Zarządzanie Publiczne
Nr 3(13)/2010
ISSN 1898-3529

Robert Delorme

# Zarządzanie bezpieczeństwem

Autor niniejszej pracy, stanowiącej fragment książki pt. *Deep Complexity and the Social Sciences. Experience, Modelling and Operationality*, poddaje szczegółowej analizie kwestię niemożności zredukowania do zera ryzyka występowania wypadków w systemach złożonych. Odwołując się do prac autorów takich jak Charles Perrow, stawia tezę, że zasadniczą przyczynę tego rodzaju wypadków stanowi nieprzewidywalność interakcji między poszczególnymi częściami składowymi tych systemów. Następnie prezentuje koncepcję zabezpieczeń wielowarstwowych i poddaje ją krytyce ze względu na coraz większy dystans dzielący operatorów od systemów, które mają oni nadzorować, oraz nawarstwianie się tzw. problemów utajonych. Wybrany fragment pracy kończy się prezentacją różnych punktów widzenia na temat sposobów określania społecznie akceptowalnego poziomu ryzyka i jego optymalizacji w odniesieniu do zaproponowanego przez Jamesa Reasona teoretycznego modelu kompromisu między ryzykiem a wydajnością oraz omawia zastosowanie zasady ostrożności w praktyce.

Słowa kluczowe: systemy złożone, problemy utajone, akceptowalny poziom ryzyka, optymalizacja ryzyka, zasada ostrożności

## 1. Endogenizacja nieredukowalności

Jeżeli operator o pewnym poziomie aspiracji zajmuje się w sposób celowy jakimś przedmiotem zainteresowania w danej dziedzinie, wynik jego działań można uznać za zadowalający (*satisfying*) lub wystarczająco dobry (*satisficing*[1]) wtedy, gdy faktycznie osiągnie on pożądany poziom aspiracji. Oznacza to, że w tym wypadku można zmniejszyć trudności związane z osiągnięciem danego poziomu aspiracji do poziomu wystarczająco dobrego. W ten sposób można zdefiniować redukowalność i nieredukowalność *a contrario*.

Endogenizacja złożoności wymaga dobudowania kontekstu behawioralnego na podstawie najciekawszych spostrzeżeń Ashby'ego i innych autorów, którzy – ogólnie rzecz biorąc – wskazują na konieczność jasnego sprecyzowania roli operatora, której jednocześnie nie można jednak zredukować wyłącznie do subiektywności.

W kontekście bezpieczeństwa dadzą się wyróżnić dwa obszary: technologie przemysłowe wysokiego ryzyka i transport. Jedna z poddziedzin dotyczy zasady ostrożności (*precautionary principle*).

Zarządzanie bezpieczeństwem i nauka o bezpieczeństwie stanowią najprawdopodobniej najlepsze przykłady dziedzin, w których nieredukowalność – rozumiana jako niemożność całkowitego wyeliminowania poważniejszych wypadków – zawsze pozostaje kwestią kluczową. Publikacje z tej dziedziny pojawiają się od niedawna, a ich liczba stale rośnie. Wśród nich można wskazać następujące pozycje: Perrow (1984 [1999a]), Reason (1993, 1998), Rasmussen (1997), Rasmussen i Svedung (2000), Paté-Cornell (1993), Amalberti (1996,

Robert Delorme – Université de Versailles, Francja.

Przełożył Rafał Śmietana. Tekst oryginalny pt. „Irreducibility Endogenised" stanowi rozdział z książki Roberta Delorme'a *Deep Complexity and the Social Sciences: Experience, Modelling and Operationality*, New Horizons in Institutional and Evolutionary Economics, Edward Elgar, Cheltenham, UK – Northampton, MA 2010.

[1] *Satisficing* – termin powstały z połączenia dwóch słów angielskich *satisfying* (zadowalający) i *sufficing* (wystarczający), oznaczający cechę rozwiązania problemu lub strategii działania, które wystarczająco dobrze sprawdzają się w danym kontekście przy uwzględnieniu kosztów procesu decyzyjnego, nie będąc jednocześnie rozwiązaniami ani strategiami optymalnymi. W tekście będzie stosowane określenie „wystarczająco dobry" (przyp. tłum.).

1997, 1999, 2001), Vaughan (1996) i Hollnagel (2004). W piśmiennictwie wyróżniono kilka poziomów i odpowiadających im modeli, które opisują omawiane zagadnienie, począwszy od poziomu operatorów pierwszej linii i interakcji człowiek–maszyna, przez poziomy miejsca pracy, organizacji, systemu socjotechnicznego, a na poziomach regulacji i poziomie społecznym skończywszy. Na potrzeby niniejszej pracy wybrałem trzy reprezentatywne opisy. Ich autorami są Charles Perrow (poziom systemowy), James Reason (wypadki na poziomie organizacji) oraz René Amalberti (interakcje człowiek–maszyna o charakterze ergonomicznym).

## 2. Zwyczajne wypadki

W książce *Normal Accidents: Living with High-Risk Technologies*, opublikowanej w roku 1984 (w 1999 r. ukazało się drugie wydanie), Charles Perrow, zajmujący się teorią organizacji, formułuje tezę, że w bardzo złożonych systemach, których elementy wchodzą ze sobą w skomplikowane interakcje – takich jak elektrownie jądrowe, zakłady chemiczne, samoloty itp. – nie da się uniknąć wypadków bez względu na poziom umiejętności operatorów, zarządzających i projektantów tych systemów. Termin „zwyczajny wypadek" i jego odpowiednik „wypadek systemowy" mają wskazywać na fakt, że są one nieodłącznymi elementami funkcjonowania systemów, które wykazują pewne cechy wynikające z kombinacji interakcji i powiązań technicznych między ich częściami składowymi. Innymi słowy, większość systemów wysokiego ryzyka wykazuje pewne cechy, które sprawiają, że wypadki są nieuniknione, a nawet są czymś „zwyczajnym". Nie da się ich zatem całkowicie wyeliminować, mimo podejmowanych w tym celu wysiłków. Nieredukowalność jest tu czymś oczywistym. Aby jednak uniknąć potencjalnych nieporozumień, musimy przyjrzeć się uważniej argumentacji Perrowa. Najpierw przedstawimy więc podstawowe definicje, następnie omówimy interakcje i zależności, a na koniec odniesiemy je do ryzyka wystąpienia zwyczajnego wypadku wynikającego ze złożoności tych interakcji i zależności.

