32%–53% among the 199 nurses. This increase demonstrates that the divergence is highest precisely when formal procedures are most difficult to follow, indicating that adaptation is a functional necessity. Hollnagel's Safety-I and Safety-II frameworks suggest that removing these informal adaptations can paradoxically reduce safety by stripping the system of its essential, latent flexibility. Rather than viewing these deviations as errors to be eliminated, resilience engineering posits that they are the mechanisms that allow complex systems to continue operating. Attempts to force strict adherence to work-as-imagined may therefore inadvertently undermine the very resilience that keeps the system functioning during periods of high instability.

ในสถานการณ์ฉุกเฉิน การละเมิดระเบียบที่รายงานเองในกลุ่มพยาบาล 199 คนเพิ่มขึ้นอย่างมีนัยสำคัญเป็น 32%–53% งานวิจัยของ Alper และคณะในปี 2012 ยืนยันเรื่องนี้เพิ่มเติม ความแตกต่างจึงสูงที่สุดตรงจุดที่ขั้นตอนทางการทำตามได้ยากที่สุดพอดี การปรับตัวเป็นความจำเป็นเชิงหน้าที่ Erik Hollnagel เรียกกลไกนี้ว่าหลักการ ETTO หรือการแลกเปลี่ยนระหว่างประสิทธิภาพและความถี่ถ้วน ผู้ปฏิบัติงานถ่วงดุลแรงกดดันสองด้านที่ขัดกันนี้อยู่ตลอดเวลาเพื่อให้ยังทำหน้าที่ของตนได้ผล กรอบแนวคิด Safety-I และ Safety-II ของ Hollnagel ชี้ต่อไปว่าการกำจัดการปรับตัวแบบไม่เป็นทางการเหล่านี้อาจทำให้ความปลอดภัยลดลง ผลย้อนแย้งนั้นเกิดเพราะระบบถูกตัดความยืดหยุ่นแฝงที่จำเป็นออกไป Resilience engineering จึงไม่มองการเปี่ยงเบนเหล่านี้เป็นข้อผิดพลาดที่ต้องกำจัด แต่ตั้งสมมติฐานว่ามันคือกลไกที่ทำให้ระบบซับซ้อนเดินต่อไปได้ ความพยายามบังคับให้ทำตามงานอย่างที่เราคิดว่าทำอย่างเคร่งครัด จึงอาจบั่นทอนความยืดหยุ่น ทนทานที่ค้ำระบบไว้ในช่วงที่ไม่มั่นคงสูงโดยไม่ได้ตั้งใจ

Evidence and institutional critique

หลักฐานและคำวิจารณ์เชิงสถาบัน

The validity of these approaches remains contested within the safety community, as M.D. Cooper argued in a 2022 critique published in *Safety Science*. Cooper contends that the Emperor has no clothes, asserting that there is no published, peer-reviewed empirical evidence showing that resilience engineering actually improves safety outcomes. He maintains that these new approaches often rely on traditional Safety-I methodologies in practice, despite their theoretical claims of offering a fundamentally different perspective.

ความถูกต้องของแนวทางเหล่านี้ยังเป็นที่ถกเถียงในวงการความปลอดภัย M.D. Cooper ได้แย้งไว้ในบทความปี 2022 ที่ตีพิมพ์ใน *Safety Science* ว่าแนวคิดนี้คือนิทานเรื่องชุดใหม่ของพระราชายังไม่มีหลักฐานเชิงประจักษ์ที่ตีพิมพ์และผ่านการตรวจสอบโดยผู้ทรงคุณวุฒิขึ้นใดแสดงว่า Resilience engineering ทำให้ผลลัพธ์ด้านความปลอดภัยดีขึ้นจริง Cooper ยืนยันต่อว่าในทางปฏิบัติ แนวทางใหม่เหล่านี้มักพึ่งระเบียบวิธีแบบ Safety-I แบบดั้งเดิม แม้ในทางทฤษฎีจะอ้างว่าเสนอมุมมองที่ต่างออกไปโดยสิ้นเชิงก็ตาม

Example: A pilot following the manual precisely in a storm might crash, while one who adapts the procedure to the wind survives.

