Architektura ryzyka i pułapki systemowe w ujęciu Charlesa Perrowa

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje koncepcję Normal Accident Theory (NAT) Charlesa Perrowa na przykładzie katastrofy w Three Mile Island. Autor dowodzi, że wypadek nie był wynikiem pojedynczego błędu ludzkiego, lecz efektem systemowej nieczytelności i złożoności interakcyjnej. Kluczowym problemem okazała się rozbieżność między stanem fizycznym instalacji a informacjami dostarczanymi przez wskaźniki, co doprowadziło do błędu wymuszonego poznawczo. W systemach wysokiego ryzyka fałszywe dane zakażają interpretację całego procesu, sprawiając, że racjonalne działania operatorów stają się niebezpieczne. Tekst podkreśla, że w obliczu ścisłego sprzężenia i szumu informacyjnego, niektóre awarie są niemal nieuniknione ze względu na samą strukturę systemu.

The article analyzes Charles Perrow's Normal Accident Theory (NAT) using the example of the Three Mile Island disaster. The author demonstrates that the accident was not the result of a single human error, but an effect of systemic opacity and interactive complexity. A key problem proved to be the discrepancy between the physical state of the plant and the information provided by the indicators, which led to a cognitively forced error. In high-risk systems, false data contaminates the interpretation of the entire process, making the rational actions of operators dangerous. The text emphasizes that in the face of tight coupling and information noise, some failures are almost inevitable due to the very structure of the system.

Artykuł stanowi krytyczną analizę systemów wysokiego ryzyka w oparciu o Teorię Normalnych Wypadków (NAT) Charlesa Perrowa, wykorzystując katastrofę w Three Mile Island jako dowód na to, że pewne awarie są nieuchronne. Główną tezą autora jest twierdzenie, że w systemach charakteryzujących się wysoką złożonością interakcyjną i ścisłym sprzężeniem, katastrofy wynikają z samej architektury systemu, a nie z błędów

operatorów. Autor argumentuje, że tzw. „błąd ludzki” jest często wymuszony przez systemową nieczytelność – sytuację, w której technologia dostarcza mylące sygnały i fałszywe reprezentacje rzeczywistości, uniemożliwiając trafną decyzję pod presją czasu. Tekst konfrontuje optymizm Teorii Wysokiej Niezawodności (HRT), wierzącej w moc procedur i kultury bezpieczeństwa, z brutalnym sceptycyzmem NAT, wskazując, że samo doskonalenie organizacji nie eliminuje ryzyka strukturalnego. W konsekwencji autor postuluje konieczność etycznej oceny dopuszczalności danych technologii, szczególnie gdy generują one nieodwracalne zagrożenia dla osób postronnych i przyszłych pokoleń, których zgoda na takie ryzyko nigdy nie została uzyskana.

SŁOWA KLUCZOWE

architektura ryzyka | pułapki systemowe | Charles Perrow | Normal Accident Theory | High Reliability Organizations | złożoność interakcyjna | ścisłe sprzężenie | systemowa nieczytelność | fałszywe wskaźniki | paradoks redundancji | błąd wymuszony poznawczo | bezpieczeństwo systemów wysokiego ryzyka | epistemologia organizacyjna | kultura bezpieczeństwa | zarządzanie ryzykiem strukturalnym

Three Mile Island jako dowód na systemową nieczytelność

Katastrofa w elektrowni jądrowej Three Mile Island jest dla teorii Charlesa Perrowa czymś więcej niż tylko przykładem. To przypadek założycielski, soczewka skupiająca kluczowe pojęcia NAT: złożoność interakcyjną, ścisłe sprzężenie, szum informacyjny, zawodność procedur, paradoks redundancji oraz presję czasu i skłonność organizacji do zrzucania winy na operatorów. TMI nie jest historią o jednym człowieku, który „źle nacisnął przycisk”, ani prostą opowieścią o pojedynczym, zaciętym zaworze. To historia systemu, który wytworzył sytuację poznawczo nieprzejrzystą i operacyjnie pilną. Operatorzy musieli działać szybko, choć nie byli w stanie w pełni pojąć przebiegu zdarzeń. Właśnie w tym napięciu rodzi się normalny wypadek. Najbardziej niebezpieczna awaria to nie zawsze ta, która od razu krzyczy. Czasem najgroźniejsza jest ta, która mówi półprawdą.

Refleksje Perrowa wyrosły z analizy zdarzeń z 1979 roku. Dostrzegł on w nich coś, czego nie da się uczciwie wyjaśnić tradycyjnym językiem „awarii technicznej" czy „błędu ludzkiego". W TMI ujawniła się struktura zdarzenia systemowego: kilka drobnych usterek, z których każda z osobna wydawała się opanowywalna, weszło w konfigurację nieprzewidzianą przez projektantów, procedury i modele mentalne obsługi. Tradycyjne ujęcie sugerowałoby, że najpierw wystąpił problem techniczny, a potem operatorzy zareagowali błędnie. Takie wyjaśnienie jest jednak zbyt ubogie – więcej zasłania, niż odsłania. Sednem TMI był fakt, że system dostarczał ludziom sygnały niepełne, mylące i sprzeczne.

Operatorzy nie obserwowali reaktora bezpośrednio; patrzyli na świat zbudowany z lampek, wskaźników, alarmów i procedur. Ten obraz zaczął rozmijać się z rzeczywistością, co jest klasycznym przejawem systemów interakcyjnie złożonych. Awaria nie jest tu jedynie stanem technicznym, lecz przede wszystkim kryzysem informacji. Zgodnie z rekonstrukcją zdarzeń w krótkim czasie wystąpiło kilka niezależnych zakłóceń: zablokowany polerownik kondensatu, problemy z zaworami awaryjnymi, zacięty zawór PORV oraz błędny wskaźnik sugerujący jego zamknięcie. Żadne z tych zdarzeń nie powinno być analizowane w izolacji. Sam zablokowany element czy pojedynczy zacięty zawór nie tłumaczą katastrofy; dopiero ich interakcja sprawia, że system przestaje być czytelny. Należy podkreślić: operatorzy nie działali w świecie obiektywnym, dostępnym później dla komisji śledczej, lecz w świecie odczytów. Jeśli kontrolka sugerowała zamknięcie zaworu, który w rzeczywistości pozostawał otwarty, operatorzy mierzyli się nie z samą awarią, lecz z jej fałszywą reprezentacją.

Wyobraźmy sobie kierowcę, któremu wskaźnik paliwa pokazuje pełny bak, mimo że zbiornik jest pusty. Można później stwierdzić: „powinien był zatankować", jednak jego świat decyzyjny podawał mu inną informację. W systemie jądrowym konsekwencje takiej rozbieżności są nieporównanie poważniejsze, ale logika poznawcza pozostaje ta sama: człowiek reaguje na model rzeczywistości dostarczony przez system. Jeśli ten model kłamie, nawet rozsądne działanie może stać się niebezpieczne.

Systemowa nieczytelność i wymuszony błąd operatora

W analizie TMI kluczową rolę odgrywa zawór PORV – zawór upustowy, który zaciął się w pozycji otwartej. Problem nie sprowadzał się jednak wyłącznie do samej awarii mechanicznej; krytyczna była kwestia systemu informacyjnego, który nie dostarczył operatorom wiarygodnego obrazu rzeczywistego stanu urządzenia. Wskaźnik sugerował zamknięcie, podczas gdy zawór nadal wypuszczał chłodziwo. To podręcznikowy przykład rozbieżności między stanem urządzenia

sterującego a stanem procesu fizycznego. System mógł informować o wysłaniu sygnału zamknięcia lub wskazywać w logice sterowania, że zawór powinien być zamknięty, lecz nie jest to to samo, co fizyczne potwierdzenie jego domknięcia. W normalnych warunkach ta różnica pozostaje niewidoczna; w kryzysie staje się dramatyczna.

Tu ujawnia się jeden z fundamentalnych problemów systemów wysokiego ryzyka: wskaźnik nie zawsze odzwierciedla rzeczywistość – czasem pokazuje jedynie intencję systemu wobec rzeczywistości. A intencja nie chłodzi rdzenia. Dla operatora różnica między „zawór powinien być zamknięty" a „zawór jest zamknięty" determinuje cały model sytuacji. Wiara w to, że zawór jest zamknięty, całkowicie zmienia interpretację poziomu wody, ciśnienia, alarmów i konieczności awaryjnego chłodzenia. Fałszywy sygnał nie jest zatem pojedynczym błędem informacyjnym, lecz błędem, który zakaża interpretację wszystkich pozostałych danych. Wypadek systemowy często zaczyna się właśnie w ten sposób: jeden fałszywy element nie tylko wprowadza w błąd, ale organizuje całe myślenie wokół błędnego założenia.

Jednym z najbardziej krytykowanych zachowań operatorów było ograniczenie działania awaryjnego wtrysku wody (HPI). Z perspektywy czasu wyglądało to fatalnie – skoro rdzeń wymagał chłodzenia, ograniczanie dopływu wody tylko pogarszało sytuację. Jednak właśnie tutaj Perrow wykazuje siłę swojej analizy. Decyzję należy oceniać w świetle tego, co operatorzy widzieli i rozumieli w danym momencie, a nie przez pryzmat pełnej wiedzy uzyskanej post factum. Obserwując rosnący poziom wody w stabilizatorze, działali zgodnie z modelem, w którym system mógł być przepełniony. Z ich perspektywy ograniczenie wtrysku nie było kaprysem ani głupotą, lecz reakcją spójną z interpretacją dostępnych sygnałów. Problem polegał na tym, że sygnały te były mylące, gdyż prawdziwy stan systemu został zamaskowany przez kombinację awarii i błędnych informacji.

To moment, w którym banalna narracja o "błędzie operatora" pęka. Operatorzy podjęli decyzję, która okazała się błędna, ale nie z powodu lekceważenia sytuacji, lecz dlatego, że system skłonił ich do mylnego rozpoznania stanu rzeczy. Perrow nie twierdzi, że ludzie są nieomylni; wskazuje raczej, że w systemach tego typu błąd człowieka często jest wymuszony poznawczo przez architekturę systemu. Nie jest to zwykłe usprawiedliwienie, lecz przesunięcie analizy z moralnej oceny jednostki na warunki możliwości działania. Jeśli system generuje fałszywy obraz, potrafi zmienić kompetentnego operatora w wykonawcę niebezpiecznej decyzji.

W książce pojawia się słowo „incomprehensible" – sytuacja stała się dla operatorów całkowicie niezrozumiała. Pojęcie to należy traktować poważnie. Nie chodzi o brak kwalifikacji czy niezrozumienie zasad pracy, lecz o fakt, że system wszedł w stan, w którym jego zachowanie przestało być czytelne nawet dla osób odpowiedzialnych za jego obsługę. Nieczytelność jest tu właściwością pewnych konfiguracji awaryjnych. W TMI operatorzy otrzymywali wiele sprzecznych

sygnałów jednocześnie: część wskazywała na jeden scenariusz, część na inny; jedne były konsekwencją pierwotnej awarii, inne skutkiem reakcji automatyki lub podjętych już decyzji.

System nie prezentował jednej, jasnej historii, lecz zbiór fragmentów, których nie dało się złożyć w poprawną całość. Zjawisko to jest szczególnie groźne, gdyż ludzki umysł dąży do spójności. W sytuacji kryzysowej operatorzy muszą zbudować jakiś model – nie mogą działać bez założeń. Gdy dane są sprzeczne, wybierają interpretację najlepiej pasującą do procedur, doświadczenia i najbardziej widocznych wskaźników. Paradoks polega na tym, że w wypadku systemowym to właśnie najbardziej widoczne wskaźniki bywają najbardziej mylące. Perrow przywołuje myśl, którą można sparafrazować tak: nie zawsze widzenie prowadzi do wiary; czasem trzeba najpierw uwierzyć w pewien model, aby móc zinterpretować dane jako sensowne. To nie słabość psychologiczna, lecz naturalny mechanizm poznawczy w warunkach niepewności, który w systemie wysokiego ryzyka staje się pułapką.

Paradoks procedur i nadmiarowości zabezpieczeń

W TMI problemem nie był wyłącznie sprzęt, lecz także procedury i modele działania. Procedury są tworzone dla określonych, rozpoznanych scenariuszy; zakładają one, że wystąpienie objawu X wymaga podjęcia działania Y. Pojawia się jednak pytanie: co, jeśli objaw X jest skutkiem nietypowej konfiguracji awarii? Co, jeśli działanie Y, właściwe w scenariuszu standardowym, okazuje się szkodliwe w konfiguracji rzeczywistej? I co, gdy operatorzy muszą wybierać między procedurą a intuicją, podczas gdy ta druga opiera się na błędnych danych?