### 2.1. Definicje

Wypadki (*accidents*) różnią się od incydentów (*incidents*) ze względu na poziom ich występowania w systemie. Systemy dzielą się na cztery poziomy o stopniowo wzrastającej złożoności: jednostki, części, podsystemy oraz systemy. Incydenty dotyczą problemów na poziomie jednostek lub części. Z kolei o wypadkach mówi się na poziomie podsystemów lub systemów jako całości. Zarówno incydenty, jak i wypadki mogą wpływać na tok produkcji, a nawet ją zatrzymywać. Rozróżniamy dwa rodzaje wypadków: „zwyczajne" i inne, które można nazwać „niezwyczajnymi". Pierwszy rodzaj obejmuje nieprzewidziane interakcje wielu awarii, podczas gdy do drugiego zalicza się jedną lub więcej awarii elementów składowych (jednostek, części lub podsystemów), które następują w przewidywalnej kolejności. Perrow nazywa je wypadkami z powodu awarii części składowych (*component failure accidents*). W praktyce przyczyną obu rodzajów wypadków są awarie elementów składowych. Jednak wypadki systemowe różnią się od innych, gdyż interakcje między kilkoma awariami są nieprzewidywalne, a nawet niezrozumiałe dla operatorów, zarządzających i projektantów systemu.

### 2.2. Interakcje i złożoność

W modelu zwyczajnych wypadków źródło złożoności tkwi w charakterze interakcji między elementami składowymi systemu (operatorami na wszystkich poziomach, częściami i procedurami). Strukturę systemu dość szczegółowo wyraża koncepcja DEPOSE (*design, equipment, procedures, operators, supplies and materials, environment* – planowanie, wyposażenie, procedury, operatorzy, zasoby i materiały, środowisko). Interakcje te mają charakter liniowy lub „złożony" zależnie od etapu, na którym pojawiają się w toku produkcji i utrzymania ciągłości działania, a także od wpływu na operatorów. Interakcje liniowe „zachodzą między elementami systemu DEPOSE, które występują bezpośrednio przed sobą lub po sobie w toku produkcji" bądź utrzymania ciągłości działania. Pojawiają się one w przewidywalnej i znanej kolejności, dlatego łatwo je dostrzec, nawet jeżeli nie zostały zapla-

Tab. 1. Porównanie interakcji złożonych i niezłożonych

| Interakcje złożone | Interakcje niezłożone |
|---|---|
| Bliskość (elementy wyposażenia znajdują się blisko siebie, poszczególne etapy produkcji następują w niewielkich odstępach czasowych) | Rozdział (elementy wyposażenia i etapy produkcji są oddalone od siebie) |
| Istnieje wiele wspólnych połączeń między elementami nieznajdującymi się w ciągu produkcyjnym | Wspólne połączenia ograniczone do zasilania i środowiska; większy udział połączeń dedykowanych (indywidualnych) |
| Utrudniony rozdział wadliwych elementów (podsystemy połączone ze sobą) | Łatwy rozdział wadliwych elementów (podsystemy oddzielone od siebie) |
| Specjalizacja personelu ogranicza zrozumienie systemu jako całości | Niewielki stopień specjalizacji personelu |
| Ograniczone możliwości zastępowania zasobów i materiałów | Szerokie możliwości zastępowania zasobów i materiałów |
| Nieznane lub nieplanowane pętle sprzężeń zwrotnych | Nieliczne nieznane lub nieplanowane pętle sprzężeń zwrotnych |
| Liczne parametry kontrolne, które mogą wchodzić we wzajemne interakcje | Nieliczne, wyspecjalizowane i oddzielone od siebie parametry kontrolne |
| Pośrednie źródła informacji; informacje uzyskiwane na podstawie wnioskowania | Bezpośrednie, bliskie źródła informacji |
| Ograniczone zrozumienie pojedynczego procesu | Szczegółowe zrozumienie wszystkich procesów |

Źródło: Perrow 1999a, s. 88.

nowane. Interakcje złożone mają miejsce wtedy, gdy poszczególne elementy mogą oddziaływać na siebie poza znanymi ciągami produkcji i utrzymania ciągłości działania w sposób nieplanowany i nieprzewidywalny, co sprawia, że „albo nie są widoczne, albo nie da się ich bezpośrednio zrozumieć" (Perrow 1999a, s. 77–78). Szczegółowe porównanie tych dwóch rodzajów interakcji przedstawiono w tabeli 1.

Tabela 1 wymaga kilku słów komentarza. Porównanie między interakcjami zapożyczyłem od Perrowa z niewielkimi zmianami zainspirowanymi potrzebą wyeksponowania niektórych różnic. Przede wszystkim zmianie uległy nagłówki kolumn. Zastosowane przez Perrowa terminy „systemy złożone" i „systemy liniowe" zostały zastąpione odpowiednio terminami „interakcje złożone" i „interakcje niezłożone". Większy problem stanowią tu przymiotniki, a nie użycie samego terminu „system". Można uznać, że połączenie kilku lub wszystkich interakcji w poszczególnych kolumnach daje w wyniku ogólną charakterystykę systemu. Na tym etapie wydaje się zasadne stosowanie terminów zgodnie z wyżej podanymi definicjami interakcji. Dlaczego mielibyśmy przeciwstawiać sobie terminy „złożone" i „liniowe", zamiast po prostu używać pary terminów „złożone" i „niezłożone" lub „liniowe" i „nieliniowe"? Perrow wyjaśnia, że „liniowe" oznacza zarówno „proste" (czyli „łatwo zrozumiałe"), jak i „nieproste" w kontekście zaawansowanych procesów i technologii obejmujących interakcje w przewidywalnej kolejności. Zarazem zauważa on, że termin „nieliniowy" jest w miarę jednoznaczny w przeciwieństwie do terminu „złożony" (ibidem, s. 78). Należy nadmienić, że Perrow uznaje przymiotnik „prosty" za przeciwieństwo „złożonego", podczas gdy w rzeczywistości to, co nie jest złożone, może być proste lub skomplikowane. Tutaj przyjmujemy, że obie własności wyraża przymiotnik „niezłożone". Różnica ta nie wpływa jednak na ogólną charakterystykę interakcji.