ตัวอย่าง: นักบินที่ทำตามคู่มือทุกตัวอักษรกลางพายุอาจประสบอุบัติเหตุ ส่วนคนที่ปรับขั้นตอนตามแรงลมรอด

Verdict. Systems depend on informal adaptations to function, meaning that rigid enforcement of written procedures often masks the true operational risks of the environment.

คำตัดสิน. ระบบทำงานได้เพราะพึ่งการปรับตัวที่ไม่เป็นทางการ การบังคับใช้ขั้นตอนที่เขียนไว้อย่างแข็งตัวจึงมักบดบังความเสี่ยงที่แท้จริงในการปฏิบัติงานของสภาพแวดล้อมนั้น

Overtured if: A series of large-scale longitudinal studies demonstrate that organizations prioritizing strict procedural adherence consistently achieve lower incident rates than those allowing for informal adaptation.

จะพลิกคำตัดสินได้เมื่อ: มีการศึกษาตามยาวขนาดใหญ่หลายชุดแสดงว่าองค์กรที่ยึดการทำตามขั้นตอนอย่างเคร่งครัดเป็นหลัก มีอัตราอุบัติการณ์ต่ำกว่าอย่างสม่ำเสมอเทียบกับองค์กรที่ปล่อยให้ปรับตัวแบบไม่เป็นทางการ

Sources. 2012 · Alper, S.J. et al., "Self-Reported Violations During Medication Administration in Two Pediatric Hospitals" — [PMC](<https://pmc.ncbi.nlm.nih.gov/articles/PMC4174297>) · **2022** · Cooper, M.D., "The Emperor has no clothes: A critique of Safety-II" — [ScienceDirect](<https://www.sciencedirect.com/science/article/abs/pii/S0925753520304446>)

แหล่งอ้างอิง. 2012 · Alper, S.J. et al., "Self-Reported Violations During Medication Administration in Two Pediatric Hospitals" — [PMC](<https://pmc.ncbi.nlm.nih.gov/articles/PMC4174297>) · **2022** · Cooper, M.D., "The Emperor has no clothes: A critique of Safety-II" — [ScienceDirect](<https://www.sciencedirect.com/science/article/abs/pii/S0925753520304446>)

11. Control, Not Components — Leveson's Reframing

The Failure of Component-Reliability Models

ความล้มเหลวของแบบจำลองความน่าเชื่อถือของส่วนประกอบ

Traditional safety engineering often relies on techniques like FMEA or FTA to identify hazards, but these methods focus primarily on individual component failures. Nancy Leveson of MIT argues that this paradigm is fundamentally limited because it ignores accidents caused by unsafe interactions between perfectly functional system components. In complex software-intensive systems, nothing physically breaks or fails in the traditional sense, yet the system can still reach an unsafe state through logic errors. The 2012 book *Engineering a Safer World* by Nancy Leveson establishes that safety should be reframed as a control problem rather than a reliability problem. This shift in perspective requires moving away from the assumption that if every component works correctly, the entire system will be inherently safe.

ความปลอดภัยเป็นปัญหาด้านการควบคุม ไม่ใช่ปัญหาด้านความน่าเชื่อถือ กรอบนี้ หนังสือ *Engineering a Safer World* ปี 2012 โดย Nancy Leveson เป็นผู้วางไว้ วิศวกรรมความปลอดภัยแบบดั้งเดิมมักพึ่งเทคนิคอย่าง FMEA หรือ FTA เพื่อระบุ ภัยอันตราย แต่เทคนิคเหล่านี้มองความล้มเหลวของส่วนประกอบที่ละชิ้นเป็นหลัก Nancy Leveson จาก MIT ได้แย้งว่ากระบวนการนี้จำกัดตั้งแต่แรก เพราะมันมองข้ามอุบัติเหตุ ที่เกิดจากปฏิสัมพันธ์ที่ไม่ปลอดภัยระหว่างส่วนประกอบที่ทำงานสมบูรณ์ทุกชิ้น ในระบบ ซับซ้อนที่พึ่งซอฟต์แวร์หนัก ไม่มีอะไรแตกหรือพังในเชิงกายภาพตามความหมายเดิม แต่ระบบยังเข้าสู่สถานะไม่ปลอดภัยได้ผ่านข้อผิดพลาดทางตรรกะ มุมมองใหม่นี้บังคับ ให้ทั้งสมมติฐานเดิม ที่ว่าถ้าทุกชิ้นทำงานถูกต้อง ระบบทั้งหมดย่อมปลอดภัยไปเอง