TMI obrazuje dramat procedur w systemach złożonych. W systemie liniowym procedura funkcjonuje jak instrukcja naprawy. W systemie interakcyjnie złożonym może ona stać się mapą, która była prawdziwa wczoraj, ale dziś rzeka zmieniła koryto. Nie oznacza to, że procedury są zbędne — byłby to wniosek absurdalny. Wynika z tego raczej, że w systemach wysokiego ryzyka muszą być one projektowane wraz z mechanizmami rozpoznawania sytuacji, w których przestają pasować do rzeczywistości. Organizacja musi wiedzieć nie tylko, jak stosować instrukcję, ale także kiedy podejrzewać, że opisuje ona niewłaściwy świat. Jest to zadanie trudne, gdyż wymaga kultury operacyjnej łączącej dyscyplinę z krytycznym myśleniem. Niedobór dyscypliny prowadzi do chaosu, nadmiar zaś skutkuje zjawiskiem, jakim jest automatyczne wykonywanie błędu.

Katastrofa TMI ukazuje również ambiwalentną rolę zabezpieczeń. Systemy jądrowe obfitują w układy awaryjne, wskaźniki i redundancję, co w intuicji potocznej powinno oznaczać wyższy poziom bezpieczeństwa. Perrow nie zaprzecza konieczności stosowania zabezpieczeń, lecz twierdzi, że w systemie interakcyjnie złożonym każde dodatkowe rozwiązanie może stać się kolejnym

elementem złożoności. Zabezpieczenie wymaga sterowania, monitoringu i interpretacji; posiada własne sygnały oraz potencjalne tryby awarii. Może zadziałać poprawnie, lecz zostać źle odczytane, zadziałać częściowo lub zostać ograniczone w wyniku wcześniejszych procedur. Może również utwierdzić operatorów w poczuciu kontroli w momencie, gdy system wszedł już w stan nieprzewidziany. To paradoks technologicznego imperatywu bezpieczeństwa: organizacja reaguje na ryzyko, dodając kolejne warstwy techniczne, które jednocześnie powiększają liczbę możliwych interakcji.

W określonych warunkach system staje się bezpieczniejszy wobec znanych awarii, lecz mniej czytelny w obliczu tych nieznanych. Nie chodzi o porzucenie zabezpieczeń, lecz o zaprzestanie mylenia ich liczby z miarą bezpieczeństwa. Bezpieczeństwo nie rośnie automatycznie wraz z ilością urządzeń; wzrasta wtedy, gdy zabezpieczenia redukują niepewność, a nie ją przemnażają. W TMI kluczowe było to, że awaria rozgrywała się w systemie ściśle sprzężonym. Reaktor nie pozwala na odroczenie działań — procesy termiczne i ciśnieniowe zachodzą w czasie rzeczywistym, każda minuta zmienia stan instalacji, a decyzje muszą być podejmowane bezzwłocznie.

Systemowa pułapka błędu operatora

Operatorzy nie mieli luksusu pełnej diagnozy; musieli działać, zanim system stał się poznawczo przejrzysty. To właśnie połączenie nieczytelności z presją czasu jest najgroźniejsze. W systemie luźno sprzężonym można zatrzymać proces, sprawdzić dane, odizolować problem i porównać hipotezy. Jednak w systemie ściśle sprzężonym awaria nie czeka na seminarium. Nie daje czasu na pełne zrozumienie sytuacji, wymuszając decyzje oparte na niepełnych danych. Dlatego TMI stanowi tak silny argument Perrowa przeciwko naiwnemu optymizmowi w zarządzaniu ryzykiem.

Nie wystarczy stwierdzić, że należało lepiej przeszkolić operatorów. Szkolenie pomaga, lecz nie rozwiązuje sprzeczności między tempem zdarzeń a nieczytelnością systemu. Można wyszkolić ludzi do znanych scenariuszy, ale znacznie trudniej przygotować ich do konfiguracji, których nikt wcześniej nie potrafił sobie wyobrazić. Po katastrofach często pojawiają się oceny formułowane z wygodnej pozycji wiedzy po fakcie. Perrow przywołuje krytyczne uwagi wobec operatorów, w tym zarzut „nieświadomości" zagrożenia oraz oskarżenia o „głupie błędy". Perrow odpiera te interpretacje: to system spowodował wypadek, a nie operatorzy w prostym sensie tego słowa. Jest to kluczowe dla kultury bezpieczeństwa. Jeśli organizacja szybko znajduje winnych na pierwszej linii, może uniknąć pytań o projekt, procedury, przepływ informacji, sprzężenia i strukturę władzy. Kozioł ofiarny jest tani.

Zmiana architektury systemu jest droga. Obwinianie operatorów pełni kilka funkcji: uspokaja opinię publiczną prostą odpowiedzią, chroni prestiż technologii sugerując, że zawiódł człowiek, a nie system, zabezpiecza kierownictwo poprzez przeniesienie uwagi na ostatni etap działania i zdejmuje odpowiedzialność z regulatorów, którzy dopuścili taką konfigurację ryzyka. Z punktu widzenia prewencji jest to jednak fatalna droga. Jeśli źródłem wypadku była interakcja systemowa, ukaranie operatora nie usuwa warunków, które w przyszłości stworzą podobną pułapkę. Zmieni się człowiek przy pulpicie, ale pulpit będzie nadal mówił półprawdą.

Perrow nie twierdzi, że operatorzy w TMI działali idealnie – taki wniosek byłby równie uproszczony, co teza przeciwna. Jego stanowisko jest subtelniejsze i mocniejsze: kategoria „błędu operatora" może opisywać fragment zdarzenia, ale nie może być jego pełnym wyjaśnieniem. Decyzja, która po fakcie okazała się błędna, została ukształtowana przez: - fałszywe lub mylące wskaźniki, - niepełny obraz realnego stanu zaworu, - procedury dopasowane do innego scenariusza, - presję czasu wynikającą ze ścisłego sprzężenia, - złożoność interakcji między podsystemami, - wcześniejsze założenia szkoleniowe i mentalne modele pracy reaktora.

Pominięcie tych elementów na rzecz hasła „błąd operatora" daje wyjaśnienie moralnie wygodne, lecz naukowo słabe. To jak w analizie wypadku drogowego stwierdzenie, że kierowca skręcił w złym momencie, przy jednoczesnym pominięciu sprzecznych znaków, opóźnionej reakcji hamulców, oblodzonej nawierzchni i źle zsynchronizowanych świateł. Sam manewr jest faktem, ale nie jest całą przyczyną.

Three Mile Island to nie tylko studium technologii jądrowej, lecz lekcja epistemologii organizacyjnej – nauki o tym, jak organizacje wiedzą to, co wiedzą, i dlaczego mogą nie wiedzieć tego, co powinny. Systemy wysokiego ryzyka nie są czystą materią; są materią wraz z informacją o niej. Operator nie wkłada głowy do rdzenia reaktora, lecz otrzymuje reprezentację stanu systemu. Dlatego bezpieczeństwo zależy nie tylko od sprawności urządzeń, ale i od jakości tej reprezentacji: czy wskaźniki są właściwe, alarmy hierarchizowane, dane jednoznaczne, a procedury pomagają interpretować sytuację. TMI pokazuje, że system może być technicznie złożony i informacyjnie zwodniczy, co w układzie ściśle sprzężonym jest śmiertelnie groźne. Projektowanie bezpieczeństwa to zatem projektowanie prawdy operacyjnej. System nie powinien tylko działać – powinien umieć powiedzieć ludziom, co naprawdę się z nim dzieje.

Fałszywe wskaźniki jako źródło ryzyka systemowego

Analiza TMI dostarcza silnych analogii dla państwa, administracji i dużych organizacji. W instytucjach również funkcjonują zawory PORV – elementy, których realny stan różni się od tego,

co sugeruje formalny wskaźnik. System informatyczny wskazuje, że sprawa została obsłużona, choć obywatel nie otrzymał rozstrzygnięcia. Raport potwierdza wykonanie procedury, podczas gdy problem społeczny narasta. Budżet wykazuje alokację środków, mimo że usługa publiczna nie działa. Wskaźnik odnotowuje spadek zaległości tylko dlatego, że zmieniono sposób ich liczenia. Audyt potwierdza zgodność formalną, choć operacyjnie system pozostaje kruchy. Ministerstwo prezentuje strategię, podczas gdy na dole brakuje narzędzi do jej realizacji.

To są instytucjonalne odpowiedniki fałszywych wskaźników. Nie zawsze wynikają one z oszustwa; często są efektem błędnego modelu informacji. Organizacja mierzy to, co łatwo zmierzyć, a następnie zaczyna wierzyć, że zmierzyła rzeczywistość. W państwie normalny wypadek może nastąpić wtedy, gdy decydenci reagują na wskaźniki, które przestały opisywać realny proces. Podobnie jak operator TMI mógł ufać stanowi zaworu, którego nie widział bezpośrednio, tak administracja może wierzyć w sprawność systemu, znając go wyłącznie z raportów. Niebezpieczeństwo pojawia się, gdy papier mówi "zamknięte", a rzeczywistość nadal jest otwarta.

Z perspektywy NAT najważniejsze lekcje TMI nie ograniczają się do pojedynczej modernizacji technicznej. Chodzi o całą filozofię projektowania systemów wysokiego ryzyka. Po pierwsze, kluczowe wskaźniki muszą odzwierciedlać realny stan procesów, a nie tylko status sygnałów sterujących. Jeśli operator musi wiedzieć, czy zawór jest fizycznie zamknięty, system nie może ograniczać się do informacji o wysłaniu polecenia zamknięcia. Po drugie, alarmy powinny być hierarchizowane i interpretowalne. Nadmiar powiadomień bywa równie groźny co ich brak, gdyż w kryzysie człowiek potrzebuje sensu, a nie kakofonii. Po trzecie, procedury muszą zawierać mechanizmy kwestionowania scenariusza. Dobra procedura nie tylko instruuje, co robić, ale pomaga rozpoznać moment, w którym sytuacja odbiega od założeń, dla których została napisana. Po czwarte, szkolenia powinny obejmować nie tylko standardowe reakcje, lecz także myślenie w warunkach sprzecznych danych. Operatorzy systemów wysokiego ryzyka muszą potrafić rozpoznać sytuacje, w których system informacyjny wprowadza ich w błąd. Po piąte, organizacja musi wypracować kulturę, w której zatrzymanie, spowolnienie lub zakwestionowanie procesu nie jest automatycznie uznawane za porażkę. W systemie ściśle sprzężonym każda możliwość odzyskania czasu staje się zasobem bezpieczeństwa.

Nowoczesna technologia ucyfrowiła problem systemowej nieczytelności

Po szóste, analiza powypadkowa musi badać nie tylko ostatnią decyzję, ale cały układ, który sprawił, że ta decyzja w danym momencie wydawała się sensowna. Można by rzec: TMI to historia

technologii z końca lat siedemdziesiątych; dziś dysponujemy lepszymi czujnikami, automatyką, symulacjami i procedurami.

To prawda, lecz tylko częściowo. Głęboka lekcja Perrowa nie starzeje się tak łatwo, ponieważ nie dotyczy konkretnego modelu reaktora, lecz relacji między złożonością, informacją, czasem a odpowiedzialnością. Współczesne systemy są jeszcze silniej powiązane, automatyka bardziej rozwinięta, a algorytmy podejmują decyzje szybciej niż ludzie.

Infrastruktury zostały połączone cyfrowo. Organizacje polegają na wskaźnikach, dashboardach i modelach predykcyjnych, przez co decydenci coraz częściej postrzegają rzeczywistość przez warstwy reprezentacji. Oznacza to, że problem TMI nie zniknął. Zmienił kostium. Dziś fałszywym wskaźnikiem może być nie lampka przy zaworze, lecz błędny model danych, mylący algorytm ryzyka, źle skalibrowany system ostrzegania, raport syntetyczny maskujący lokalną awarię czy cyfrowy status „zrealizowano" pozbawiony realnego efektu. Nowoczesność nie uwolniła nas od problemu Perrowa. Ona go ucyfrowiła.

Three Mile Island pokazuje, że „normalny wypadek" nie jest opowieścią o ludzkiej głupocie, lecz o ograniczeniach poznawczych w systemach, które same generują nieczytelność, a następnie wymagają natychmiastowej decyzji. Operatorzy mogą się mylić, ale kluczowe pytanie brzmi: dlaczego system stworzył sytuację, w której pomyłka była tak prawdopodobna, trudna do rozpoznania i kosztowna? TMI uczy, że w systemach wysokiego ryzyka bezpieczeństwo nie polega wyłącznie na mnożeniu urządzeń, procedur czy szkoleń. Polega na tym, by system był poznawczo uczciwy wobec ludzi, którzy mają go kontrolować. Powinien pokazywać prawdę o sobie, dawać czas na reakcję, izolować awarie, redukować fałszywe sprzężenia i nie karać operatorów za to, że nie widzą rzeczy, których system im nie wyświetla. Najkrócej: nie można wymagać trafnej decyzji od człowieka, któremu system podaje fałszywy obraz świata.