## 2.3. Sprzężenie

Sprzężenie to termin zapożyczony z mechaniki. Może mieć charakter ścisły (synchroniczny) lub luźny (asynchroniczny). W wypadku pierwszego rodzaju sprzężenia można mówić o braku pewnego luzu lub bufora między dwoma elementami. Wszystko to, co dzieje się w jednym z nich, wpływa na sytuację w drugim. W systemach o ścisłym sprzężeniu elementów proce-

Tab. 2. Porównanie tendencji w systemach o różnych rodzajach sprzężeń

| Kryterium | Sprzężenie ścisłe | Sprzężenie luźne |
|---|---|---|
| Możliwość opóźnienia przetwarzania? | Nie | Tak |
| Kolejność działań | Niezmienna | Może ulec zmianie |
| Metody użyte do osiągnięcia celu | Tylko jedna metoda | Dostępne metody alternatywne |
| Dostępność buforów i redundancji (nadmiarowości) | Zintegrowana (wbudowana), celowa | Niewbudowane w system |
| Dostępność dodatkowych zasobów na wypadek deficytu (personel, surowce, wyposażenie) | Raczej niedostępne | Potencjalnie dostępne |
| Możliwość zastąpienia zasobów | Ograniczone i zintegrowane (wbudowane) | Niewbudowane w system |

Źródło: Perrow 1999a, s. 96.

sy mogą przebiegać bardzo szybko i nie da się ich zatrzymać. Elementów, które uległy awarii, nie sposób odizolować od innych, przynajmniej przez pewien czas. Nie istnieje żadna alternatywa, która pozwoliłaby zachować ciągłość produkcji. Nie da się szybko odwrócić efektów problemu wyjściowego, a jego skutki obejmują stopniowo coraz większą część systemu. Ścisłe sprzężenie zakłada pewne z góry określone sposoby postępowania ze strony operatora, a także stałość ciągów wydarzeń, których nie można szybko zmienić.

Tabela 2, zaadaptowana z pewnymi zmianami z pracy Perrowa, przedstawia szereg kryteriów służących do porównywania tendencji obserwowanych w systemach ściśle i luźno sprzężonych. Dla uproszczenia, tendencje te reprezentowane są przez przypadki skrajne. W systemach funkcjonujących w rzeczywistości pewne ich cechy będą występować w mniejszym lub większym nasileniu, a żaden z nich nie będzie wykazywał wszystkich cech wymienionych tylko w jednej lub tylko w drugiej kolumnie.

## 2.4. Interakcje i sprzężenie łącznie

Z połączenia interakcji i sprzężenia można otrzymać cztery różne systemy. Używając nazewnictwa Perrowa, można je sklasyfikować w następujący sposób: interakcje liniowe (niezłożone) ze sprzężeniem luźnym (np. agencje jednozadaniowe, większość produkcji przemysłowej), interakcje liniowe ze sprzężeniem ścisłym (np. transport kolejowy i morski, zapory wodne, sieci energetyczne); interakcje złożone ze sprzężeniem luźnym (np. uniwersytety, agencje wielozadaniowe) i na koniec interakcje złożone ze sprzężeniem ścisłym (np. elektrownie jądrowe, samoloty, zakłady chemiczne). Najbardziej istotny z naszego punktu widzenia jest ostatni rodzaj systemów, gdyż opisuje sytuację, w której istnieje największe ryzyko wystąpienia wypadków systemowych lub zwyczajnych. Złożoność interaktywna oznacza, że dowolna część systemu może wchodzić w takie interakcje z pozostałymi elementami, jakich nie przewidzieli jego twórcy/projektanci ani których nie jest także w stanie zrozumieć żaden operator. Gdy te nieprzewidziane interakcje względnie drobnych awarii łączą się ze ścisłym sprzężeniem, zaistniałe warunki mogą spowodować niesprawność systemu bezpieczeństwa, np. elektrowni, samolotu.

Zwyczajne wypadki należy odróżnić od katastrof. Chociaż w niektórych przypadkach rzeczywiście miewają one katastrofalne skutki, do prawdziwych katastrof dochodzi rzadko. Według szacunków zamieszczonych przez Perrowa w pierwszym wydaniu jego książki, spośród ok. 3 tys. zdarzeń zgłaszanych każdego roku przez ponad 70 elektrowni jądrowych, mniej więcej 300 można uznać za wypadki, z czego 15–30 przypuszczalnie było zwyczajnymi wypadkami (Perrow 1999a, s. 71).

Parafrazując Perrowa, zwyczajne wypadki mają swoje źródło w systemie, a nie w jego elementach składowych (ibidem, s. 351). Zwyczajnych

wypadków z definicji nie można wyeliminować mimo deklarowanego celu, jakim jest unikanie katastrof (Perrow 1999b, s. 70). Tym samym zwyczajnych wypadków nie da się zredukować do poziomu gwarantującego ograniczenie do zera liczby katastrof lub poważnych wypadków.

## 3. Wypadki na poziomie organizacji

W książce *Managing the Risks of Organizational Accidents* (1998) James Reason podkreśla udział czynnika organizacyjnego w genezie wypadków, obok czynników ludzkich i technicznych. Podobnie jak Perrow, uważa on, że konwencjonalne próby zapewniania bezpieczeństwa – czyli wbudowywanie dodatkowych ostrzeżeń i zabezpieczeń – nie są skuteczne. Perrow wykazał, że z powodu złożoności systemów awarie są nieuniknione, a typowe środki zapobiegawcze zwiększające tę złożoność mogą się nawet przyczynić do powstania nowych rodzajów wypadków. Dlatego też potrzebne są nowe ramy do oceny ryzyka. Reason analizuje kwestie związane z zarządzaniem bezpieczeństwem w kontekście cech organizacyjnych nowoczesnych technologii. W ten sposób kontynuuje pracę podjętą przez Perrowa, lecz kładzie szczególny nacisk na pojęcie nieprzejrzystości (*opacity*). Poniżej przedstawiam podsumowanie analizy Reasona w podziale na wypadki na poziomie organizacji, zabezpieczenia wielowarstwowe (*defences-in--depth*) oraz problemy utajone (*latent conditions*). Następnie omówię płynące z tych spostrzeżeń wnioski w kategoriach kompleksowości.

### 3.1. Definicja wypadku na poziomie organizacji

Reason rozróżnia dwa rodzaje wypadków: te, które przytrafiają się jednostkom, i te, które dotyczą organizacji. Niekiedy wytyczenie granicy między nimi może przysparzać pewnych trudności, jednak porównanie ich według kilku różnych kryteriów uzasadnia ich traktowanie jako dwóch odmiennych rodzajów zdarzeń. Różnią się przede wszystkim częstością i kontekstem występowania, przyczynami, rozmiarami i zakresem, a także zabezpieczeniami, które tworzy się, aby im zapobiegać.