STAMP and the Evidence of Control

STAMP และหลักฐานของการควบคุม

To address the limitations of component-failure analysis, Leveson developed STAMP, a systems-theoretic approach that views safety as a control problem involving feedback loops. In a 2018 study published in *Software Quality Journal*, Sulaman et al. applied both FMEA and STPA to a forward collision-avoidance system to measure their efficacy. The researchers found that 13 hazards were identified in common by both methods, proving that they share some ground in detecting basic system risks. However, the STPA method surfaced detailed causal factors—including software and communication-related causes—that the component-failure framing of FMEA entirely missed during the analysis process. This evidence demonstrates that a control-based method can capture systemic interactions that remain invisible to traditional models that look only for broken hardware parts.

วิธีที่มองการควบคุมจับปฏิสัมพันธ์เชิงระบบที่วิธีมองชิ้นส่วนพังจับไม่ได้ หลักฐานอยู่ในการศึกษาปี 2018 ที่ตีพิมพ์ใน *Software Quality Journal* ต้นทางของวิธีนั้นคือ STAMP ที่ Leveson พัฒนาขึ้นเพื่อแก้ข้อจำกัดของการวิเคราะห์ความล้มเหลวรายชิ้น เป็นแนวทางเชิงทฤษฎีระบบที่มองความปลอดภัยเป็นปัญหาด้านการควบคุม มีวงจรป้อนกลับอยู่ข้างใน ทีมของ Sulaman ใช้ทั้ง FMEA และ STPA กับระบบป้องกันการชนด้านหน้าเพื่อวัดว่าแต่ละวิธีได้ผลแค่ไหน ทั้งสองวิธีหาภัยอันตรายเจอร่วมกัน 13 รายการ นี่พิสูจน์ว่าทั้งคู่มีจุดร่วมในการจับความเสี่ยงพื้นฐานของระบบ แต่ STPA เผยปัจจัยเชิงสาเหตุออกมาละเอียดกว่า รวมถึงสาเหตุจากซอฟต์แวร์และการสื่อสาร กรอบความล้มเหลวรายชิ้นของ FMEA พลัดทั้งหมดนี้ไปตลอดกระบวนการวิเคราะห์ แบบจำลองดั้งเดิมมองหาแต่ชิ้นส่วนฮาร์ดแวร์ที่เสีย ปฏิสัมพันธ์เชิงระบบจึงล่องหนสำหรับมัน

The Limits of Methodological Superiority

ขีดจำกัดของความเหนือกว่าเชิงระเบียบวิธี

The 2018 comparison by Sulaman et al. remains contested because the study concluded that neither method is strictly superior to the other for safety analysis. The authors noted that some hazards were unique to FMEA, suggesting that both methods complement each other rather than one replacing the other entirely. Furthermore, the STPA Handbook (2018) by Leveson and Thomas acknowledges that STPA requires more analyst time and specific training to implement effectively.