Analiza Three Mile Island pozwala zrozumieć, dlaczego Charles Perrow nie traktuje wszystkich niebezpiecznych technologii jednakowo. Jest to istotne, gdyż jego teoria bywa błędnie streszczana jako prosty pesymizm technologiczny: skoro złożone systemy zawodzą, należy odrzucić nowoczesność. To nieporozumienie. Perrow nie jest kaznodzieją powrotu do świeczki, konia i ręcznego liczydła. Jego stanowisko jest bardziej precyzyjne, a przez to bardziej wymagające.

Perrow pyta: jaki typ ryzyka wytwarza dany system? Jak bardzo jest on interakcyjnie złożony i ściśle sprzężony? Jakie są potencjalne kategorie ofiar, czy istnieją bezpieczniejsze alternatywy i kto ponosi koszty katastrofy? To nie moralna niechęć do technologii, lecz socjologiczna analiza architektury ryzyka.

Właśnie dlatego w jego ujęciu elektrownia jądrowa, zakład petrochemiczny, tama, kopalnia, lotnictwo, transport morski, misja kosmiczna czy inżynieria genetyczna nie należą do jednej kategorii. Wszystkie mogą być niebezpieczne, ale nie każda w ten sam sposób. W analizie systemowej sposób generowania zagrożenia jest ważniejszy niż sama jego obecność. Aby to zrozumieć, należy wrócić do mapy Perrowa.

Wysoka złożoność i ścisłe sprzężenie jako źródło nieuchronnych katastrof

Technologie można umieścić na dwóch osiach. Pierwsza to złożoność interakcyjna: pytanie o to, czy elementy systemu oddziałują przewidywalnie i liniowo, czy też w sposób ukryty, nieliniowy, pośredni i trudny do zrozumienia. Druga oś to sprzężenie: określa ono, czy system posiada luz, bufory, alternatywy i czas na reakcję, czy działa szybko, sztywno i bez marginesu błędu. Najgroźniejszy obszar znajduje się tam, gdzie spotykają się wysoka złożoność i ścisłe sprzężenie. To tam rodzą się normalne wypadki w najczystszej postaci.

Dzieje się tak nie dlatego, że ludzie są szczególnie nieodpowiedzialni, ale dlatego, że system może stać się jednocześnie nieczytelny i niecierpliwy. Nie daje się on zrozumieć, a jednocześnie wymaga natychmiastowej reakcji. System liniowy i luźno sprzężony jest znacznie łatwiejszy do poprawiania. System liniowy i ściśle sprzężony może być groźny, lecz jego awarie są zazwyczaj bardziej zrozumiałe. Z kolei system złożony, lecz luźno sprzężony, może stwarzać trudności organizacyjne, ale daje czas i przestrzeń na interpretację. Największy problem pojawia się w ćwiartce: złożone plus ciasno sprzężone. To właśnie tam Perrow każe nam zachować największą nieufność wobec słowa "kontrola".

Energetyka jądrowa jest dla Perrowa przypadkiem szczególnie problematycznym. Nie tylko ze względu na ogromne konsekwencje ewentualnej awarii, lecz dlatego, że łączy ona w sobie kilka najtrudniejszych cech systemu wysokiego ryzyka: procesy transformacyjne, ukryte reakcje, wysoką zależność od chłodzenia, ścisłe sprzężenie czasowe, pośrednie źródła informacji oraz potencjalne ofiary trzeciej i czwartej kategorii.

W reaktorze nie obserwujemy procesu tak, jak obserwuje się taśmę montażową. Nie widzimy bezpośrednio rdzenia, promieniowania, stanu materiałów, mikropęknięć czy dynamiki chłodziwa; operujemy na wskaźnikach, modelach i sygnałach. System jest więc poznawczo zapośredniczony. Gdy wskaźniki są prawdziwe, procedury adekwatne, a sytuacja typowa – organizacja może działać sprawnie. Jednak gdy kilka elementów zaczyna oddziaływać nieoczekiwanie, operatorzy mogą

zostać odcięci od rzeczywistego obrazu sytuacji. Perrow zwraca uwagę między innymi na problem kruchości rdzenia i zbiornika, na procesy zachodzące pod wpływem bombardowania neutronami oraz na ryzyko gwałtownych reakcji związanych z chłodzeniem. W tego typu systemie awaria nie jest wyłącznie kwestią wymiany części; może dotyczyć procesów, których graniczne zachowanie nie jest w pełni uchwytne w rutynowym działaniu.

Kluczowe jest jednak coś jeszcze: skutki awarii jądrowej nie kończą się na operatorach i bezpośrednich użytkownikach. Mogą one dotknąć osoby postronne oraz przyszłe pokolenia, co przesuwa analizę z poziomu techniki na poziom etyki i polityki. Kto ma prawo nakładać takie ryzyko na ludzi, którzy nie wyrazili zgody i nie czerpią proporcjonalnych korzyści?

Dlatego Perrow zalicza energetykę jądrową do systemów, które – w jego własnym rygorystycznym ujęciu – należałoby porzucić. Nie twierdzi on, że każda elektrownia musi jutro ulec katastrofie, lecz raczej, że jeśli taka wystąpi, jej skala, nieodwracalność, nieprzejrzystość i międzypokoleniowy charakter przekraczają próg społecznej akceptowalności. Jest to argument o strukturze ryzyka, a nie statystyczne straszenie. Jeszcze ostrzej Perrow ocenia broń jądrową.

Tu normalny wypadek łączy się z problemem celowego zniszczenia, błędnych alarmów, automatyzacji decyzji, wojskowej tajemnicy, systemów wczesnego ostrzegania i gigantycznego potencjału ofiar trzeciej oraz czwartej kategorii. Broń jądrowa jest systemem, w którym błąd interpretacji, fałszywy sygnał, awaria komunikacji, napięcie polityczne, presja czasu i ścisłe procedury odwetu mogą doprowadzić do katastrofy niewyobrażalnej. To system, który musi być zawsze gotowy, a jednocześnie nigdy nie powinien zostać użyty. Już sama ta sprzeczność ma charakter perrowowski: organizacja utrzymuje mechanizm, którego najwyższa sprawność polega na tym, że nie przejdzie do swojego ostatecznego działania.

Perrow widzi tu nie tylko ryzyko techniczne, ale problem władzy. Decyzje o istnieniu i utrzymywaniu takiego systemu podejmują elity polityczne i wojskowe, podczas gdy konsekwencje ewentualnej awarii, eskalacji lub użycia poniosłyby całe społeczeństwa, także te nieuczestniczące w decyzji. W tym przypadku rekomendacja Perrowa jest najostrzejsza: taki system należy demontować, gdyż jego potencjalne skutki są tak skrajne, że klasyczny rachunek kosztów i korzyści przestaje być moralnie oraz politycznie wystarczający.

Przemysł chemiczny i morski jako systemy wysokiego ryzyka

Zakłady petrochemiczne również stanowią systemy interakcyjnie złożone, często o ścisłym sprzężeniu. Opierają się na procesach transformacyjnych, w których substancje zmieniają swoje właściwości pod wpływem temperatury, ciśnienia, reakcji chemicznych i przepływów. Awaria pojedynczego elementu może tu błyskawicznie wywołać zmianę stężeń, wzrost ciśnienia, pożar, eksplozję lub skażenie. Operatorzy polegają na wskaźnikach, podczas gdy sytuacja kryzysowa rozwija się z ogromną dynamiką. Przykłady Texas City i Flixborough obrazują te mechanizmy. W pierwszym przypadku groźna konfiguracja procesu doprowadziła do niezamierzonego stężenia substancji i eksplozji. W drugim uszkodzony reaktor zastąpiono prowizorycznym obejściem, wykonanym pod presją utrzymania produkcji i bez należytych obliczeń konstrukcyjnych. Efektem było rozerwanie instalacji oraz wybuch chmury par cykloheksanu, co zniszczyło zakład i kosztowało życie 28 osób.

Przypadek Flixborough jest szczególnie pouczający, gdyż pokazuje, jak presja ekonomiczna staje się integralnym elementem systemu awarii. Katastrofa nie była wynikiem wyłącznie błędów chemicznych czy mechanicznych; wynikała z decyzji organizacyjnej o konieczności kontynuowania produkcji. Prowizoryczne rozwiązanie techniczne stanowiło odpowiedź na wymóg ciągłości działania, a „ciągłość działania” w systemach wysokiego ryzyka bywa często jedynie eufemizmem dla lekkomyślność w garniturze.

Mimo to Perrow nie traktuje przemysłu chemicznego w ten sam sposób co energetyki jądrowej. Wynika to z faktu, że chemia jest głęboko wpleciona w gospodarkę, medycynę, rolnictwo, transport i codzienne życie. Całkowite porzucenie tej technologii byłoby społecznie nierealistyczne. Dlatego rekomendacja nie brzmi: „natychmiast zdemontować”, lecz: radykalnie ograniczać ryzyko poprzez poprawę projektów, regulacje, zmniejszanie złożoności i wzmacnianie buforów, tak aby presja produkcyjna nigdy nie unieważniała bezpieczeństwa. To kluczowe rozróżnienie: Perrow nie pyta tylko o stopień zagrożenia systemu, ale także o jego zastępowalność, przynoszone korzyści oraz realną możliwość redukcji ryzyka.

Transport morski stanowi kolejny istotny przypadek, łącząc technologię ze zmiennym środowiskiem naturalnym i presją ekonomiczną. Statki są systemami technicznymi operującymi w warunkach niepewności: pogoda, prądy, ruch innych jednostek, zmęczenie załogi czy koszty opóźnień wynikające z harmonogramu. Perrow analizuje m.in. kolizje tankowców, w których załogi błędnie konstruowały obraz sytuacji na podstawie niepełnych informacji. W transporcie morskim

kluczową rolę odgrywa społeczna konstrukcja rzeczywistości: załoga musi zinterpretować intencje innych jednostek, ocenić odległości i przewidzieć manewry w kontekście własnych ograniczeń.

Jeśli model sytuacji jest błędny, kolejne działania ratunkowe mogą jedynie pogłębić problem. Przykład Torrey Canyon ukazuje splot presji ekonomicznej i decyzyjnej: skrócenie trasy, chęć zdążenia przed odpływem oraz manewry w trudnym obszarze, zwieńczone błędem w trybie sterowania. Nie mamy tu do czynienia z pojedynczym, prostym błędem, lecz z systemową niewydolnością.

Różnice między ryzykiem systemowym a liniowym

Mamy konkretną konfigurację: harmonogram, decyzja kapitana, środowisko, technika sterowania, ograniczenia czasowe i wielka masa statku, której nie zatrzymuje się jak roweru pod sklepem. Transport morski toksycznych i wybuchowych materiałów Perrow zalicza do systemów wymagających rygorystycznego ograniczenia i modyfikacji. Nie chodzi o to, że każdy transport morski jest nietolerowalny. Chodzi o to, że przewożenie skrajnie niebezpiecznych ładunków na ogromne odległości, w trudnych warunkach, w imię prywatnego zysku – przy potencjalnych kosztach przerzucanych na środowisko i osoby postronne – wymaga zupełnie innego rygoru społecznego. Inaczej mówiąc: jeśli ryzyko jest publiczne, zysk prywatny nie może być jedynym kompasem.

Lotnictwo stanowi jeden z najciekawszych przypadków, ponieważ intuicyjnie wydaje się systemem ekstremalnie ryzykownym. Samolot jest technicznie skomplikowany, a błąd może być śmiertelny. A jednak sektor ten osiągnął bardzo wysoki poziom bezpieczeństwa. Perrow uznaje go za system, który można tolerować i udoskonalać, między innymi dlatego, że posiada liczne bufory, silną kulturę uczenia się, powtarzalność operacji oraz możliwość analizowania ogromnej liczby startów, lądowań i incydentów. To ważna korekta wobec zbyt prostego pesymizmu.

