Digitalization Pitfalls

Software & Complexity

https://koertsconsultancy.webex.com/koertsconsultancy/j.php?MTID=mc595126a4dfc7f1dbf188fff256e502a

Topics

- Cases
- Nancy Leveson
- Experience
- Guidance

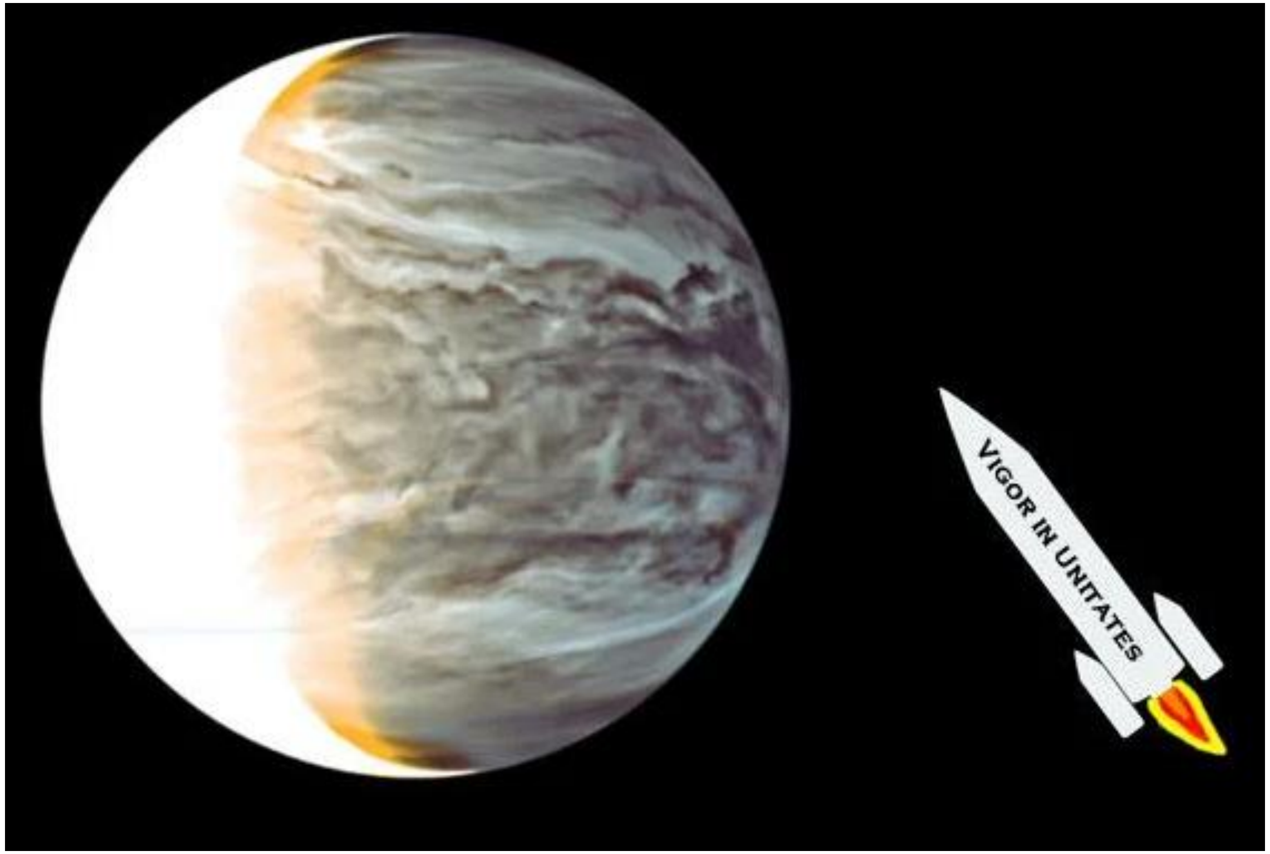
Ariane Rocket Launch
June 4 1996

- Dead routine
- Multiple software bugs

The launch, which took place on Tuesday, 4 June 1996, ended in failure due to multiple errors in the software design: Dead code (running, but intentionally so only for Ariane 4) with inadequate protection against integer overflow led to an exception handled inappropriately—halting the whole inertial navigation system