Wypadki na poziomie organizacji występują rzadko. Częściej mamy do czynienia z wypadkami na poziomie jednostek, chociaż obecnie nie są one tak liczne, jak dawniej. Zdaniem Reasona, mimo że stosunkowo rzadkie, wypadki na poziomie organizacji występują zwłaszcza w dziedzinach, w których wykorzystywane są złożone nowoczesne technologie, takich jak elektrownie jądrowe, lotnictwo pasażerskie, przemysł petrochemiczny, zakłady chemiczne, transport kolejowy i morski, nie wspominając o bankach i stadionach sportowych. Niedawne wydarzenia związane z zakażeniami na skutek przetaczania krwi i skażeniem żywności mogą wskazywać na konieczność przedłużenia powyższej listy. Wypadki na poziomie organizacji są więc wytworem ostatnich czasów, a mówiąc dokładniej, produktem innowacji technologicznych, które zmieniły relacje między systemami i człowiekiem jako jednym z ich elementów, podczas gdy liczba wypadków na poziomie jednostek praktycznie pozostała bez zmian. Wypadki pierwszego rodzaju zwykle mają wiele przyczyn związanych z działaniem licznych osób na różnych poziomach i w różnym czasie, natomiast w wypadkach indywidualnych dana jednostka lub grupa osób często bywa jednocześnie sprawcą i ofiarą. Wypadki organizacyjne nierzadko prowadzą do katastrofalnych skutków i mogą wpływać na grupy ludzi, składniki majątku i środowisko nienależące do tych organizacji. Natomiast wypadki indywidualne zazwyczaj dotyczą osób bezpośrednio w nich uczestniczących i mają ograniczony zasięg. Wypadek oznacza więc, że zabezpieczenia mające zapewnić bezpieczeństwo ludzi i składników majątku oraz odseparowanie ich od zagrożeń zostały naruszone. Jedna z najważniejszych różnic między omawianymi rodzajami wypadków wynika z rodzaju zabezpieczeń.

### 3.2. Zabezpieczenia wielowarstwowe

Zabezpieczenia wielowarstwowe to bariery i środki ochronne spełniające funkcje takie, jak: zrozumienie, świadomość, kierowanie, ostrzeganie, przywracanie, blokowanie, powstrzymanie, ucieczka i ratunek. Wymienione w tym porządku funkcje odpowiadają kolejnym warstwom ochronnym, z których każda ma chronić przed niesprawnością warstwy poprzedzającej, poczy-

nając od zrozumienia i uświadomienia lokalnych zagrożeń na pierwszym etapie, a kończąc na zapewnieniu środków pozwalających na ucieczkę i ratunek na wypadek niemożności opanowania zagrożenia.

Wielość tych nakładających się na siebie i wspomagających wzajemnie środków zabezpieczających zmieniła oblicze wypadków przemysłowych. Współczesne systemy technologiczne są w większości odporne na pojedyncze awarie. W dziedzinach, w których wykorzystuje się starsze lub tradycyjne technologie, wciąż dochodzi do dużej liczby wypadków na poziomie jednostki. Natomiast systemy nowoczesnych technologii są w dużej mierze odporne na odosobnione awarie, a wypadki na poziomie jednostek zdarzają się stosunkowo rzadko. Główne zagrożenie stanowią wypadki na poziomie organizacji, w których udział przyczynowy mają osoby rozproszone zarówno w systemie, jak i w czasie. W kontekście dawniejszych technologii działalność człowieka przeważnie sprowadzała się do produkcji. Funkcjonowanie nowoczesnych technologii opiera się na ogół na zautomatyzowanych systemach, mniej przejrzystych dla operatorów, którzy pełnią przede wszystkim funkcję nadzorczą. Coraz bardziej oddalają się – zarówno przestrzennie, jak i intelektualnie – od procesów produkcyjnych, nad którymi nominalnie sprawują nadzór. W wyniku tego ma miejsce „podstępne" nawarstwianie utajonych problemów (Reason 1998, s. 8).

### 3.3. Problemy utajone

Ludzie przyczyniają się do powstawania wypadków na dwa sposoby. Najczęściej podejmują niebezpieczne działania o bezpośrednich skutkach niepożądanych (czyli tzw. niepowodzenia czynne). Jednakże coraz popularniejszy staje się pogląd, że osoby funkcjonujące w złożonych systemach dopuszczają się niebezpiecznych działań z powodów, które przeważnie nie wynikają z omylności i psychologii jednostek. W rzeczywistości chodzi o tzw. problemy utajone. Reason pisze, że problemy utajone są dla organizacji technologicznych tym samym, czym patogeny obecne w organizmie człowieka:

> Tak jak patogeny, problemy utajone – np. projekty o niskiej jakości, luki w nadzorze, niewykryte defekty produkcyjne lub nieodpowiednia konserwacja, niewykonalne procedury, nieudolna automatyzacja, braki w wyszkoleniu, nieodpowiednie narzędzia i wyposażenie – mogą być obecne przez wiele lat, nim wreszcie w połączeniu z pewnymi okolicznościami i czynnymi niepowodzeniami dojdzie do naruszenia licznych warstw obronnych systemu. Powstają na skutek strategicznych i zewnętrznych decyzji podejmowanych na najwyższych szczeblach przez rządy, prawodawców, producentów, twórców i kierownictwa organizacji. Tego rodzaju decyzje wpływają na całe organizacje, kształtując określoną kulturę korporacyjną i przyczyniając się do powstawania w poszczególnych miejscach pracy czynników sprzyjających popełnianiu błędów (ibidem, s. 10).
>
> Problemy utajone stanowią zatem nieodłączną część systemów złożonych ze względu na związek z podstawowymi procesami organizacyjnymi: projektowaniem, budową, eksploatacją, utrzymaniem, porozumiewaniem się, dokonywaniem wyborów, szkoleniem, nadzorowaniem i zarządzaniem. (…) Stanowią podstawowe elementy każdego procesu produkcji (ibidem, s. 36).

