ITMO UNIVERSITY

Saint Petersburg, Russia

How complex systems fails?

Ivan A. Perl / ivan.perl@corp.ifmo.ru

About myself

- Graduated in ITMO university
  - 2009 – Master
  - 2012 – PhD
- More then 12 years in IT industry
  - 2006-2014 – Motorola (Mobility, Google, ARRIS)
  - 2014 – *short stop at* Zodiac Interactive
  - 2014-now – Oracle Inc, (Staring 2017 in California)
  - 2006-now – teaching a University ITMO

Agenda

- What are complicated systems and where they live
- What Hegel and dialectics doing in software engineering?
- Signs of complex systems by Grady Booch
- Rule of “Hierarchical compensations” by Evgeny Sedov
- How Complex Systems Fail?

Hegelian dialectics

Dialectic or **dialectics** (Greek: διαλεκτική, *dialektikḗ*), also known as the **dialectical method**, is a discourse between two or more people holding different points of view about a subject but wishing to establish the truth through reasoned arguments.

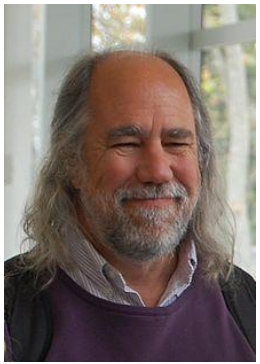
Hegelian dialectics concepts

Hegelian dialectics is based upon four concepts:

- Everything is transient and finite, existing in the medium of time.
- Everything is composed of contradictions (opposing forces).
- Gradual changes lead to crises, turning points when one force overcomes its opponent force (quantitative change leads to qualitative change).
- Change is helical (periodic without returning to the same position), not circular (negation of the negation).

The concept of dialectic (as a unity of opposites) existed in the philosophy of Heraclitus of Ephesus, who proposed that everything is in constant change, as a result of inner strife and opposition.

Grady Booch



Grady Booch (born February 27, 1955) is an American software engineer, best known for developing the Unified Modeling Language (UML) with **Ivar Jacobson** and **James Rumbaugh**.

He is recognized internationally for his innovative work in software architecture, software engineering, and collaborative development environments.

Attributes of a Complex System

- Hierarchic Structure
- Relative Primitives
- Separation of Concerns
- Common Patterns
- Stable Intermediate Forms

Attributes of a Complex System

Hierarchic Structure

"All systems have subsystems and all systems are parts of larger systems. . . . The value added by a system must come from the relationships between the parts, not from the parts per se"

Attributes of a Complex System

Relative Primitives

"The choice of what components in a system are primitive is relatively arbitrary and is largely up to the discretion of the observer of the system."

Attributes of a Complex System

Separation of Concerns

"Intracomponent linkages are generally stronger than intercomponent linkages. This fact has the effect of separating the high-frequency dynamics of the components—involving the internal structure of the components—from the low-frequency dynamics—involving interaction among components."

Attributes of a Complex System

Common Patterns

"Hierarchic systems are usually composed of only a few different kinds of subsystems in various combinations and arrangements."

Attributes of a Complex System

Stable Intermediate Forms

"A complex system that works is invariably found to have evolved from a simple system that worked.... A complex system designed from scratch never works and cannot be patched up to make it work. You have to start over, beginning with a working simple system."

Evgeny Sedov

Evgeny Alexandrovich Sedov (1929-1993) is a Russian scientist, PhD (к.т.н.), PDF (доктор философских наук).

Supervised the development and implementation of many types of electronic control and monitoring devices and systems: in ultra-long-range hypersonic communications - space and terrestrial; in the automated control systems of production of blocks of devices of computer facilities and communications; in the development of the foundations of artificial intelligence.

The law of hierarchical compensation by Sedov

“The growth of diversity at the top level of hierarchical organization is ensured by limiting diversity on the previous levels, and increased diversity on the lower level destroys the top level of the organization. ”

How Complex Systems Fail?

ITMO UNIVERSITY

Richard I. Cook, M.D.

Physician, researcher, and educator Richard Cook is presently a research scientist in the Department of Integrated Systems Engineering at the Ohio State University in Columbus, Ohio, and emeritus professor of healthcare systems safety at Sweden's KTH.

Richard is an internationally recognized expert on safety, accidents, and human performance at the sharp end of complex, adaptive systems. His most often cited publication is "Going Solid: A Model of System Dynamics and Consequences for Patient Safety."