Lotnictwo pokazuje, że system ryzykowny może być zarządzany skutecznie, jeśli towarzyszą mu odpowiednie warunki organizacyjne: standardy, trening, symulacje, raportowanie incydentów, niezależne badanie wypadków i redundancja. Kluczowa jest tu zdolność uczenia się na zdarzeniach, które nie zakończyły się katastrofą. Lotnictwo korzysta z powtarzalności procesów i ogromnej liczby operacji; pozwala to wykrywać wzorce, analizować bliskie pomyłki oraz poprawiać konstrukcje i procedury. To odróżnia je od systemów, w których pojedyncza katastrofa może być tak wielka, że „uczenie się” na niej jest społecznie niedopuszczalne. Nie oznacza to, że lotnictwo jest wolne od wypadków. Historia zna przypadki złożonych interakcji między automatyką, pilotami, pogodą, obsługą techniczną i organizacją. Jednak jako sektor wypracowało ono mechanizmy wysokiej

niezawodności, które realnie zmniejszają ryzyko. W tym miejscu Perrow może spotkać się z teorią HRT: tam, gdzie system daje się trenować, obserwować, raportować i poprawiać, wysoka niezawodność nie jest pustym hasłem. Najważniejsza lekcja lotnictwa brzmi: bezpieczeństwo nie wynika z jednego geniuszu technicznego, lecz z całej kultury instytucjonalnej, która traktuje incydent jako źródło wiedzy, a nie jako pretekst do polowania na kozła ofiarnego.

Kontrola ruchu lotniczego posiada wiele cech systemu ściśle sprzężonego: decyzje są czasowo wrażliwe, błędy mogą się szybko kumulować, informacja musi być stale aktualizowana, a w powietrzu znajduje się wiele obiektów jednocześnie. A jednak system ten osiąga wysoką niezawodność dzięki intensywnemu szkoleniu, procedurom, technice, redundancji komunikacyjnej i standaryzacji kultury operacyjnej. To przykład systemu, w którym sama groźba nie przesądza jeszcze o nietolerowalności. Kluczowe jest to, czy organizacja potrafi skutecznie monitorować, korygować i wyciągać wnioski. Jeśli błędy są wykrywane wcześnie, system absorbuje zakłócenia, personel jest dobrze wyszkolony, a kanały komunikacji umożliwiają natychmiastową korektę – ryzyko można poważnie ograniczyć. Ale nawet tutaj Perrow kazałby zachować sceptycyzm.

Każdy wzrost zagęszczenia ruchu, każda automatyzacja, nowy system informatyczny czy presja kosztowa mogą zmieniać parametry ryzyka. Wysoka niezawodność nie jest stanem danym raz na zawsze; to praktyka nieustannego utrzymywania czujności. Instytucja może być HRO w poniedziałek i przestać nią być w piątek, jeśli ktoś w środę postanowił „zoptymalizować" obsadę.

Perrow wyróżnia tamy i kopalnie jako systemy bardzo niebezpieczne, których awarie jednak częściej mają charakter liniowy niż systemowy. Pęknięcie tamy może zabić tysiące ludzi, a wypadek w kopalni być tragedią dla pracowników i ich rodzin. Mechanizmy tych katastrof bywają jednak bardziej zrozumiałe: zły projekt, słaby materiał, błędna ocena geologii, brak konserwacji, zaniedbanie wentylacji czy ignorowanie znanych zagrożeń.

To rozróżnienie jest etycznie ważne. Nie oznacza ono, że życie górników czy mieszkańców doliny jest mniej cenne, lecz że droga poprawy bezpieczeństwa jest inna. W systemach liniowych skuteczniej działają klasyczne narzędzia: lepsze normy, inspekcje, rygorystyczne projektowanie i konserwacja, egzekwowanie przepisów, szkolenia oraz sprzęt ochronny. Porażka wynika tu częściej z zaniedbania znanego ryzyka niż z tajemniczej interakcji ukrytych podsystemów. To czyni odpowiedzialność bardziej uchwytną. Można wskazać, kto zlekceważył ostrzeżenia lub oszczędzał na zabezpieczeniach. Inaczej mówiąc: w systemie liniowym problemem bywa brak dyscypliny wobec wiedzy, którą już mamy. W systemie interakcyjnie złożonym problemem jest również to, że nie wiemy, czego nie wiemy.

Misje kosmiczne są dla Perrowa fascynującym polem analizy, gdyż łączą skrajną techniczną złożoność, ograniczone zasoby i środowisko wrogie życiu z ścisłymi zależnościami między podsystemami. Przykład Apollo 13 pokazuje niemal podręcznikowy wypadek systemowy: wcześniejszy błąd testowy, niewidoczny defekt, iskra, eksplozja zbiornika tlenu, sprzeczne wskaźniki i konieczność improwizacji. A jednak Apollo 13 jest także historią sukcesu organizacyjnego. System posiadał niezwykły zasób: ludzi zdolnych do improwizacji, zapasowy moduł, intensywne wsparcie naziemne i kulturę rozwiązywania problemów, co pozwoliło przekształcić lądownik księżycowy w „szalupę ratunkową". To dowodzi, że nawet w systemie wysokiego ryzyka odpowiednie bufory i kompetencje mogą uratować sytuację. Apollo 13 uczy więc dwóch rzeczy naraz.

Typologia technologii i ryzyka ekosystemowego

Po pierwsze, nawet starannie zaprojektowany system może stać się areną nieoczekiwanych interakcji awaryjnych. Po drugie jednak zdolność do improwizacji, redundancja funkcjonalna i kompetencje zespołów mogą złagodzić skutki katastrofy. To istotna korekta wobec fatalizmu: choć wypadek może być wpisany w strukturę systemu, jego finał nie musi być ostateczny. Różnica tkwi w tym, czy system posiada margines błędu, odpowiednich ludzi, alternatywy i kulturę operacyjnej wyobraźni.

Szczególnie pouczające są przypadki, które Perrow określa mianem wypadków ekosystemowych. Przykład jeziora Peigneur obrazuje, jak dwa pozornie niezależne systemy – wiertnia ropy i kopalnia soli – zostały połączone przez środowisko naturalne w sposób katastrofalny. Przewiercenie się do kopalni wywołało spływ wody z jeziora, powstanie gigantycznego wiru oraz wciągnięcie platformy, barek i elementów otoczenia.

Jest to przypadek kluczowy dla współczesnego myślenia o ryzyku, gdyż dowodzi, że granice systemów są często umowne. Firma wiertnicza widzi swój system, kopalnia – swój, a regulator operuje sektorami. Przyroda natomiast widzi połączenia. Wypadek ekosystemowy przypomina, że środowisko nie jest tłem, lecz aktywnym medium sprzężenia. Dwa systemy mogą funkcjonować liniowo osobno, ale gdy zostaną połączone przez wodę, geologię, atmosferę, łańcuch pokarmowy czy klimat, mogą stworzyć złożoną katastrofę. Ma to fundamentalne znaczenie dla inżynierii genetycznej, biotechnologii, rolnictwa przemysłowego, gospodarki wodnej, energetyki, urbanistyki i walki ze zmianami klimatycznymi. Natura nie uznaje granic resortowych. Nie składa wniosków o uzgodnienie międzyinstytucjonalne – ona po prostu przenosi skutki.

Perrow traktuje inżynierię genetyczną inaczej niż energetykę jądrową, dostrzegając w niej ogromny potencjał dla medycyny, rolnictwa czy ochrony zdrowia. Właśnie dlatego nie zaleca jej prostego odrzucenia, lecz rygorystyczne ograniczanie i regulowanie; korzyści mogą być bowiem wielkie, podczas gdy ryzyka – zwłaszcza ekologiczne i militarne – pozostają trudne do oszacowania. Najbardziej niepokojąca jest tu możliwość wystąpienia wypadków ekosystemowych. Organizmy, geny, patogeny i wektory biologiczne mogą tworzyć sprzężenia, których po uwolnieniu nie da się zamknąć w murach laboratorium. W przeciwieństwie do maszyn, systemy biologiczne rozmnażają się, adaptują i wchodzą w relacje z istniejącymi ekosystemami, co radykalnie zmienia strukturę ryzyka. W maszynie można czasem wyłączyć zasilanie. W ekosystemie "wyłączenie" bywa metaforą bez przełącznika.

Perrow obawia się także połączenia inżynierii genetycznej z bronią biologiczną oraz presji zysku, która może przyspieszać wdrożenia, zanim społeczeństwo i organy regulacyjne zrozumieją skalę konsekwencji. Nie jest to argument przeciwko wiedzy, lecz przeciwko pośpiechowi, który udaje postęp, a w rzeczywistości prywatyzuje korzyści i uspołecznia ryzyko.

Wnioski Perrowa można uporządkować w trzy grupy. Pierwsza obejmuje systemy, które należy porzucić, gdyż ich potencjał katastrofalny, nieodwracalność skutków oraz ryzyko dla osób postronnych i przyszłych pokoleń przeważają nad racjonalnymi korzyściami – do tej kategorii zalicza broń jądrową i energetykę jądrową. Druga grupa to systemy wymagające radykalnego ograniczenia, regulacji i modyfikacji, m.in. morski transport skrajnie niebezpiecznych substancji oraz inżynieria genetyczna.

Nie są to technologie, które Perrow nakazuje unicestwić, lecz takie, które wymagają surowego nadzoru, redukcji pośpiechu i ograniczenia prymatu zysku, przy jednoczesnym uznaniu, że koszty mogą spaść na ludzi niepodejmujących świadomie ryzyka. Trzecia grupa to systemy tolerowalne i możliwe do usprawniania: zakłady chemiczne, lotnictwo, kontrola ruchu lotniczego, górnictwo, tamy czy bezpieczeństwo drogowe. Nie dlatego, że są bezpieczne z natury, lecz dlatego, że można je skuteczniej poprawiać poprzez projektowanie, regulacje, kulturę bezpieczeństwa, szkolenia i uczenie się na błędach.

To podejście pragmatyczne: nie każda groźna technologia wymaga tej samej odpowiedzi. Państwo nie powinno ani ślepo czcić technologii, ani bezkrytycznie jej potępiać. Powinno pytać: jaki to system, jakie ma sprzężenia, kto ponosi ryzyko, czy istnieją alternatywy i czy korzyści nie są kupowane cudzym strachem. Perrow krytykuje również wąsko rozumianą ocenę ryzyka, która redukuje problem do statystycznych prawdopodobieństw i strat finansowych. Statystyka jest potrzebna, ale nie wystarcza.

Społeczeństwa inaczej oceniają ryzyko dobrowolne i narzucone, znane i nieznane, lokalne i masowe, odwracalne i nieodwracalne. Ryzyko osoby prowadzącej samochód nie jest tożsame z ryzykiem skażenia całego regionu. Ryzyko zawodowe operatora różni się od ryzyka dziecka mieszkającego obok zakładu. Ryzyko krótkotrwałe nie jest tym samym, co ryzyko genetyczne lub ekologiczne.

Regulacja oparta na architekturze ryzyka zamiast błędu ludzkiego

Technokrata może argumentować, że prawdopodobieństwo awarii jest małe. Społeczeństwo odpowie jednak: ale skutek jest niewybaczalny. Taka postawa nie musi być nieracjonalna; może opierać się na racjonalności kulturowej i społecznej, w której znaczenie ma nie tylko średnia strata, lecz także charakter krzywdy, dobrowolność narażenia, możliwość kontroli, sprawiedliwość rozłożenia kosztów oraz prawo przyszłych pokoleń do świata nieuszkodzonego przez cudzą kalkulację. Nie wszystko, co statystycznie rzadkie, jest politycznie akceptowalne.

Zastosowanie tej typologii w praktyce państwowej prowadzi do konkretnego wniosku: regulacje nie powinny być jednakowe dla wszystkich sektorów, lecz zależeć od architektury ryzyka. Inaczej należy regulować system liniowy i lokalny, inaczej system interakcyjnie złożony, ale luźno sprzężony, a jeszcze inaczej system złożony i ściśle sprzężony, którego awaria może dotknąć osoby postronne i przyszłe pokolenia. Prawo „dla wszystkich” bywa wygodne administracyjnie, lecz ślepe systemowo. Regulator powinien zatem pytać: czy system można zatrzymać bez katastrofy? Czy awaria pozostanie lokalna, czy może się rozlać? Czy informacje są bezpośrednie, czy pośrednie? Czy operatorzy widzą realny stan procesu i czy istnieją alternatywne ścieżki działania? Czy korzyści i ryzyka ponoszą ci sami ludzie? Czy skutki awarii są odwracalne i czy możliwe jest uczenie się na małych błędach? Czy prywatny zysk nie wymusza publicznego ryzyka?

Taka regulacja w duchu Perrowa oznacza mniej wiary w deklaracje bezpieczeństwa, a więcej analizy sprzężeń. Porównanie technologii wysokiego ryzyka pokazuje, że teoria normalnych wypadków nie jest prostym antytechnologicznym manifestem, lecz metodą rozróżniania. Perrow nie twierdzi, że wszystko jest niebezpieczne i należy to odrzucić. Sugeruje raczej: sprawdźmy, które systemy mają taką strukturę, że ich katastrofy są wpisane w logikę działania; sprawdźmy, czy możemy je rozluźnić, uprościć, regulować, zastąpić albo porzucić. To myślenie dojrzałe, gdyż nie utożsamia postępu z automatycznym dobrem. Nowoczesność nie jest niewinna tylko dlatego, że jest nowoczesna, a technologia nie otrzymuje immunitetu od etyki dzięki skomplikowanej aparaturze i certyfikatom. System mogący skrzywdzić osoby postronne i przyszłe pokolenia musi być oceniany

surowiej niż taki, którego awaria dotyka głównie świadomych uczestników. Najkrócej: nie pytajmy tylko, jak często system zawodzi, lecz co się dzieje, gdy zawiedzie – i kto zapłaci rachunek.