W przeciwieństwie do niepowodzeń czynnych problemy utajone nie wywierają natychmiastowych skutków, mogą pozostawać nieaktywne przez dowolny okres, nie powodując szkód do chwili, gdy dojdzie do interakcji z lokalnym splotem okoliczności i naruszenia zabezpieczeń systemu. O ile większość niepowodzeń czynnych ma miejsce na pierwszej linii, na styku człowiek–system, o tyle problemy utajone rodzą się na wyższych szczeblach i w toku powiązanych z nimi procesów. Mogą się łączyć z czynnikami lokalnymi danego miejsca pracy i naruszać zabezpieczenia niezależnie od jakichkolwiek bezpośrednich ryzykownych działań. Tego rodzaju działanie nie jest warunkiem koniecznym zaistnienia wypadku na poziomie organizacyjnym. Jest nim rzadko spotykane ujawnienie się kilku luk w kolejnych zabezpieczeniach oraz utajonych problemów.

Porównując hipotetyczny wypadek dyliżansu z wypadkiem jumbo jeta, Reason przekonująco argumentuje, że podobne dochodzenie skupione wokół jednostki nie miałoby praktycznie szans na zwiększenie bezpieczeństwa działania jumbo jeta jako systemu. Zabezpieczenia wielowarstwowe mają swoje wady i zalety: z jednej stro-

ny chronią system, lecz z drugiej same w sobie bywają źródłem zagrożeń, zwłaszcza na skutek przemieszczania potencjalnych źródeł błędów poprzez mnożenie elementów i połączeń między nimi, co w rezultacie zmniejsza przejrzystość całego systemu dla operatorów, zwiększając ich poczucie bezpieczeństwa i obniżając czujność. Tym samym przyczyniają się do narastania utajonych problemów.

3.4. Podsumowanie

- Utajonych problemów nie da się uniknąć. Stanowią zagrożenie we wszystkich niebezpiecznych dziedzinach wykorzystujących nowoczesne technologie, podczas gdy czynnik ludzki wpływa na te dziedziny w zmiennym zakresie.
- Rozpoznawanie i eliminacja utajonych problemów stanowią główny sposób poprawy bezpieczeństwa. Jest to jednak ciągły i niekończący się proces, gdyż w miejsce jednego rozwiązanego problemu pojawią się inne.
- Często czynniki, które wywołały wypadek, wydają się oczywiste po fakcie. Niestety równie często zapomina się o tym, że pewien sygnał może stanowić zwiastun katastrofy „tylko wtedy, gdy wiadomo, jaka to będzie katastrofa" (Reason 1998, s. 39). Jednak z punktu widzenia podmiotów biorących udział w pewnych wypadkach wiele z nich to „wypadki niemożliwe", a dochodzi do nich dlatego, że „ludzie nie wierzą, iż naprawdę mogą się wydarzyć" (Wagenaar, Groeneweg, cyt. za: ibidem). Wiedza na temat rzeczywistego przebiegu wydarzeń wpływa na naszą ocenę zachowań osób, które brały w nich udział. Wynika to ze zjawiska, które psychologowie nazywają złudzeniem myślenia wstecznego (Fischhoff 1975).
- Istnieje pewna asymetria zastosowań. Podejście organizacyjne przedstawione powyżej uzupełnia tradycyjne opisy skoncentrowane na działaniach jednostek oraz na zjawiskach zachodzących na styku człowiek–maszyna. Jednak chociaż podejście organizacyjne można zastosować do ograniczania ryzyka obrażeń ciała, podejście personalistyczne nie nadaje się do rozwiązywania problemów związanych z tym rodzajem nieredukowalności, jaki spotykamy, analizując rolę odgrywaną przez czynniki organizacyjne w powstawaniu wypadków na poziomie organizacji. Tego rodzaju nieuchronność i nieredukowalna nieprzejrzystość to cechy, z istnieniem których musi się pogodzić nauka o bezpieczeństwie i zarządzaniu bezpieczeństwem w systemach kompleksowych.

## 4. Nieredukowalne ryzyko i systemy o wysokim poziomie bezpieczeństwa

Analizy wypadków zwyczajnych i wypadków na poziomie organizacji świadczą o tym, że nie da się całkowicie wyeliminować poważnych wypadków związanych z wykorzystywaniem nowoczesnych technologii ze względu na cechy systemów i występowanie utajonych problemów w organizacji. To bardzo ważny wniosek, dający podstawy do dalszej refleksji. Eksponuje on nieredukowalność jako nieodłączną cechę nowoczesnych systemów łączących zaawansowaną technologię, wysoką specjalizację operatorów i naciski konkurencji, która wymusza coraz większą wydajność zarówno produkcyjną, jak i komercyjną. Analizę tę przeprowadzono na podstawie awarii, błędów i wypadków obserwowanych na poziomie globalnym. Można ją kontynuować w kilku kierunkach. Po pierwsze, drugą stronę wypadków stanowi zarządzanie bezpieczeństwem. Wśród systemów badanych przez Perrowa i Reasona znajdują się takie, w których osiąga się wysoki poziom bezpieczeństwa, a poważne wypadki, chociaż nieuniknione, zdarzają się rzadko. Takie systemy to m.in. lotnictwo pasażerskie, elektrownie jądrowe oraz nowoczesne kolejnictwo. Na ich podstawie można badać granice poprawy poziomów bezpieczeństwa, a także to, w jakich warunkach ryzyko resztkowe uznaje się za wystarczająco niskie. Po drugie, w tego rodzaju analizach zwykle nie uwzględnia się tego, jak wykonują swoje zadania operatorzy pierwszej linii. A jednak istnieją zarówno bezpośrednie, jak i pośrednie związki między czynnikami systemowymi i organizacyjnymi z jednej strony a zdarzeniami – z drugiej. Ryzyko akceptowalne i nieredukowalne można więc analizować także na poziomie operatorów z punktu widzenia ergonomii stosowanej w kontekście systemów o wysokim pozio-

mie bezpieczeństwa. Zajmiemy się tymi kwestiami poniżej. Ostatnia, trzecia możliwość, polega na uzupełnieniu rozważań o wysokim poziomie bezpieczeństwa i akceptowalnym ryzyku resztkowym na poziomach regulacji i społecznym o zasadę ostrożności, którą będziemy omawiać w kolejnej części.