ไม่มีวิธีใดเหนืออีกวิธีอย่างเด็ดขาดสำหรับการวิเคราะห์ความปลอดภัย นั่นคือข้อสรุปของการเปรียบเทียบปี 2018 โดยทีมของ Sulaman เอง และเป็นเหตุผลที่ผลเปรียบเทียบนี้ยังเป็นที่ถกเถียง ผู้เขียนตั้งข้อสังเกตว่าภัยอันตรายบางรายการพบเฉพาะใน FMEA ทั้งสองวิธีจึงเสริมกัน ไม่ใช่วิธีหนึ่งเข้ามาแทนอีกวิธีทั้งหมด นอกจากนี้ STPA Handbook (2018) โดย Leveson และ Thomas ยอมรับเองว่า STPA กินเวลาของนักวิเคราะห์มากกว่า และต้องฝึกเฉพาะทางก่อนจึงจะใช้ได้ผล

Example: Comparing FMEA to STPA is like checking for a flat tire versus analyzing the complex software logic that governs the autonomous steering system.

ตัวอย่าง: FMEA กับ STPA ต่างกันเหมือนการตรวจว่ายางแบนหรือไม่ กับการไล่ตรรกะซอฟต์แวร์ที่ซับซ้อนซึ่งคุมระบบพวงมาลัยอัตโนมัติ

Verdict. Safety is a control problem, yet the practical application of STPA requires significant time investment and does not render traditional component-based methods obsolete.

คำตัดสิน. ความปลอดภัยเป็นปัญหาด้านการควบคุม แต่ STPA ในทางปฏิบัติต้องลงเวลามาก และไม่ได้ทำให้วิธีดั้งเดิมที่มองรายชิ้นล้าสมัยไปแต่อย่างใด

Overtuned if: A future meta-analysis finds that STPA consistently identifies all hazards found by FMEA while reducing the total analyst time required for safety certification.

จะพลิกคำตัดสินได้เมื่อ: การวิเคราะห์ห่อภิมาณในอนาคตพบว่า STPA หากันตรายที่ FMEA หาเจอได้ครบทุกรายการอย่างสม่าเสมอ และลดเวลารวมของนักวิเคราะห์ที่ต้องใช้เพื่อการรับรองความปลอดภัยลงด้วย

Sources. 2012 · Leveson, N.G., "Engineering a Safer World: Systems Thinking Applied to Safety" — [MIT Press Open Access](<https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied>) · **2018** · Sulaman, S.M., Beer, A., Felderer, M. & Höst, M., "Comparison of the FMEA and STPA safety analysis methods – a case study" — [diva-portal.org](<http://www.diva-portal.org/smash/get/diva2:1166953/FULLTEXT01.pdf>)

แหล่งอ้างอิง. 2012 · Leveson, N.G., "Engineering a Safer World: Systems Thinking Applied to Safety" — [MIT Press Open Access](<https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied>) · **2018** · Sulaman, S.M., Beer, A., Felderer, M. & Höst, M., "Comparison of the FMEA and STPA safety analysis methods – a case study" — [diva-portal.org](<http://www.diva-portal.org/smash/get/diva2:1166953/FULLTEXT01.pdf>)

12. Finding Your Own Seams — The Procedure

Mapping the Architecture of Latent Conditions

การทำแผนที่สถาปัตยกรรมของเงื่อนไขแฝง

Systems rarely fail at their central components, but rather at the invisible boundaries where different parts meet under unstated assumptions neither side truly owns. James Reason, in his 2000 BMJ article (Vol. 320, pp. 768–770), established that safety depends on hunting for latent conditions that accumulate before they eventually trigger. Listing every boundary before examining any individual component forces a practitioner to acknowledge that reliability is a property of the interfaces connecting the entire system. This procedure synthesizes the latent-condition thinking of Reason with the control-based analysis favored by Nancy Leveson to ensure that safety is treated as a constraint. By documenting these seams, the practitioner identifies where assumptions reside, effectively shifting the focus from the isolated parts to the interactions that govern system behavior. The evidence from 2000 shows that failing to map these boundaries leaves the system vulnerable to the silent accumulation of conditions that precede any catastrophic failure.