Venus missed Kersten Blunder 2 billion loss

- mm to inches error
- 24.5 instead of 25.4



Mars Polar Lander crash

PSI to bar

Airospace

Warsaw A320 Accident

Software thought airplane had not landed

Computer logic prevented the activation of both ground spoilers and thrust reversers until a minimum compression load of at least 6.3 tons was sensed on each main landing gear strut, thus preventing the crew from achieving any braking action by the two systems before this condition was met

Boing 737 Max, software upgrade overruling the pilot

Nancy Leveson   Engineering a safer world

Safety is an emergent property of systems, not a component property.

— Nancy Leveson —

Types of Accidents

- Component Failure Accidents

  Single or multiple component failures

  Usually assume random failure

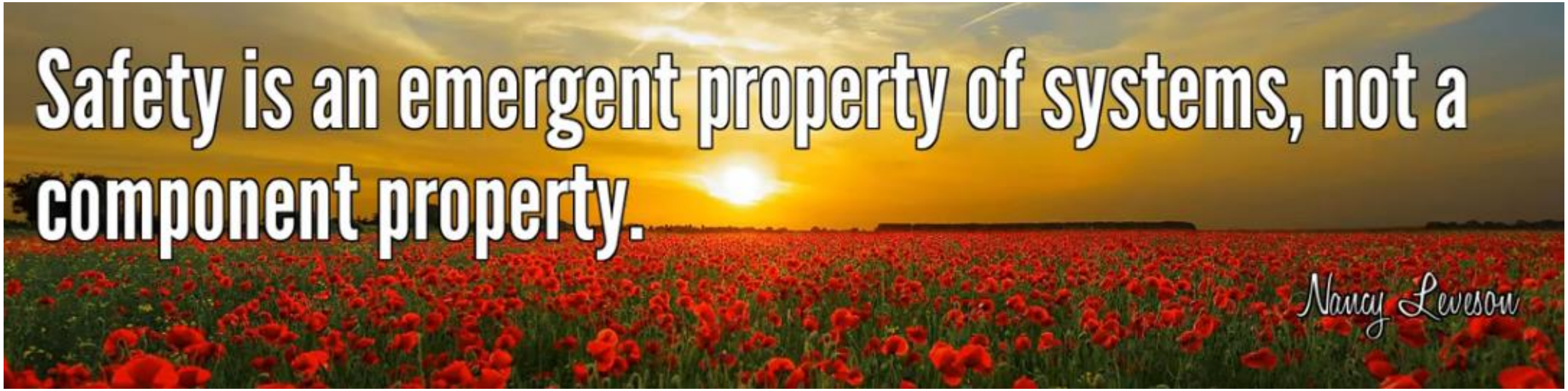
- System Accidents

  Arise in interactions among components

  No components may have "failed"

  Caused by interactive complexity and tight coupling

  Exacerbated by the introduction of computers.



Safety is an emergent property of systems, not a component property.

Nancy Leveson

Highly reliable components are not necessarily safe. .