Po analizie technologii wysokiego ryzyka należy przejść z poziomu maszyn, reaktorów czy zakładów chemicznych do figury najbardziej niewygodnej: człowieka stojącego najbliżej awarii. W teorii Charlesa Perrowa jest nim operator – pilot, dyspozytor, technik, lekarz na dyżurze czy urzędnik obsługujący krytyczny proces; człowiek, którego ręka, głos, decyzja albo zaniechanie stają się widoczne w ostatnich minutach przed katastrofą. W klasycznych raportach powypadkowych osoba ta często zostaje nazwana sprawcą. Mówi się o „błędzie operatora", „błędzie ludzkim" czy „braku należytej ostrożności". Perrow nie zaprzecza, że ludzie popełniają błędy – przeciwnie: robią to stale, bo są ludźmi, a nie aniołami z certyfikatem ISO. Jego argument jest jednak poważniejszy: w systemach interakcyjnie złożonych i ściśle sprzężonych kategoria „błędu operatora" zbyt często działa jak organizacyjny parawan, który zasłania architekturę awarii.

Najłatwiej obwinić człowieka przy pulpicie; najtrudniej system, który przez lata projektowano tak, by w chwili próby generował nieczytelność, presję czasu i fałszywe sygnały. W wielu analizach „błąd ludzki" pojawia się jako przyczyna dominująca – według perspektywy Perrowa przypisuje mu się często odsetek awarii rzędu 60-80 procent. Już ta liczba powinna budzić sceptycyzm. Jeśli niemal wszystko tłumaczymy błędem człowieka, być może nie odkryliśmy prawdy, lecz stworzyliśmy pojemnik na niewiedzę. „Błąd ludzki" bywa kategorią wygodną i elastyczną: może oznaczać złą diagnozę, opóźnioną reakcję, nieuwagę czy naruszenie procedury. Problem polega na tym, że tak szeroka kategoria zaczyna wyjaśniać wszystko, a przez to przestaje wyjaśniać cokolwiek.

Perrow nakazuje zapytać: czy operator popełnił błąd mimo dobrego systemu, czy dlatego, że system skonstruował warunki błędu? To rozróżnienie jest zasadnicze. Jeżeli człowiek dysponował jasną informacją, czasem i realnymi alternatywami, a mimo to działał rażąco źle, odpowiedzialność jednostkowa jest silna. Jeśli jednak działał pod presją sekund, wśród sprzecznych alarmów i fałszywych wskaźników, w systemie o niewidocznym stanie, słowo „błąd" opisuje jedynie powierzchnię. Głębiej znajduje się pytanie o projekt, sprzężenia, procedury, szkolenia oraz kulturę organizacyjną i presję produkcyjną.

Systemowa nieprzejrzystość i pułapka wiedzy po fakcie

W ujęciu Perrowa operator nie jest postacią idealizowaną ani całkowicie bezbronną, lecz człowiekiem wpisanym w strukturę systemu. Posiada określone kompetencje, obowiązki i ograniczenia, kieruje się rutynami oraz modelami mentalnymi i ponosi odpowiedzialność. Jednak w systemach normalnych wypadków może stać się on pierwszą ofiarą systemowej nieprzejrzystości.

To kluczowe przesunięcie akcentów: katastrofa nie zawsze wynika z faktu, że operator czegoś „nie widzi". Często zaczyna się od tego, że system nie pokazuje stanu faktycznego. Nie prezentuje realnego położenia zaworu, lecz stan sygnału sterującego; nie pokazuje rzeczywistego przepływu, lecz pośredni odczyt. Nie ukazuje konfiguracji awarii, lecz zestaw alarmów, z których każdy osobno ma sens, ale razem tworzą kakofonię. System nie wskazuje przyczyny, lecz skutki; nie pokazuje sieci, lecz fragmenty. W takiej sytuacji operator buduje obraz świata z dostępnych elementów. Jeśli są one mylące, może stworzyć obraz spójny, lecz fałszywy. Tak właśnie wypadek systemowy staje się także katastrofą poznawczą. Człowiek nie tyle „nie chce wiedzieć", ile nie ma dostępu do prawdy w czasie, w którym decyzja jest jeszcze skuteczna. Operator nie jest zatem jedynie wykonawcą procedur, lecz interpretatorem systemu. Jeśli system posługuje się językiem sprzecznych znaków, interpretator może popełnić błąd bez winy w potocznym rozumieniu tego słowa.

Można go później osądzić, jednak rzetelna analiza musi najpierw odtworzyć jego świat informacyjny. Jednym z najsilniejszych mechanizmów niesprawiedliwego obwiniania operatorów jest hindsight bias, czyli złudzenie wiedzy po fakcie. Po katastrofie znamy sekwencję zdarzeń. Wiemy, który sygnał był decydujący, który wskaźnik wprowadzał w błąd i jaka procedura okazała się nieadekwatna. Wiemy, które zabezpieczenie zawiodło i że należało postąpić inaczej. Jednak wiedza po fakcie nie była dostępna w trakcie zdarzenia. To oczywistość, którą należy powtarzać, gdyż instytucje nieustannie ją ignorują. Komisja powypadkowa dysponuje czasem, dokumentacją, ekspertami, zapisami i symulacjami w spokojnej sali konferencyjnej. Operator miał jedynie alarmy, presję czasu, fragmentaryczne dane i tykający zegar.

Różnica między tymi pozycjami poznawczymi jest fundamentalna. Z perspektywy czasu nawet skomplikowana katastrofa jawi się jako prosta ścieżka. Dlatego raporty i komentarze medialne tak łatwo stwierdzają: „wystarczyło zauważyć", „należało sprawdzić" lub „powinni byli przewidzieć". Czasem jest to prawda, często jednak stanowi to retoryczna przemoc wiedzy późniejszej nad człowiekiem, który działał wcześniej. Perrow przypomina: analiza musi odtworzyć nie tylko obiektywną sekwencję awarii, lecz także subiektywnie dostępny obraz sytuacji. W przeciwnym razie mylimy rekonstrukcję z oceną.

Błędy wymuszone jako efekt systemowej hipokryzji

Szczególnie istotna u Perrowa jest kategoria błędów wymuszonych. Dotyczy ona sytuacji, w których organizacja formalnie wymaga bezpieczeństwa, lecz w praktyce wymusza zachowania ryzykowne. Pracownik ma przestrzegać procedur, a jednocześnie utrzymać tempo. Powinien zatrzymać proces w razie zagrożenia, ale wie, że przestój będzie kosztowny i źle oceniony. Ma nie obchodzić

zabezpieczeń, choć te przeszkadzają w realizacji nierealnej normy. Ma działać ostrożnie, lecz system wynagradza szybkość. To centralna hipokryzja wielu organizacji wysokiego ryzyka: bezpieczeństwo jest na plakatach, wydajność w premiach. Perrow dowodzi, że w takich warunkach „błąd operatora" może być w istocie błędem organizacji przeniesionym na najniższy poziom. Człowiek łamie procedurę, bo inaczej nie wykona zadania; obchodzi zabezpieczenie, by linia nie stanęła; podejmuje decyzję bez pełnych danych, gdyż system nie przewidział czasu na ich zebranie; improwizuje, ponieważ formalne narzędzia są nieadekwatne. Po wypadku organizacja odkrywa z oburzeniem, że pracownik robił dokładnie to, czego od dawna milcząco od niego oczekiwano.

Wnioski te mają kluczowe znaczenie dla analizy państwa i administracji. Gdy urzędnik ma załatwiać sprawy szybko przy niejasnych przepisach; gdy lekarz ma zachować standard mimo zbyt małej obsady; gdy policjant ma działać rozważnie pod presją polityczną i medialną; gdy nauczyciel ma indywidualizować pracę, będąc obciążonym biurokracją – wtedy błędy jednostek są wymuszane przez architekturę pracy. Pytanie „kto zawinił?" należy wówczas poprzedzić pytaniem: kto zaprojektował niemożliwe warunki poprawnego działania? Perrow zauważa, że obwinianie operatora ma często wymiar klasowy i hierarchiczny. Łatwiej wskazać pracownika pierwszej linii niż projektanta systemu, zarząd, regulatora, ministerstwo czy radę nadzorczą. Prościej stwierdzić, że „technik nie dopilnował", niż przyznać, iż model biznesowy usuwał rezerwy bezpieczeństwa. Łatwiej oskarżyć pilota, niż zapytać o szkolenia, harmonogramy i presję ekonomiczną. Łatwiej obciążyć urzędnika niż przyznać, że prawo było napisane jak labirynt po nocnym posiedzeniu komisji. Systemy władzy mają naturalną skłonność do przerzucania winy w dół. Dół jest widoczny, konkretny i wymienialny. Góra jest abstrakcyjna, kolegialna i otoczona językiem strategii.

Nie oznacza to, że pracownik pierwszej linii nigdy nie ponosi odpowiedzialności. Oznacza jedynie, że widoczność działania nie jest tożsama z głębokością przyczyny. Ostatni człowiek w sekwencji zdarzeń nie musi być pierwszym źródłem katastrofy. W instytucjach publicznych ten mechanizm jest szczególnie jaskrawy. Gdy system zawodzi, gniew obywatela spada na urzędnika przy okienku, pielęgniarkę na dyżurze, nauczyciela w klasie czy policjanta na miejscu zdarzenia.

Hierarchia ofiar i iluzja dobrowolnego ryzyka

Tymczasem realne źródła awarii mogą tkwić w budżecie, legislacji, informatyce, zarządzaniu kadrami, nadmiernej centralizacji, wadliwym nadzorze lub politycznych obietnicach bez pokrycia. Najniższy szczebel staje się twarzą systemu, lecz niekoniecznie jego mózgiem. Perrow nie analizuje człowieka w systemie wyłącznie przez pryzmat winy; kluczowe jest dla niego również pojęcie ofiar. Wyróżnia on cztery kategorie osób poszkodowanych. Pierwszą z nich są operatorzy i pracownicy

bezpośrednio związani z działaniem systemu. To oni znajdują się najbliżej instalacji, statku, reaktora, maszyny czy procesu technologicznego – najbliżej miejsca katastrofy. To oni często giną jako pierwsi albo ponoszą obrażenia. Paradoks jest brutalny: grupa, którą po katastrofie najłatwiej obwinić, jest często grupą, która jako pierwsza płaci ciałem. Operatorzy nie są abstrakcyjną funkcją; to pracownicy funkcjonujący w konkretnych warunkach ekonomicznych. Mogą być zmuszeni przez rynek pracy do podejmowania ryzyka, mogą nie mieć realnej siły negocjacyjnej lub pracować w kulturze, w której zgłaszanie zagrożeń jest niemile widziane. Bywają formalnie "uprawnieni" do zatrzymania procesu, lecz w praktyce karani za spowolnienie produkcji. Perrow każe więc rozumieć ryzyko zawodowe nie tylko technicznie, ale społecznie.

Nie zawsze jest to dobrowolny kontrakt równych stron. Często mamy do czynienia z układem, w którym pracownik sprzedaje swoją obecność w strefie ryzyka, a organizacja później udaje, że ta obecność była dowodem pełnej zgody na wszystko. Drugą kategorią są użytkownicy systemu i osoby funkcjonalnie z nim powiązane, choć nie mające wpływu na jego zarządzanie. Przykładem są pasażerowie samolotów, statków czy pociągów, ale także dostawcy i osoby wykonujące usługi na rzecz zakładu przemysłowego. Podejmują oni pewne ryzyko bardziej świadomie niż przypadkowi mieszkańcy, jednak nie kontrolują systemu, od którego zależy ich bezpieczeństwo.