ระบบไม่ค่อยล้มที่ส่วนประกอบหลัก มันล้มที่ขอบเขตที่มองไม่เห็น ตรงที่ส่วนต่าง ๆ มาบรรจบกันภายใต้สมมติฐานที่ไม่มีใครเขียนไว้ชัดเจน และไม่มีฝ่ายใดเป็นเจ้าของจริง James Reason วางหลักไว้ในบทความ BMJ ปี 2000 (เล่มที่ 320, หน้า 768–770) ว่าความปลอดภัยขึ้นอยู่กับการไล่ล่าเงื่อนไขแฝงที่สะสมตัวอยู่ก่อนจะถึงจุดวิกฤต ไล่รายการขอบเขตทั้งหมดก่อน แล้วค่อยตรวจสอบส่วนประกอบทีละชิ้น ลำดับนี้บังคับให้ผู้ปฏิบัติงานยอมรับว่าความน่าเชื่อถือคือคุณสมบัติของจุดเชื่อมต่อที่ร้อยทั้งระบบเข้าด้วยกัน ขั้นตอนนี้สังเคราะห์แนวคิดเรื่องเงื่อนไขแฝงของ Reason เข้ากับการวิเคราะห์เชิงควบคุมที่ Nancy Leveson สนับสนุน เพื่อให้ความปลอดภัยถูกปฏิบัติเสมือนข้อจำกัดบันทึกรอยต่อเหล่านี้ไว้ ผู้ปฏิบัติงานก็จะรู้ว่าสมมติฐานซ่อนอยู่ตรงไหน จุดเน้นจึงย้ายจากชิ้นส่วนที่แยกกันอยู่ไปสู่การปฏิสัมพันธ์ที่กำกับพฤติกรรมของระบบ หลักฐานจากปี 2000 ชี้ว่าถ้าไม่ทำแผนที่ขอบเขตเหล่านี้ ระบบจะเปราะบางต่อการสะสมเงื่อนไขอย่างเงียบ ๆ และการสะสมนั้นคือสิ่งที่มาก่อนความล้มเหลวระดับหายนะทุกครั้ง

Testing the Constraints at the Seam

การทดสอบข้อจำกัดที่รอยต่อ

Nancy Leveson, through her 2012 STAMP framework at MIT Press, argues that safety must be managed as a control problem rather than a component problem. Testing the seam requires asking what each side of an interface assumes the other side guarantees, rather than merely verifying the functionality of the parts. A robust procedure mandates writing down these mutual guarantees so that the next person to inherit the system understands the assumptions built into the architecture. This approach acknowledges that safety is a control constraint on interaction, which is a fundamentally different perspective than viewing safety as a property of components. The 2012 work by Leveson demonstrates that testing these seams prevents the propagation of errors that occur when expectations are not explicitly aligned across the boundary. Prioritizing the interface over the component ensures that the control structure remains intact, effectively mitigating the risks that arise when assumptions remain hidden from view.

Nancy Leveson ได้แย้งผ่านกรอบแนวคิด STAMP ปี 2012 ของเธอที่ MIT Press ว่าความปลอดภัยต้องถูกจัดการในฐานะปัญหาการควบคุม ไม่ใช่ปัญหาของส่วนประกอบ ทดสอบรอยต่อคือถามว่าแต่ละด้านของจุดเชื่อมต่อคาดหวังว่าอีกฝ่ายรับประกันอะไรให้ ไม่ใช่แค่ตรวจว่าชิ้นส่วนแต่ละชิ้นทำงานได้ ขั้นตอนที่เน้นหน้าบังคับให้จัดการรับประกันร่วมกันเหล่านี้นี้ลงไป คนที่รับช่วงระบบต่อจะได้เข้าใจสมมติฐานที่ฝังอยู่ในสถาปัตยกรรม แนวทางนี้ยอมรับว่าความปลอดภัยคือข้อจำกัดเชิงควบคุมต่อการปฏิสัมพันธ์ มุมมองนี้ต่างจากการมองว่าความปลอดภัยเป็นคุณสมบัติของส่วนประกอบตั้งแต่แรก ผลงานปี 2012 ของ Leveson แสดงว่าการทดสอบรอยต่อเหล่านี้กันไม่ให้ข้อผิดพลาดลุกลาม ข้อผิดพลาดชนิดที่เกิดเมื่อความคาดหวังสองฝั่งของขอบเขตไม่ได้ถูกจัดให้ตรงกันอย่างชัดเจน ให้จุดเชื่อมต่อก่อนส่วนประกอบ โครงสร้างการควบคุมจะยังอยู่ครบ และความเสี่ยงที่เกิดเมื่อสมมติฐานยังซ่อนอยู่ก็ลดลง