Nancy Leveson

Best in class NASA software programs

- 3 errors per page

➢ Software engineers not trained in methods that avoid errors

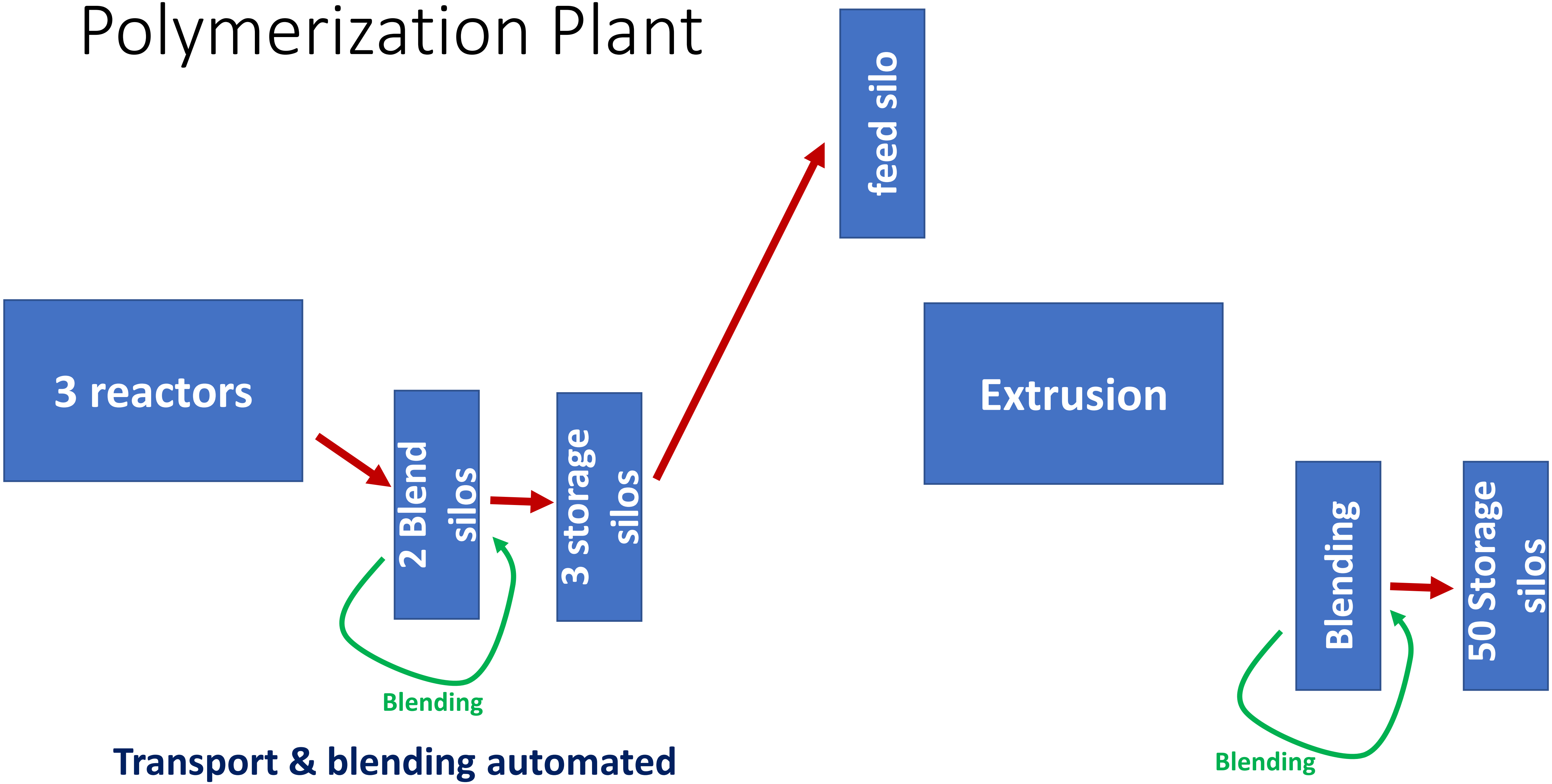
➢ Not all errors can be found in testing

Self driving cars

- Fatal incidents

- 100.000 pages programming…

Polymerization Plant



3 reactors

2 Blend silos

Blending

3 storage silos

feed silo

Extrusion

Blending

50 Storage silos

Blending

Transport & blending automated

MOC new PLC + software for transport

- Design
- Programming
- SAT (Supplier testing)
- FAT (Factory testing)
- Plant shutdowns by remaining errors

➢All the special situations are hard to foresee

STAMP

(System-Theoretic Accident Model and Processes)

- A new, more powerful accident/loss causality model
- Based on systems theory, not reliability theory
- Defines accidents/losses as a dynamic control problem (vs. a failure problem)
- Applies to VERY complex systems