Pasażer kupuje bilet, ale nie projektuje samolotu. Dostawca wjeżdża na teren zakładu, lecz nie ustala kultury bezpieczeństwa. Pracownik biurowy rafinerii przebywa w obrębie systemu, ale nie decyduje o stanie instalacji. Ich dobrowolność jest zatem częściowa. To istotne, gdyż w debacie publicznej często nadużywa się argumentu zgody: "wiedzieli, że istnieje ryzyko". Wiedzieć o abstrakcyjnym ryzyku to nie to samo, co mieć wpływ na jego strukturę. Pasażer wie, że lotnictwo nie jest metafizycznie wolne od wypadków, ale ufa, że system spełnia normy, regulator działa, linia nie oszczędza patologicznie, samolot jest sprawny, piloci nie są przemęczeni, a procedury nie są fikcją. Zgoda użytkownika opiera się więc na zaufaniu instytucjonalnym. Jeśli instytucje zawodzą, nie można łatwo stwierdzić: "sam się zgodził". Trzecia kategoria jest dla Perrowa szczególnie istotna: niewinne osoby postronne. To ludzie, którzy nie pracują w systemie, nie korzystają bezpośrednio z jego usług, nie czerpią proporcjonalnych korzyści i nie podpisali żadnego kontraktu z ryzykiem, a mimo to mogą ponieść skutki katastrofy. Mieszkańcy okolic zakładu chemicznego, ludzie żyjący w pobliżu elektrowni, społeczności narażone na skażenie czy osoby mieszkające poniżej tamy. Przechodnie, sąsiedzi, dzieci, lokalne wspólnoty. W ich przypadku dobrowolność ryzyka jest minimalna albo żadna. To przesuwa debatę z poziomu techniki na poziom sprawiedliwości.

Niesprawiedliwość rozkładu ryzyka i odpowiedzialność międzypokoleniowa

System wysokiego ryzyka przestaje być prywatną sprawą operatora i właściciela w momencie, gdy jego awaria może uderzyć w osoby postronne. Wówczas kwestia bezpieczeństwa zyskuje wymiar demokratyczny: kto ma prawo decydować o ryzyku narzucanym innym? Perrow krytykuje tutaj wąski rachunek ekonomiczny. Prywatny podmiot może wyliczać opłacalność inwestycji, lecz nie powinien mieć swobody w przerzucaniu katastrofalnego ryzyka na lokalną społeczność. Gdy korzyści są skoncentrowane, a ryzyko rozproszone, mamy do czynienia nie tylko z błędem w zarządzaniu, ale z problemem władzy. Tu pojawia się jedno z najostrzejszych pytań Perrowa: czy nowoczesne technologie wysokiego ryzyka nie stały się narzędziem, za pomocą którego elity gospodarcze i polityczne obciążają większość zagrożeniem, by generować zyski dla mniejszości?

Czwarta kategoria ofiar jest najbardziej dramatyczna: przyszłe pokolenia. Chodzi o ludzi, którzy nie przyszli jeszcze na świat, a mogą odziedziczyć skutki skażenia promieniotwórczego, toksycznego, chemicznego, biologicznego lub ekologicznego. Mowa tu o uszkodzeniach genetycznych, zniszczeniu środowiska, długotrwałym zatruciu łańcuchów pokarmowych i konsekwencjach, których obecne pokolenie nie będzie już musiało oglądać. Ta kategoria radykalnie komplikuje klasyczny rachunek ryzyka.

Przyszłe pokolenia nie mogą wyrazić zgody. Nie uczestniczą w konsultacjach społecznych, nie składają odwołań, nie wynajmują kancelarii, nie przychodzą na sesje rady gminy ani nie piszą skarg do regulatora. A mimo to ponoszą koszty decyzji podejmowanych dziś. To najpoważniejszy argument przeciwko technokratycznej nonszalancji. Jeśli ryzyko ma charakter międzypokoleniowy, nie wolno traktować go jak zwykłego parametru inwestycyjnego. Krótkoterminowa korzyść obecnych nie może mieć moralnego prawa automatycznie przeważać nad długotrwałą krzywdą tych, którzy nie mają głosu.

W tym punkcie Perrow zbliża się do filozofii odpowiedzialności. Systemy wysokiego ryzyka należy oceniać nie tylko przez pryzmat prawdopodobieństwa awarii, ale przede wszystkim przez charakter potencjalnych ofiar. Im mniej dobrowolna ekspozycja, im słabsza kontrola i większa nieodwracalność skutków, tym surowsze powinny być wymogi społecznej akceptacji. Perrow podkreśla istotną regułę: w miarę przechodzenia od pierwszej do czwartej kategorii ofiar rośnie liczba poszkodowanych, a ryzyko staje się coraz mniej znane, mniej dobrowolne i gorzej rekompensowane. Operator przynajmniej ma świadomość pracy w systemie ryzyka, choć jego zgoda bywa wymuszona ekonomicznie. Użytkownik wie, że korzysta z usługi lub transportu, lecz nie zna rzeczywistych parametrów bezpieczeństwa. Osoba postronna często nie posiada ani wiedzy,

ani wyboru. Przyszłe pokolenie w chwili podejmowania decyzji nie ma nawet istnienia politycznego. To tworzy geometrię niesprawiedliwości. Im dalej od centrum decyzji, tym większa bezbronność; im większa bezbronność, tym większy obowiązek ostrożności po stronie projektantów, regulatorów i eksploatatorów systemu.

Perrow jawi się zatem nie tylko jako socjolog organizacji, ale i teoretyk odpowiedzialności publicznej. Dowodzi, że ryzyko nie rozkłada się neutralnie – posiada strukturę klasową, przestrzenną, pokoleniową i polityczną. Po katastrofie kamera rejestruje miejsce zdarzenia, twarze ratowników, operatorów czy lokalnych kierowników. Rzadziej jednak pokazuje decyzje sprzed lat: oszczędności na konserwacji, redukcję personelu, lobbing przeciwko regulacjom, skracanie testów, outsourcing kompetencji, presję harmonogramu, tolerowanie nieformalnych obejść czy kulturę karania za zgłaszanie problemów. A przecież wypadek systemowy często ma długą prehistorię; ostatnie minuty są jedynie finałem. Wielu autorów katastrofy nie ma na miejscu w chwili wybuchu, pożaru czy skażenia.

Odpowiedzialność projektantów a mity o operatorach

Odpowiedzialność spoczywa w zarządach, ministerstwach, biurach projektowych i działach finansowych; w urzędach regulacyjnych i komisjach zatwierdzających, a także w systemach premiowych, które nagradzały wydajność kosztem ostrożności. Analiza Perrowa nakazuje rozszerzyć kadr: nie patrzeć wyłącznie na człowieka przy pulpicie, lecz na cały łańcuch decyzji. To on sprawił, że pulpit był taki, wskaźniki takie, procedury i obsada takie, presja taka, a możliwość zatrzymania procesu stała się politycznie lub ekonomicznie zbyt kosztowna.

Wymaga to innej kultury odpowiedzialności. Nie mniejszej, lecz większej. Odrzucenia narracji, że „nikt nie jest winny, bo system". Przeciwnie: skoro system został zbudowany przez ludzi, odpowiedzialność ponoszą ci, którzy go projektowali, utrzymywali, finansowali, deregulowali i nadzorowali, a także ci, którzy świadomie ignorowali sygnały ostrzegawcze.

System nie jest bogiem; ma swoich autorów. Organizacje zwykle operują dwoma skrajnymi mitami na temat operatorów. Pierwszy to mit heroiczny: wiara, że człowiek na pierwszej linii uratuje system dzięki odwadze, intuicji i poświęceniu. Drugi to mit winnego operatora: przekonanie, że jeśli system się zawali, to tylko dlatego, iż człowiek na pierwszej linii nie był dość dobry. Oba mity są niebezpieczne, gdyż przerzucają odpowiedzialność za architekturę całości na jednostkę. Mit heroiczny sugeruje, że nie trzeba projektować systemu wybaczającego błędy, bo „dobry człowiek sobie poradzi". Mit winnego operatora podpowiada, że nie trzeba zmieniać systemu – wystarczy zastąpić gorszego człowieka lepszym.

Perrow odrzuca oba te uproszczenia. Bezpieczeństwo nie powinno opierać się na standardowym wymogu bohaterstwa. Jeśli organizacja funkcjonuje tylko dlatego, że ludzie stale nadrabiają jej wady, to nie jest ona niezawodna. To organizacja pasożytująca na sumienności pracowników. Bohaterstwo bywa piękne w literaturze, lecz w zarządzaniu ryzykiem często stanowi dowód złego projektu.

Aby zachować równowagę, należy jasno stwierdzić: człowiek nie jest wyłącznie ofiarą systemu; może być także źródłem jego odporności. Ludzie potrafią dostrzegać anomalie, improwizować, łączyć dane, łamać rutynę i ratować sytuacje, których automatyka nie rozumie. Wiele katastrof zostało unikniętych właśnie dzięki mądrej reakcji osób na pierwszej linii.

To jednak wzmacnia, a nie osłabia argumentację Perrowa. Jeśli człowiek ma być źródłem odporności, system musi mu stworzyć odpowiednie warunki: zapewnić wiarygodne informacje, czas i prawo do zatrzymania procesu bez obawy o karę. Wymaga to szkolenia w myśleniu systemowym, możliwości komunikacji poziomej, dostępu do ekspertów oraz procedur, które pomagają, a nie kneblują. Człowiek nie jest magicznym bezpiecznikiem, lecz inteligentnym uczestnikiem systemu.

Można go przeciążyć, oślepić, zastraszyć lub zmusić do niemożliwego, ale można go też uczynić realnym elementem odporności. To decyzja organizacyjna. W administracji publicznej analogia jest oczywista: obywatel styka się z systemem poprzez osobę na pierwszej linii. Gdy sprawa utknie, winny wydaje się urzędnik; gdy pacjent czeka, rejestratorka lub lekarz; gdy szkoła nie działa – nauczyciel, a gdy pomoc społeczna zawodzi – pracownik terenowy. Choć jednostki czasem zawodzą, bardzo często są oni operatorami źle zaprojektowanego systemu. Zmagają się z brakiem czasu, nadmiarem spraw, sprzecznymi przepisami, wadliwym oprogramowaniem i presją przełożonych przy jednoczesnym gniewie obywateli.

Państwo, które stale obwinia pierwszą linię, uczy się błędnie. Zamiast naprawiać sprzężenia, wymienia twarze. Zamiast uprościć procedury, mnoży kontrole; zamiast dać zasoby – komunikaty; zamiast stworzyć bufory – kampanie informacyjne. W efekcie system publiczny może stać się maszyną do produkowania frustracji: obywatel obwinia urzędnika, ten przepisy, ministerstwo wykonawców, a wykonawcy system informatyczny, który milczy, bo jako jedyny rozumie, że nie musi niczego tłumaczyć.

Z teorii Perrowa można wyprowadzić zestaw pytań do każdej sytuacji, w której pojawia się zarzut błędu ludzkiego: Jakie informacje były dostępne operatorowi w chwili decyzji? Czy były one bezpośrednie, czy pośrednie? Czy wskaźniki pokazywały realny stan procesu, czy tylko stan urządzeń sterujących? Czy alarmy były hierarchiczne i zrozumiałe? Czy procedura pasowała do

rzeczywistej konfiguracji zdarzenia? Czy operator miał czas na diagnozę i mógł zatrzymać proces bez sankcji organizacyjnych? Czy szkolenie obejmowało podobne scenariusze? Czy presja ekonomiczna lub polityczna wymuszała tempo działania? Czy podobne odstępstwa były wcześniej tolerowane? Czy błąd był jednostkowy, czy powtarzalny w organizacji? I wreszcie: czy organizacja otrzymała sygnały ostrzegawcze i je zignorowała?

Spór między optymizmem organizacyjnym HRT a sceptycyzmem strukturalnym NAT

Dopiero po zadaniu tych pytań można uczciwie mówić o winie. Bez nich „błąd operatora" jest często tylko szybką etykietą naklejoną na wolno dojrzewającą katastrofę. Perrowowska analiza człowieka w systemie nie unieważnia odpowiedzialności jednostki, lecz ją cywilizuje. Pokazuje, że odpowiedzialność musi być przypisywana zgodnie z realną strukturą działania, a nie według prostoty medialnej narracji. Człowiek może popełnić błąd, ale system może ten błąd wymusić, ukryć, przyspieszyć lub uczynić nieodwracalnym, przerzucając koszty na ludzi, którzy nie mieli żadnego wpływu na decyzje. Dlatego w systemach wysokiego ryzyka pytanie o operatora musi prowadzić do pytania o projekt, władzę, zasoby, sprzężenia, procedury i sprawiedliwość rozkładu ryzyka. Najkrócej: nie każdy błąd człowieka jest ludzką przyczyną katastrofy; czasem jest ostatnim widocznym ruchem systemu, który zawodził już wcześniej.

Po omówieniu roli człowieka należy przejść do fundamentalnego sporu teoretycznego, jaki wyrasta wokół Charlesa Perrowa: starcia między Teorią Normalnych Wypadków (NAT – Normal Accident Theory) a Teorią Wysokiej Niezawodności (HRT – High Reliability Theory). To nie jest akademicka sprzeczka o etykiety, lecz spór o granice zarządzania, sens kultury bezpieczeństwa i możliwość uczenia się na błędach. Pytanie brzmi: czy wystarczy „bardziej się starać", by ujarzmić systemy, które same w sobie są nieprzejrzyste, szybkie i katastrofogenne?