ITMOre than a UNIVERSITY

1. Complex systems are intrinsically hazardous systems.

All of the interesting systems (e.g. transportation, healthcare, power generation) are inherently and unavoidably hazardous by the own nature. The frequency of hazard exposure can sometimes be changed but the processes involved in the system are themselves intrinsically and irreducibly hazardous. It is the presence of these hazards that drives the creation of defenses against hazard that characterize these systems.

2. Complex systems are heavily and successfully defended against failure.

The high consequences of failure lead over time to the construction of multiple layers of defense against failure. These defenses include obvious technical components (e.g. backup systems, ‘safety’ features of equipment) and human components (e.g. training, knowledge) but also a variety of organizational, institutional, and regulatory defenses (e.g. policies and procedures, certification, work rules, team training). The effect of these measures is to provide a series of shields that normally divert operations away from accidents.

3. Catastrophe requires multiple failures – single point failures are not enough..

The array of defenses works. System operations are generally successful. Overt catastrophic failure occurs when small, apparently innocuous failures join to create opportunity for a systemic accident. Each of these small failures is necessary to cause catastrophe but only the combination is sufficient to permit failure. Put another way, there are many more failure opportunities than overt system accidents. Most initial failure trajectories are blocked by designed system safety components. Trajectories that reach the operational level are mostly blocked, usually by practitioners.

4. Complex systems contain changing mixtures of failures latent within them.

The complexity of these systems makes it impossible for them to run without multiple flaws being present. Because these are individually insufficient to cause failure they are regarded as minor factors during operations. Eradication of all latent failures is limited primarily by economic cost but also because it is difficult before the fact to see how such failures might contribute to an accident. The failures change constantly because of changing technology, work organization, and efforts to eradicate failures.

5. Complex systems run in degraded mode.

A corollary to the preceding point is that complex systems run as broken systems. The system continues to function because it contains so many redundancies and because people can make it function, despite the presence of many flaws. After accident reviews nearly always note that the system has a history of prior ‘proto-accidents’ that nearly generated catastrophe. Arguments that these degraded conditions should have been recognized before the overt accident are usually predicated on naïve notions of system performance. System operations are dynamic, with components (organizational, human, technical) failing and being replaced continuously.

ITMO UNIVERSITY

6. Catastrophe is always just around the corner.

Complex systems possess potential for catastrophic failure. Human practitioners are nearly always in close physical and temporal proximity to these potential failures – disaster can occur at any time and in nearly any place. The potential for catastrophic outcome is a hallmark of complex systems. It is impossible to eliminate the potential for such catastrophic failure; the potential for such failure is always present by the system's own nature.

ITMO more than a UNIVERSITY

7. Post-accident attribution accident to a ‘root cause’ is fundamentally wrong.

Because overt failure requires multiple faults, there is no isolated ‘cause’ of an accident. There are multiple contributors to accidents. Each of these is necessary insufficient in itself to create an accident. Only jointly are these causes sufficient to create an accident. Indeed, it is the linking of these causes together that creates the circumstances required for the accident. Thus, no isolation of the ‘root cause’ of an accident is possible. The evaluations based on such reasoning as ‘root cause’ do not reflect a technical understanding of the nature of failure but rather the social, cultural need to blame specific, localized forces or events for outcomes.

ITMO UNIVERSITY

8. Hindsight biases post-accident assessments of human performance.

Knowledge of the outcome makes it seem that events leading to the outcome should have appeared more salient to practitioners at the time than was actually the case. This means that ex post facto accident analysis of human performance is inaccurate. The outcome knowledge poisons the ability of after-accident observers to recreate the view of practitioners before the accident of those same factors. It seems that practitioners “should have known” that the factors would “inevitably” lead to an accident

ITMO more than a UNIVERSITY

ITMO UNIVERSITY

9. Human operators have dual roles: as producers & as defenders against failure.

The system practitioners operate the system in order to produce its desired product and also work to forestall accidents. This dynamic quality of system operation, the balancing of demands for production against the possibility of incipient failure is unavoidable. Outsiders rarely acknowledge the duality of this role. In non-accident filled times, the production role is emphasized. After accidents, the defense against failure role is emphasized. At either time, the outsider's view misapprehends the operator's constant, simultaneous engagement with both roles.