Wnioski przedstawione przez Perrowa i Reasona prowokują, ponieważ zakładają, że – niezależnie od wysiłków podejmowanych przez ludzi, czy to twórców, kierowników, czy operatorów – poważnych wypadków nie da się uniknąć w systemach i organizacjach wykorzystujących nowoczesne, zautomatyzowane technologie. Jednak ten rodzaj endogenizacji ma *de facto* charakter częściowy. Można obrać dwa kierunki analizy, przyjmując ogólne założenie, że najwięcej można się dowiedzieć z badania sytuacji skrajnych, tj. takich, w których w zwykłych okolicznościach utrzymuje się wysokie ryzyko resztkowe w tzw. systemach o wysokim poziomie bezpieczeństwa (*high-safety system*). Pierwszy kierunek bazuje na pojęciu akceptowalnego ryzyka, natomiast drugi dotyczy ergonomii kognitywnej bezpieczeństwa na poziomie operatorów pierwszej linii.

Nieredukowalność ryzyka i niemożność uniknięcia poważnych wypadków, nawet w przypadku systemów o wysokim poziomie bezpieczeństwa, wymagają odpowiedzi na pytania, jakie są granice akceptowalności ryzyka oraz jaki poziom bezpieczeństwa konkretne podmioty uznają za dostateczny lub wystarczająco dobry. W kontekście nieredukowalności akceptowalność ryzyka i metody stosowane do jego osiągnięcia stanowią przykłady praktycznej realizacji wyżej opisanej koncepcji progu, a także pozwalają zbadać dogłębniej jej implikacje dla złożoności.

Dalsze rozważania przebiegać będą dwutorowo. Poniżej zajmiemy się operatorami pierwszej linii na poziomie mikro, a następnie przeanalizujemy poziom regulacji w podrozdziale poświęconym zasadzie ostrożności. Tym samym poddamy analizie łącznie cztery poziomy nieredukowalności w zarządzaniu bezpieczeństwem i nauce o bezpieczeństwie, przechodząc od poziomu mikro do poziomu organizacji, systemu, regulacji i społeczeństwa.

### 4.1. Systemy o wysokim poziomie bezpieczeństwa

Systemy o wysokim poziomie bezpieczeństwa to te, w których prawdopodobieństwo wystąpienia poważnego wypadku z co najmniej jedną ofiarą śmiertelną wynosi mniej więcej jeden na milion operacji. Do systemów tych zaliczają się np. lotnictwo pasażerskie, elektrownie jądrowe i nowoczesne kolejnictwo. W lotnictwie pasażerskim, czyli w dziedzinie, na której się skupimy, przeciętne ryzyko oszacowano na $10^{-6}$ na podstawie liczby startów i lądowań. W 1995 r. liczba ta dla różnych przewoźników lotniczych wahała się między 1 na 260 tys. w najgorszych przypadkach, a 1 na 11 mln – w najlepszych, można więc mówić o 42-krotnej różnicy (Reason 1998, s. 191). Z kolei na początku lat 90. różniła się między rozmaitymi obszarami geograficznymi dziesięciokrotnie i wynosiła od $5 \times 10^{-6}$ w najgorszych przypadkach (kraje wschodnioeuropejskie, Afryka, niektóre kraje azjatyckie) do $0{,}5 \times 10^{-6}$ w USA (Amalberti 1996, s. 30). Z historycznego punktu widzenia ryzyko to zmniejszało się wyraźnie do końca lat 60. i osiągnęło obecny poziom w połowie lat 70. Od tego czasu nie uległo dalszemu spadkowi. Od ponad trzech dziesięcioleci mamy więc do czynienia z pewnego rodzaju asymptotą. Zakładając brak dalszych postępów w dziedzinie bezpieczeństwa i biorąc pod uwagę tendencję wzrostową w ruchu lotniczym, która dała się zaobserwować przed wydarzeniami z 11 września 2001 r., można się było spodziewać, że w roku 2010 dojdzie do dwukrotnie większej liczby wypadków niż w roku 2000, co przełożyłoby się na ok. 50 poważnych wypadków rocznie. Liczbę $0{,}5 \times 10^{-6}$ wyrażającą ryzyko wystąpienia wypadku o rozmiarach katastrofalnych (ofiary śmiertelne lub inne znaczące konsekwencje) na jednostkę bezpieczeństwa (zmienna w zależności od branży i rodzaju transportu) można więc uznać za asymptotę bezpieczeństwa dla dzisiejszych ultrabezpiecznych systemów makrotechnicznych, takich jak energetyka jądrowa, lotnictwo pasażerskie oraz europejska sieć kolejowa (Amalberti 2001, s. 110).

Podane powyżej dane liczbowe wskazują na jeden z paradoksów obecnych systemów o wysokim poziomie bezpieczeństwa: nowoczesne systemy technologiczne są bardziej wydajne i nie-

zawodne od swoich poprzedników, mimo to poziom ryzyka resztkowego trudniej zaakceptować niż dawniej. Źródłem kolejnego paradoksu jest fakt, że związana z rozwojem technologicznym poprawa wydajności wydaje się nie mieć granic, podczas gdy postępy na drodze do zwiększania bezpieczeństwa wydają się napotykać na wyraźne ograniczenia. Widać to najlepiej na przykładzie przeciętnego ryzyka wystąpienia poważnych wypadków, które ustabilizowało się na poziomie $10^{-6}$.

Skąd się bierze to ograniczenie? Nie ma raczej przyczyn o charakterze technicznym, zwłaszcza w lotnictwie. Przeskok do poziomu ryzyka rzędu $10^{-7}$ w ciągu następnych dwudziestu kilku lat nie wydaje się nieosiągalny intelektualnie, wtedy jednak będziemy mieli do czynienia z zupełnie innym systemem (Durand, Alliot 1999). Jego koszty będą bardzo wysokie. Z praktycznego punktu widzenia pozostaje on więc poza naszym zasięgiem.