W największym uproszczeniu HRT głosi, że organizacje mogą osiągać bardzo wysoki poziom bezpieczeństwa nawet w ryzykownych środowiskach, o ile są odpowiednio zaprojektowane, zdyscyplinowane i czujne. NAT odpowiada: to prawda tylko częściowo. W systemach interakcyjnie złożonych i ściśle sprzężonych pewnych wypadków nie da się wyeliminować, ponieważ wynikają one z samej architektury systemu. To spór między optymizmem organizacyjnym a sceptycyzmem strukturalnym; między wiarą w kulturę bezpieczeństwa a podejrzeniem, że może ona stać się eleganckim opakowaniem dla systemu, którego nie powinno się eksploatować w obecnej postaci.

Teoria wysokiej niezawodności wyrosła z obserwacji organizacji, które mimo ogromnego ryzyka funkcjonują z zaskakująco małą liczbą katastrof – mowa tu o lotniskowcach, kontroli ruchu lotniczego, elektrowniach czy systemach ratowniczych operujących pod presją czasu. HRT zakłada, że można budować organizacje szczególnie czujne, które nie popadają w samozadowolenie i nie traktują drobnych odchyleń jako „normalnych", lecz jako sygnały ostrzegawcze. Organizacje wysokiej niezawodności mają stale monitorować własne błędy, doskonalić procedury i utrzymywać bezpieczeństwo jako realny priorytet, a nie jako hasła z plakatu przy windzie. W tej perspektywie katastrofa nie jest nieuchronną konsekwencją technologii, lecz skutkiem niedostatecznej organizacji. Jeśli ludzie są dobrze wyszkoleni, komunikacja jasna, a hierarchia elastyczna, można osiągać niezwykle wysoką niezawodność. HRT jest zatem teorią nadziei organizacyjnej: ryzyko jest wielkie, ale organizacja może do niego dorosnąć.

Perrow nie odrzuca tej nadziei w całości, lecz pyta, w jakich systemach jest ona uzasadniona, a w jakich staje się ideologią samozadowolenia. Najgłębsza różnica między HRT a NAT dotyczy pojęcia kontroli. HRT zakłada, że dzięki dyscyplinie i odpowiedniemu projektowi można kontrolować nawet bardzo ryzykowne środowiska poprzez trening, standardy i kulturę niekarania za zgłaszanie błędów. NAT ripostuje: to może działać tam, gdzie system daje się obserwować i zatrzymywać. Jednak tam, gdzie występuje jednocześnie złożoność interakcyjna i ścisłe sprzężenie, kontrola jest ograniczona przez strukturę, a nie brak dobrej woli. System może wytwarzać konfiguracje awarii, których nikt nie przewidział, a które rozwijają się zbyt szybko, by organizacja zdążyła je zrozumieć. To różnica między błędem jako niedoskonałością zarządzania a błędem jako produktem architektury.

HRT mówi: zbudujmy lepszą organizację. NAT odpowiada: najpierw sprawdźmy, czy ten typ systemu w ogóle daje się uczynić bezpiecznym, bo jeśli nie, to doskonalenie organizacji może być tylko polerowaniem granatu. Perrow nie jest dogmatycznym przeciwnikiem wysokiej niezawodności; uznaje, że solidne szkolenia i uczenie się na błędach są skuteczne – ale przede wszystkim w systemach bardziej liniowych i luźniej sprzężonych.

To kluczowe rozróżnienie. Jeśli system ma widoczne sekwencje przyczynowe, awarie są lokalne, a proces można zatrzymać bez katastrofalnych skutków, wtedy HRT ma wielką wartość. Lotnictwo jest tu dobrym przykładem: mimo ryzyka wypracowało silne mechanizmy uczenia się, raportowania i redundancji. Nie oznacza to, że lotnictwo jest wolne od wypadków systemowych, lecz pokazuje, że w określonych warunkach organizacje mogą znacząco zmniejszać ryzyko.

Paradoks złożoności bezpieczeństwa w systemach wysokiego ryzyka

Perrow nie twierdzi zatem, że HRT jest fałszywa. Sugeruje raczej, iż nie stanowi ona uniwersalnego lekarstwa i nie można stosować jej jak zaklęcia nad każdym systemem wysokiego ryzyka. Jego najostrzejsza krytyka dotyczy sytuacji, w której zwolennicy wysokiej niezawodności przenoszą swoje założenia na systemy charakteryzujące się jednocześnie złożonością interakcyjną i ścisłym sprzężeniem. W takich warunkach „większe starania" mogą okazać się niewystarczające, a wręcz pogorszyć sytuację.

Dlaczego tak się dzieje? Ponieważ mnożenie procedur, kontroli, czujników i warstw organizacyjnych nieuchronnie zwiększa złożoność. Tworzy to nowe zależności, dodatkowe punkty awarii oraz pole do błędnych interpretacji. Organizacja dąży do opanowania systemu poprzez dodawanie mechanizmów kontroli, lecz każdy z nich staje się nowym elementem układu, który sam wymaga nadzoru. W efekcie powstaje paradoks: system jest coraz lepiej zabezpieczony przed awariami znanymi, ale staje się coraz trudniejszy do zrozumienia w obliczu zdarzeń nieprzewidzianych. HRT zakłada bowiem, że wzrost czujności, raportowania i liczby procedur automatycznie przekłada się na bezpieczeństwo.

NAT odpowiada: tak, lecz tylko do pewnej granicy. Po jej przekroczeniu organizacja zaczyna produkować złożoność bezpieczeństwa - labirynt procedur i zabezpieczeń, który sam staje się źródłem ryzyka. Przypomina to medycynę: lek może ratować życie, ale polipragmazja, czyli nadmiar leków, może wywołać interakcje groźniejsze niż pierwotna choroba.

HRT jako teoria eksploatacji a NAT jako teoria granic

Systemy wysokiego ryzyka mogą zostać również „przeleczone" kontrolą. Perrow krytykuje HRT przede wszystkim za zbyt optymistyczne założenie dotyczące racjonalności organizacji. Teoria wysokiej niezawodności zakłada, że organizacje potrafią konsekwentnie stawiać bezpieczeństwo na pierwszym miejscu, podczas gdy w rzeczywistości są one areną ścierania się interesów, nacisków, hierarchii, budżetów i polityki wewnętrznej.

W realnym świecie bezpieczeństwo często przegrywa nie w deklaracjach, lecz w codziennych decyzjach. Nikt nie mówi wprost: „lekceważymy bezpieczeństwo". Słyszy się raczej: „musimy utrzymać harmonogram", „budżet jest napięty", „ryzyko jest akceptowalne" czy „to tylko tymczasowe obejście". Organizacja może więc oficjalnie czcić bezpieczeństwo, a operacyjnie

nagradzać ryzyko. Menedżerowie bywają rozliczani z wyników finansowych i wydajności szybciej i surowiej niż z marginalnego zwiększania poziomu ryzyka. Gdy katastrofa jest rzadka, a presja wyniku codzienna, system bodźców staje się asymetryczny: bezpieczeństwo pozostaje odległą możliwością, podczas gdy produkcja jest dzisiejszym obowiązkiem.

Nie jest to kwestia złej woli ludzi, lecz ograniczonej racjonalności i struktury motywacyjnej. Organizacje robią to, za co są nagradzane. Jeśli przestój jest karany surowiej niż ciche usuwanie buforów bezpieczeństwa, system będzie te bufory eliminował, nazywając to później optymalizacją.

Kolejnym filarem HRT jest organizacyjne uczenie się poprzez analizę incydentów i błędów. Perrow nie neguje wartości tego procesu, lecz kwestionuje łatwość, z jaką HRT zakłada realną zdolność organizacji do nauki. Po pierwsze, wypadki systemowe często wynikają z unikatowych konfiguracji zdarzeń. Organizacja może wyciągnąć wnioski z konkretnego incydentu, ale niekoniecznie przewidzi kolejny. Naprawia drzwi, przez które weszła poprzednia awaria, a kolejna wchodzi oknem, kominem albo przez system wentylacji.

Po drugie, uczenie się jest selektywne. Analizuje się katastrofy, pomijając sytuacje, które nie doprowadziły do wypadku, choć były niemal identyczne. Bez porównania „katastrof" z „prawie katastrofami" łatwo pomylić przyczynę z przypadkowym elementem zdarzenia. Po trzecie, proces ten jest polityczny. Przyznanie, że system jest strukturalnie niebezpieczny, wiązałoby się z ogromnymi kosztami, odpowiedzialnością zarządu lub koniecznością zmiany technologii. Organizacja ma więc motywację, by uczyć się w sposób wygodny: poprawić procedurę czy przeszkolić personel, zamiast pytać o dopuszczalność całego modelu działania.

Po czwarte, katastrofy o najwyższych konsekwencjach są zbyt kosztowne, by służyć jako materiał edukacyjny. Nie można uznać, że po kilku stopieniach rdzenia nauczymy się lepiej; istnieją błędy, na których społeczeństwo nie powinno być zmuszane do nauki. Perrow zarzuca HRT, że wykonuje tylko „połowę pracy". Doskonali zarządzanie i kulturę bezpieczeństwa, ale nie pyta, czy dany system powinien w ogóle istnieć w obecnej formie i kto ma władzę narzucać to ryzyko innym.

HRT skupia się na tym, jak bezpieczniej zarządzać systemem. NAT pyta, czy powinniśmy zarządzać właśnie takim systemem. HRT poprawia pilotaż; NAT pyta, czy konstrukcja samolotu nie sprawia, że przy pewnych awariach zawsze wpada on w niekontrolowany lot. HRT doskonali kulturę operacyjną elektrowni; NAT pyta, czy elektrownia jądrowa jest społecznie tolerowalnym systemem przy potencjale ofiar trzeciej i czwartej kategorii.

HRT jest teorią lepszej eksploatacji, natomiast NAT jest teorią granic eksploatacji. To rozróżnienie ma kluczowe znaczenie polityczne. Organizacje chętnie przyjmują HRT, gdyż pozwala ona działać dalej, tyle że „lepiej". NAT jest mniej wygodna, bo sugeruje konieczność ograniczenia lub

porzucenia pewnych sposobów działania. Dlatego HRT jest atrakcyjna dla zarządów i elit technologicznych, podczas gdy NAT psuje przyjęcie.

HRT jako narzędzie i NAT jako granica pychy

Pojawia się paradoks: systemy interakcyjnie złożone wymagają decentralizacji, gdyż niezbędna jest w nich lokalna wiedza, elastyczność i interpretacja. Z kolei systemy ściśle sprzężone wymuszają centralizację – tutaj decyzje muszą być szybkie, skoordynowane i zgodne z procedurą. Perrow dostrzega w tym jedną z kluczowych sprzeczności organizacji wysokiego ryzyka. HRT próbuje rozwiązać ten problem poprzez tworzenie struktur łączących hierarchię z elastycznością. W normalnych warunkach to hierarchia utrzymuje standardy, jednak w sytuacji kryzysowej głos ekspertów znajdujących się najbliżej problemu powinien zyskać na znaczeniu. To cenna intuicja: organizacja wysokoniezawodna ma potrafić chwilowo przesunąć autorytet tam, gdzie aktualnie znajduje się wiedza. Perrow byłby jednak sceptyczny co do stabilności takiego rozwiązania w systemach skrajnie złożonych i ciasno sprzężonych, gdyż w prawdziwym kryzysie nie zawsze wiadomo, kto dysponuje właściwą wiedzą.

Lokalny operator widzi jedynie fragment. Centrum dostrzega szerszy obraz, lecz z opóźnieniem i przez pryzmat reprezentacji. Eksperci operują modelami, które mogą nie obejmować nietypowej konfiguracji zdarzeń. Automatyka działa szybko, ale może podążać błędnym scenariuszem. Organizacja mierzy się więc nie tylko z problemem władzy, lecz przede wszystkim z problemem epistemologicznym: gdzie w danej chwili znajduje się prawda o systemie? HRT zakłada, że dobrze zaprojektowana organizacja potrafi przekierować uwagę we właściwe miejsce. NAT pyta natomiast, czy w trakcie wypadku istnieje jeszcze jakiekolwiek „właściwe miejsce”, skoro problem rodzi się pomiędzy nimi.

Współczesne organizacje często odwołują się do kultury bezpieczeństwa. To słuszny kierunek. Oznacza ona, że ludzie mogą zgłaszać problemy bez strachu, incydenty są rzetelnie analizowane, kierownictwo słucha pierwszej linii, procedury są traktowane poważnie, a odchylenia nie są normalizowane i nie karze się za ostrożność. Perrow nie miałby powodu odrzucać tych postulatów – są one rozsądne. Problem zaczyna się jednak wtedy, gdy kultura bezpieczeństwa zostaje przedstawiona jako wystarczająca odpowiedź na ryzyko strukturalne. Może ona zmniejszyć liczbę błędów, poprawić komunikację, ujawnić słabe sygnały czy zwiększyć szansę na zatrzymanie procesu.