ITMO more than a UNIVERSITY

ITMO UNIVERSITY

10. All practitioner actions are gambles.

After accidents, the overt failure often appears to have been inevitable and the practitioner's actions as blunders or deliberate willful disregard of certain impending failure. But all practitioner actions are actually gambles, that is, acts that take place in the face of uncertain outcomes. The degree of uncertainty may change from moment to moment. That practitioner actions are gambles appears clear after accidents; in general, post hoc analysis regards these gambles as poor ones. But the converse: that successful outcomes are also the result of gambles; is not widely appreciated.

ITMO more than a UNIVERSITY

ITMO UNIVERSITY

11. Actions at the sharp end resolve all ambiguity.

Organizations are ambiguous, often intentionally, about the relationship between production targets, efficient use of resources, economy and costs of operations, and acceptable risks of low and high consequence accidents. All ambiguity is resolved by actions of practitioners at the sharp end of the system. After an accident, practitioner actions may be regarded as ‘errors’ or ‘violations’ but these evaluations are heavily biased by hindsight and ignore the other driving forces, especially production pressure.

ITMOre than a UNIVERSITY

ITMO UNIVERSITY

12. Human practitioners are the adaptable element of complex systems.

Practitioners and first line management actively adapt the system to maximize production and minimize accidents. These adaptations often occur on a moment by moment basis. Some of these adaptations include:

(1) Restructuring the system in order to reduce exposure of vulnerable parts to failure.

(2) Concentrating critical resources in areas of expected high demand.

(3) Providing pathways for retreat or recovery from expected and unexpected faults.

(4) Establishing means for early detection of changed system performance in order to allow graceful cutbacks in production or other means of increasing resiliency.

13. Human expertise in complex systems is constantly changing.

Complex systems require substantial human expertise in their operation and management. This expertise changes in character as technology changes but it also changes because of the need to replace experts who leave. In every case, training and refinement of skill and expertise is one part of the function of the system itself. At any moment, therefore, a given complex system will contain practitioners and trainees with varying degrees of expertise. Critical issues related to expertise arise from

(1) the need to use scarce expertise as a resource for the most difficult or demanding production needs and

(2) (2) the need to develop expertise for future use

14. Change introduces new forms of failure.

The low rate of overt accidents in reliable systems may encourage changes, especially the use of new technology, to decrease the number of low consequence but high frequency failures. These changes maybe actually create opportunities for new, low frequency but high consequence failures. When new technologies are used to eliminate well understood system failures or to gain high precision performance they often introduce new pathways to large scale, catastrophic failures.

15. Views of ‘cause’ limit the effectiveness of defenses against future events.

Post-accident remedies for “human error” are usually predicated on obstructing activities that can “cause” accidents. These end-of-the-chain measures do little to reduce the likelihood of further accidents. In fact that likelihood of an identical accident is already extraordinarily low because the pattern of latent failures changes constantly. Instead of increasing safety, post-accident remedies usually increase the coupling and complexity of the system.

ITMO UNIVERSITY

16. Safety is a characteristic of systems and not of their components

Safety is an emergent property of systems; it does not reside in a person, device or department of an organization or system. Safety cannot be purchased or manufactured; it is not a feature that is separate from the other components of the system. This means that safety cannot be manipulated like a feedstock or raw material. The state of safety in any system is always dynamic; continuous systemic change insures that hazard and its management are constantly changing.

17. People continuously create safety.

Failure free operations are the result of activities of people who work to keep the system within the boundaries of tolerable performance. These activities are, for the most part, part of normal operations and superficially straightforward. But because system operations are never trouble free, human practitioner adaptations to changing conditions actually create safety from moment to moment. These adaptations often amount to just the selection of a well-rehearsed routine from a store of available responses; sometimes, however, the adaptations are novel combinations or de novo creations of new approaches.

18. Failure free operations require experience with failure.

Recognizing hazard and successfully manipulating system operations to remain inside the tolerable performance boundaries requires intimate contact with failure. More robust system performance is likely to arise in systems where operators can discern the “edge of the envelope”. This is where system performance begins to deteriorate, becomes difficult to predict, or cannot be readily recovered. In intrinsically hazardous systems, operators are expected to encounter and appreciate hazards in ways that lead to overall performance that is desirable. Improved safety depends on providing operators with calibrated views of the hazards. It also depends on providing calibration about how their actions move system performance towards or away from the edge of the envelope.

Thank you!
Questions?

www.ifmo.ru

ITMOre than a UNIVERSITY