## 4.2. Kwestia akceptowalnego poziomu ryzyka

Pojęcie akceptowalnego poziomu ryzyka ma kilka znaczeń. Podjęcie ryzyka może się wiązać z możliwością porażki lub wypadku. Operatorzy i użytkownicy systemu podejmują je świadomie, chociaż istnieją rozwiązania mające na celu jego ograniczenie. Nie są jednak wdrażane z różnych przyczyn (koszty, spadek wydajności pracy, opór na zmiany zachowań – co dotyczy np. bezpieczeństwa ruchu drogowego itd.). W szerszym sensie akceptowalność ryzyka może się łączyć z brakiem rozwiązań zmierzających do zmniejszenia ryzyka wystąpienia poważnych wypadków w perspektywach krótko- i średnioterminowej. Dotyczy to wszystkich systemów o wysokim poziomie bezpieczeństwa. W ich przypadku akceptowalność ryzyka odnosi się do konkretnej technologii. Gdy akceptowalność znika, wzrasta prawdopodobieństwo całkowitej rezygnacji z danej technologii. Za przykład niech posłużą tak odległe od siebie zdarzenia, jak wypadek sterowca w 1937 r. oraz niedawne decyzje o zaniechaniu rozwoju energetyki jądrowej w Szwecji i Niemczech. W systemach o wysokim poziomie bezpieczeństwa szczególnie istotne jest dodatkowe rozróżnienie między dwoma rodzajami ryzyka i bezpieczeństwa. Istnieje ryzyko wywołane bieżącymi awariami i incydentami oraz dążenie do ich ograniczania do bardzo niskich poziomów, co stanowi definiującą cechę tego rodzaju systemów. Istnieje także nieuniknione ryzyko wystąpienia poważnych wypadków. Z powodu trudności uzyskania dalszej poprawy bezpieczeństwa w systemach o jego wysokim poziomie, uwzględniając wzrost nasilenia ruchu oraz naciski na zwiększenie wydajności, na pierwszy plan wysuwa się raczej utrzymanie istniejącego poziomu bezpieczeństwa i zapewnienia dopuszczalnego poziomu ryzyka wystąpienia poważnych wypadków zarówno dla bezpośrednich użytkowników danego systemu, jak i dla społeczeństwa jako całości.

Można tu wspomnieć o szeregu rozwiązań określających to, co społeczeństwo uznaje za dostateczny poziom bezpieczeństwa. Fischhoff i współpracownicy (1981 [1999]) przedstawili listę siedmiu kryteriów, jakie powinny spełniać procesy podejmowania decyzji na temat określania dopuszczalnego poziomu ryzyka. Powinny one być wszechstronne, oparte na logicznych przesłankach, praktyczne, otwarte na ocenę, akceptowalne politycznie, zgodne z profilami działania instytucji i sprzyjające uczeniu się. Podejście do ryzyka, opisywane skrótem ALARA (*as low as reasonably acceptable* – tak niskie, jak rozsądnie dopuszczalne), opiera się na pewnej liczbie odmiennych podejść. Reason (1998) omawia cztery spośród nich. Jako pierwszy wymienia wykonalność lub podejście typu ALARP (*as low as reasonably practicable* – tak niskie, jak rozsądnie wykonalne), które bazuje na logice technologicznej i ekonomicznej. Innymi słowy, podejście to zakłada, że dostateczne bezpieczeństwo występuje na pewnym poziomie, na którym dalsze jego podwyższanie nie jest ani technicznie, ani ekonomicznie wykonalne. Z kolei podejście oparte na analizie porównawczej ryzyka (*comparative risk approach*) określa wystarczający poziom bezpieczeństwa na podstawie porównań do poziomu ryzyka istniejącego w innych dziedzinach, w których jest ono dobrowolnie akceptowane (np. ruch drogowy, palenie tytoniu, transport kolejowy, lotnictwo pasażerskie itd.). Trzecią możliwość stanowi podejście *de minimis* odpowiadające definicji systemów o wysokim poziomie bezpieczeństwa zwykle określanych jako ryzyko na poziomie $10^{-6}$ lub niższe. Skrajne podejście

to tzw. podejście zerowego ryzyka, według którego bezpieczeństwo oznacza zupełny brak ryzyka poważnego wypadku. Mogą je proponować zdeklarowani przeciwnicy rozwiązań takich, jak energetyka jądrowa, lecz w praktyce oznacza ono całkowitą rezygnację z określonego rodzaju działalności.

Na koniec należy wspomnieć o dodatkowym ważnym podejściu, mianowicie partycypacyjnym. Różni aktorzy mniej lub bardziej bezpośrednio i mniej lub bardziej oficjalnie uczestniczą w procesie podejmowania decyzji. Naturalnie problem polega na tym, czy przez to stają się współdecydentami, czy też pozostają tylko dobrze poinformowanymi aktorami. We wszystkich przypadkach główną kwestią wydaje się akceptacja ryzyka. W systemach o wysokim poziomie bezpieczeństwa, w których trudno jeszcze bardziej go poprawić, akceptacja ryzyka nabiera coraz bardziej decydującej wagi, podczas gdy w innych wyraźny priorytet wyznacza dążenie do poprawy bezpieczeństwa, gdyż zakres możliwości w granicach tego rodzaju systemów pozostaje dość szeroki.

Znacząca poprawa bezpieczeństwa w systemach o wysokim poziomie bezpieczeństwa często, jak się wydaje, wymaga zmiany systemu jako takiego, co nie jest wykonalne w krótko- ani nawet średnioterminowej perspektywie czasowej. W takiej sytuacji w granicach istniejącego systemu można poszukiwać ulepszeń – systemowych lub odnoszących się do operatorów pierwszej linii. Tego rodzaju podejście rozwija René Amalberti w kategoriach ergonomii poznawczej w odróżnieniu od czystej inżynierii (Amalberti 1996, 1997, 1999).

### 4.3. Ergonomia poznawcza ryzyka

Ergonomię często nazywa się sposobem badania „zadań wziętych z życia" (Rasmussen, Jensen 1974), co pozwala na wyjście poza rozważanie wyłącznie systemów nominalnych i aspektów poznawczych. Nieodłącznym elementem tego podejścia jest uwzględnienie ludzi wykonujących daną pracę.