The Status of the Method

สถานะของวิธีการ

No serious dispute exists regarding the necessity of this procedure, as the evidence from the 2000 BMJ article and the 2012 STAMP framework remains unchallenged. The method relies on the established consensus that safety is a systemic property of controls and interfaces rather than a discrete attribute of individual parts. This chapter does not introduce a new claim but instead synthesizes the existing evidence to provide a practical guide for locating boundaries in any system.

ไม่มีข้อโต้แย้งที่จริงจังเรื่องความจำเป็นของขั้นตอนนี้ หลักฐานจากบทความ BMJ ปี 2000 และกรอบแนวคิด STAMP ปี 2012 ยังไม่มีใครหักล้างได้ วิธีนี้ยืนยันบนฉันทามติที่รับกันแล้วว่าความปลอดภัยเป็นคุณสมบัติเชิงระบบของการควบคุมและจุดเชื่อมต่อ ไม่ใช่คุณลักษณะที่แยกอยู่ในส่วนประกอบแต่ละชิ้น บทนี้ไม่ได้เสนอข้อกล่าวอ้างใหม่ มันสังเคราะห์หลักฐานที่มีอยู่ให้เป็นแนวทางปฏิบัติสำหรับหาขอบเขตในระบบใด ๆ

Example: A bridge is not just its steel beams, but the specific, documented tension at the joints where those beams connect to the concrete foundation.

ตัวอย่าง: สะพานไม่ได้มีแค่คานเหล็ก มันมีแรงตึงเฉพาะที่บันทึกไว้เป็นเอกสาร ตรงจุดเชื่อมต่อที่คานเหล็กเหล่านั้นยึดเข้ากับฐานรากคอนกรีตด้วย

Verdict. Reliability is a property of interfaces, and safety is a control problem that requires explicit documentation of the assumptions held at every boundary.

คำตัดสิน. ความน่าเชื่อถือเป็นคุณสมบัติของจุดเชื่อมต่อ และความปลอดภัยเป็นปัญหาการควบคุม ที่ต้องบันทึกสมมติฐานที่ถือไว้ในทุกขอบเขตให้ชัดเจน

Overtaken if: A study replicates the STAMP framework and demonstrates that component-level failure analysis provides a more accurate predictor of systemic collapse than interface-boundary testing.

จะพลิกคำตัดสินได้เมื่อ: มีงานศึกษาที่ทำซ้ำกรอบแนวคิด STAMP แล้วแสดงได้ว่าการวิเคราะห์ความล้มเหลวระดับส่วนประกอบทำนายการล่มสลายของระบบได้แม่นยำกว่าการทดสอบขอบเขตจุดเชื่อมต่อ

Sources. 2000 · Reason, J., "Human error: models and management" — [PubMed/BMJ 320:768–770](<https://pubmed.ncbi.nlm.nih.gov/10720363/>) · **2012** · Leveson, N.G., "Engineering a Safer World: Systems Thinking Applied to Safety" — [MIT Press Open Access](<https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied>)

แหล่งอ้างอิง. 2000 · Reason, J., "Human error: models and management" — [PubMed/BMJ 320:768–770](<https://pubmed.ncbi.nlm.nih.gov/10720363/>) · **2012** · Leveson, N.G., "Engineering a Safer World: Systems Thinking Applied to Safety" — [MIT Press Open Access](<https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied>)

Built by aice-book on 2026-09-05 from the frozen spec in SPEC.json. The English canon is the source of truth; the Thai rendition was made under source/CONTRACT.md and passed the block-parity gate. Request that produced this volume: “A book on interface failure for someone running a multi-engine system alone, written to the house standard under aice-book v1.2.0.”