Nie zmieni jednak faktu, że pewne systemy pozostają nieprzejrzyste, ściśle sprzężone, zależne od procesów transformacyjnych i potencjalnie katastrofalne dla osób postronnych. Kultura

bezpieczeństwa w złej architekturze jest jak znakomity kierowca w samochodzie bez hamulców. Lepiej, że jest znakomity, ale nadal trzeba zapytać, dlaczego jedziemy.

Najciekawsze jest to, że NAT i HRT nie muszą się całkowicie wykluczać. Możliwy jest kompromis w postaci warunkowej teorii wypadków, która uwzględnia konkretne cechy systemu. To płodne podejście: zamiast pytać abstrakcyjnie o możliwość bycia organizacją wysokoniezawodną, pytamy: w jakim typie systemu, przy jakim poziomie złożoności i sprzężenia, jakiej zdolności uczenia się, jakie są konsekwencje awarii, jaka panuje kultura i jaki jest rozkład ryzyka?

W systemach liniowych i luźno sprzężonych HRT może być bardzo skuteczna. W systemach złożonych, lecz posiadających bufory, może zmniejszać częstotliwość incydentów i poprawiać odporność. W systemach złożonych i ściśle sprzężonych może ograniczać pewne błędy, ale nie powinna być traktowana jako obietnica eliminacji katastrof. W przypadku systemów o potencjale ofiar trzeciej i czwartej kategorii należy dodatkowo pytać o dopuszczalność samego ryzyka. To najbardziej rozsądny wniosek: HRT jako narzędzie, NAT jako granica pychy.

Spór NAT-HRT jest niezwykle użyteczny w analizie państwa. Współczesne państwo aspiruje do bycia organizacją wysokiej niezawodności – chce zarządzać kryzysami, dostarczać usługi, chronić infrastrukturę i granice, finansować zdrowie publiczne, regulować gospodarkę i obsługiwać miliony obywateli bez popełniania błędów. HRT sugerowałaby budowę profesjonalnej administracji, uczenie się na incydentach, wzmacnianie procedur, raportowania, szkoleń, komunikacji międzyinstytucjonalnej oraz kultury zgłaszania problemów.

To wszystko jest słuszne, lecz NAT dodałaby: sprawdźmy, gdzie państwo samo tworzy systemy interakcyjnie złożone i ściśle sprzężone. Czy centralne systemy informatyczne nie stały się wspólnym trybem awarii? Czy legislacja nie produkuje ukrytych sprzężeń między resortami? Czy procedury kryzysowe dają realny luz, czy jedynie mnożą podpisy? Czy administracja dysponuje rezerwami kadrowymi i czy samorządy mają autonomię działania? Czy jedno opóźnienie budżetowe nie paraliżuje kilku usług jednocześnie? Czy presja medialna nie skraca czasu decyzji do poziomu niebezpiecznego automatyzmu? Państwo potrzebuje więc obu teorii: HRT wskazuje, jak wzmacniać niezawodność organizacyjną, a NAT mówi, gdzie sama architektura instytucji produkuje ryzyko, którego nie da się przykryć szkoleniem.

W przedsiębiorstwach spór ten ujawnia się szczególnie wyraźnie. Zarządy po incydentach często reagują zwiększeniem kontroli: więcej raportów, akceptacji, dashboardów, compliance i audytów. Część z tych działań jest potrzebna, ale z perspektywy Perrowa należy zapytać, czy organizacja nie dodaje złożoności zamiast odporności. Jeśli nowy raport nie dostarcza lepszej wiedzy operacyjnej, a jedynie zwiększa obciążenie pierwszej linii, może pogorszyć bezpieczeństwo. Jeśli dodatkowa

akceptacja wydłuża reakcję w systemie ściśle sprzężonym, zwiększa ryzyko. Jeśli compliance staje się rytuałem dokumentowania zgodności zamiast rozumienia realnych sprzężeń, tworzy złudzenie kontroli. Jeśli każdy dział operuje na własnych wskaźnikach, nie widząc relacji między nimi, firma posiada wiele lusterek, ale nie ma szyby przedniej.

Wysoka niezawodność nie rozgrzesza wadliwej architektury

HRT bez NAT łatwo przeobraża się w "menedżerską pobożność": więcej kultury, procedur i komunikacji. NAT przypomina jednak: najpierw sprawdź, czy system nie jest zaprojektowany tak, że każde kolejne „więcej" otwiera nowe ścieżki awarii. Spór między tymi teoriami staje się szczególnie aktualny w świecie technologii cyfrowych i sztucznej inteligencji. Systemy algorytmiczne cechują się interakcyjną złożonością – zależą od danych, modeli, infrastruktury, użytkowników, sprzężeń zwrotnych oraz nieprzewidzianych korelacji. Są one coraz ściślej sprzężone z decyzjami w realnym świecie: kredytami, ubezpieczeniami, rekrutacją, opieką zdrowotną czy administracją.

Podejście HRT sugerowałoby: testujmy, audytujmy, monitorujmy i twórzmy procedury odpowiedzialnego wdrażania. To wszystko jest konieczne, lecz NAT zadałaby kluczowe pytania: Czy system jest zrozumiały? Czy decyzje można zatrzymać? Czy istnieje człowiek z realną możliwością interwencji? Czy dane wejściowe nie stanowią wspólnego trybu awarii? Czy błędny model nie wpłynie jednocześnie na tysiące decyzji, a automatyzacja nie skróciła czasu reakcji poniżej zdolności nadzoru? I wreszcie: czy organizacja nie myli audytu formalnego z rzeczywistym rozumieniem zachowania systemu?

W cyfrowym świecie normalny wypadek nie musi przypominać eksplozji. Może objawiać się jako masowe błędne decyzje, zablokowane konta, kaskady dezinformacji czy synchronizacja zachowań rynkowych. Brak dymu nie znaczy brak katastrofy.

Najostrzejsza lekcja sporu NAT-HRT brzmi: nie wolno mylić zdolności organizacyjnej z panowaniem nad strukturą ryzyka. Można dysponować świetnymi ludźmi, znakomitymi szkoleniami i nowoczesną kontrolą, a wciąż eksploatować technologię, która przy pewnej konfiguracji stanie się nieprzejrzysta i nieopanowalna. Z drugiej strony, system groźny można okiełznać dzięki dobrej organizacji, znacząco zmniejszając częstość błędów. Dlatego pytanie nie brzmi: NAT czy HRT? Pytanie brzmi: gdzie kończy się skuteczność HRT, a zaczyna ostrzeżenie NAT?

To rozróżnienie powinno stać się standardem odpowiedzialnego zarządzania. Każdy system wysokiego ryzyka wymaga podwójnej analizy. Najpierw HRT: jak poprawić organizację, szkolenia i kulturę bezpieczeństwa? Potem NAT: czy mimo tych poprawek system pozostaje interakcyjnie złożony, ściśle sprzężony i pozbawiony buforów? Jeśli odpowiedź na drugie pytanie brzmi „tak", to pierwsze nie wystarcza.

Teoria wysokiej niezawodności chroni nas przed fatalizmem, natomiast teoria normalnych wypadków przed pychą. HRT mówi: organizacje mogą być lepsze. NAT odpowiada: niektóre systemy pozostaną niebezpieczne mimo tych ulepszeń. Najrozsądniejsza postawa łączy obie intuicje. Należy budować wysoką niezawodność tam, gdzie jest to możliwe, ale nie wolno traktować jej jako alibi dla utrzymywania struktur produkujących katastrofalne ryzyko. Można szkolić ludzi i poprawiać procedury, lecz nie wolno udawać, że rozwiązuje to problem fałszywych wskaźników czy mylić procedury z mądrością systemu. Najkrócej: wysoka niezawodność jest cnotą organizacji, ale nie jest rozgrzeszeniem złej architektury ryzyka.

> Czy w świecie zdominowanym przez cyfrowe dashboardy i algorytmiczne modele predykcyjne nie staliśmy się zakładnikami nowej formy systemowej ślepoty? Możemy mnożyć certyfikaty, audyty i szkolenia, lecz dopóki będziemy mylić liczbę zabezpieczeń z realnym poziomem bezpieczeństwa, pozostaniemy jedynie sprawnymi operatorami maszyn, które w krytycznym momencie potrafią kłamać. Ostatecznie najwyższą formą odpowiedzialności nie jest pytanie o to, jak naprawić błąd człowieka, lecz odwaga, by zapytać: czy system, który projektujemy, w ogóle powinien istnieć?

Inspiracje

[1] 

"Normal Accidents" Charles Perrow

Princeton University Press | ISBN: 9781400828494

Charles Perrow (1925–2019) był wybitnym amerykańskim socjologiem i teoretykiem organizacji. Przez wiele lat był profesorem socjologii na Uniwersytecie Yale'a, wcześniej piastując stanowiska w takich instytucjach jak Uniwersytet Michigan, Uniwersytet Wisconsin–Madison i Uniwersytet Stanowy Nowego Jorku w Stony Brook. Perrow jest najbardziej znany ze swojej pionierskiej pracy w dziedzinie teorii organizacji, a w szczególności z opracowania teorii wypadków normalnych, która bada, jak złożone, ściśle powiązane systemy są z natury podatne na katastrofalne awarie. Jego badania podważały tradycyjne poglądy na temat bezpieczeństwa i zarządzania, podkreślając, że wypadki w technologiach wysokiego ryzyka często mają charakter systemowy, a nie są wynikiem błędu ludzkiego. Jego wkład naukowy znacząco wpłynął na socjologię, politykę publiczną i zarządzanie ryzykiem, czyniąc go jedną z najważniejszych postaci w badaniach nad złożonymi organizacjami i bezpieczeństwem przemysłowym.

Charles Perrow *(1925–2019) was a prominent American sociologist and organizational theorist. He served as a professor of sociology at Yale University for many years, having previously held positions at institutions such as the University of Michigan, the University of Wisconsin–Madison, and the State University of New York at Stony Brook. Perrow is best known for his pioneering work in organizational theory, specifically his development of normal accident theory, which examines how complex, tightly coupled systems are inherently prone to catastrophic failures. His research challenged traditional views on safety and management, emphasizing that accidents in high-risk technologies are often systemic rather than the result of human error. His scholarly contributions significantly influenced the fields of sociology, public policy, and risk management, establishing him as a foundational figure in the study of complex organizations and industrial safety.*

Yale University

Literatura uzupełniająca

Książki

Książki autora i dzieła przywołane w tekście:



[1] "Complex Organizations"

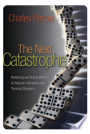
Charles Perrow

1979 | Pearson Scott Foresman

[2] "A Society of Organizations"

Charles Perrow

1990 | ISBN: 9788479190170



[3] "The Next Catastrophe"

Charles Perrow

2011 | Princeton University Press | ISBN: 9780691150161



[4] "Organizing America"

Charles Perrow

2009 | Princeton University Press | ISBN: 9781400825080



[5] "Authority, Goals and Prestige in a General Hospital"

Charles Perrow

1960



[6] "Organizational Analysis"

Charles Perrow

1974

Książki autorów przywoływanych i literatura pokrewna:

[7] "Reimagining Capitalism in a World on Fire"

Rebecca Henderson

Artykuły naukowe

Artykuły naukowe autora:

[1] "Normal Accidents: Living with High Risk Technologies"

A. J. Grimes, Charles Perrow

1985 | Academy of Management Review | DOI: 10.2307/257982

Źródło

[2] **"Ambiguity and Choice in Organizations."**
Charles Perrow, James G. March, Johan P. Olsen
1977 | Contemporary Sociology A Journal of Reviews | DOI: 10.2307/2064777
Źródło

[3] **"A Framework for the Comparative Analysis of Organizations"**
Charles Perrow
1967 | American Sociological Review | DOI: 10.2307/2091811
Źródło

[4] **"Complex Organizations: A Critical Essay"**
Neil Fligstein, Charles Perrow
1990 | Teaching Sociology | DOI: 10.2307/1318250
Źródło

[5] **"The Logic of Collective Action: Public Goods and the Theory of Groups."**
Charles Perrow, Mancur Olson
1973 | Social Forces | DOI: 10.2307/2576430
Źródło

[6] **"Insurgency of the Powerless: Farm Worker Movements (1946-1972)"**
J. Craig Jenkins, Charles Perrow
1977 | American Sociological Review | DOI: 10.2307/2094604
Źródło

[7] **"Organizational Analysis: A Sociological View"**
Charles Perrow
1970 | Medical Entomology and Zoology
Źródło

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System
Fundacja Dobre Państwo © 2026
Article ID: d00a53ce-b6b1-401c-985e-8642d9df20f3