Z perspektywy czasu warto się zastanowić, czy ergonomia jako dyscyplina dysponuje uogólnieniami zdolnymi pełnić funkcję testu. Nasze doświadczenie stawia nas w obliczu pewnej formy nieredukowalności i polega na przezwyciężaniu problemów w celu wykonania danego zadania. Ergonomia bezpieczeństwa także zajmuje się pewną formą nieredukowalności, gdy staje wobec ryzyka, którego poziomu nie da się obniżyć. Lecz rozpoczynając dociekania, nie zwracaliśmy uwagi na to podobieństwo. I rzeczywiście, mimo pojawienia się pewnych pionierskich prac w tej dziedzinie w latach 70. i 80. XX w., dopiero niedawno, dzięki badaniom poświęconym wypadkom występującym w systemach i organizacjach, stało się możliwe podjęcie prób rozwinięcia tych spostrzeżeń z perspektywy ergonomii. W książce opublikowanej w 1996 r. René Amalberti zaczyna od wyraźnego, choć krytycznego nawiązania do pracy Reasona poświęconej błędom człowieka (Reason 1993). Zwraca uwagę raczej na kwestie bezpieczeństwa niż na błędy. W tej dziedzinie istnieje obszerne piśmiennictwo. W naszej analizie wykorzystujemy głównie analizę przeprowadzoną przez Amalbertiego na temat technologii o wysokim poziomie bezpieczeństwa. Zaliczają się do nich energetyka jądrowa, lotnictwo pasażerskie i kolejnictwo. Podążając śladami tego autora, skoncentrujemy się na bezpieczeństwie w lotnictwie. Amalberti wyjaśnia, jak operatorzy pierwszej linii zarządzają bezpieczeństwem na podstawie zarówno empirycznych obserwacji tych operatorów podczas pracy – takich jak piloci samolotów za sterami maszyn na symulatorach. Modelowanie to wywodzi się z prowadzonych w systemach wysokich technologii badań normalnych warunków pracy, a nie wypadków. Ogólne tło analityczne stanowi ergonomiczna psychologia poznawcza. Perspektywa ta koncentruje się na zadaniach wziętych z życia w naturalnych warunkach pracy, co uzasadnia zastosowanie terminu „bezpieczeństwo ekologiczne" do opisu tego podejścia. Najpierw przedstawimy jej główne założenia, a następnie omówimy ją bardziej szczegółowo.

Punkt wyjścia dla tej perspektywy stanowi koncepcja, że optymalizacja nie jest możliwa z powodu ograniczonych zasobów poznawczych. Zamiast tego obserwuje się kompromis poznawczy osiągany między trzema celami: bezpieczeństwem, wydajnością oraz minimalizacją fizjologicznego i umysłowego wpływu operatora na wydajność (zmęczenie i stres). Cytowane studia przypadków wspierają stwierdzenie Amal-

bertiego, że pierwszym ryzykiem dostrzeganym przez operatora nie jest ryzyko wypadku, lecz utraty panowania nad sytuacją, stąd dynamiczny *kompromis poznawczy*, w którym przeważa akceptacja rozwiązań wystarczająco dobrych. Ten kompromis dynamiczny polega na wykonywaniu zadań i dążeniu do stabilizacji systemu poprzez zachowania dostatecznie dobre, w warunkach błyskawicznego rozwoju wydarzeń, niepełnej znajomości i zrozumienia funkcjonowania systemu jako całości. Ogólnie rzecz biorąc, pojęcia kompromisu poznawczego i bezpieczeństwa ekologicznego stanowią centralne punkty argumentacji Amalbertiego, która różni się od modelu inżynieryjnego. Ten ostatni zwykle koncentruje się na tym, jak na operatorów pierwszej linii, takich jak piloci lub pracownicy kontroli lotów, wpływa charakterystyka ich miejsca pracy, a zwłaszcza informacyjne własności płaszczyzny kontaktu (interfejsu) człowieka z maszyną. Jak ujmuje to Reason, bezpieczeństwo postrzega się jako coś, co należy „wbudować" w system i co często wyraża się w ilościowych kategoriach probabilistycznych. W tym podejściu ograniczenie liczby awarii z winy człowieka zależy od skutecznej interwencji inżynieryjnej człowieka (ergonomii), czyli od zdolności projektantów do stworzenia systemu dostosowanego do zdolności poznawczych jego operatorów.

Właśnie na tym etapie perspektywa ergonomiczna wnosi element nowości, uwzględniając zarówno poznawcze, jak i praktyczne zdolności operatorów. Reason krytykuje model inżynieryjny, gdyż bagatelizuje on rolę czynników organizacyjnych. Analiza bezpieczeństwa z punktu widzenia ergonomii poznawczej również zawiera krytykę inżynieryjnego punktu widzenia, lecz z zupełnie innej przyczyny: krytykuje nadmierną koncentrację na optymalizacji jako sposobie poprawy bezpieczeństwa. W rzeczywistości wszystkie systemy o wysokim poziomie bezpieczeństwa opierają się na stopniowej (zaplanowanej) optymalizacji komponentów bezpieczeństwa. Jednak strategia ta jest bardziej skuteczna w warunkach istnienia znacznych marginesów bezpieczeństwa, gdy nadal znajduje się ono poniżej wysokiego poziomu. Dość często spotyka się opinie, że systemy zaprojektowane są tak, aby działały na maksymalnym poziomie bezpieczeństwa, lecz nie mogą tego osiągnąć z powodu awarii, jakim ulegają. Dlatego celem działania powinna być eliminacja wszystkich ludzkich błędów i awarii technicznych zidentyfikowanych w systemie. Jak wspomina Amalberti, pogląd ten opiera się na dwóch błędnych założeniach nowoczesnego postrzegania bezpieczeństwa: po pierwsze, że system bezpieczny to taki, który nie ulega awariom, a po drugie, że wszystkie awarie należy eliminować. Właśnie te założenia stopniowo zamknęły w ślepym zaułku myślenie o bezpieczeństwie w systemach o wysokim jego poziomie, bez względu na efektywność tego rozumowania w innych kontekstach.

Na plan pierwszy wysuwają się paradoksalne skutki automatyzacji i konieczność zachowania ścisłego związku między zautomatyzowanym systemem a operatorem (człowiekiem), ponieważ w przypadku awarii takiego systemu bezpieczeństwo w ostatecznym rozrachunku zależy od jego interwencji (Bainbridge 1987). Automatyzacja skupiona na człowieku zyskuje coraz więcej zwolenników, zwłaszcza w lotnictwie (Billings 1997) i kontroli ruchu lotniczego (Villiers 1998). Po drugie, w systemach o wysokim poziomie bezpieczeństwa zarządzanie bezpieczeństwem nie może odwoływać się do wypadków z przeszłości ze względu na niewielką ich liczbę. Polega ono raczej na prekursorach, zwiastunach, słabych sygnałach i incydentach oraz na ich systematycznej eliminacji. Lecz obecność incydentów przydaje się, gdyż pomaga utrzymać odpowiedni poziom koncentracji i czujności operatorów. Naturalnie należy dążyć do kompromisu między dwiema skrajnościami – lekceważeniem wszystkich incydentów i próbami ich zupełnej eliminacji. W wyniku systematycznej eliminacji liczby incydentów rośnie zaufanie pokładane w funkcjonowanie systemu, wzrasta wydajność i zawężają się marginesy działania operatorów. Tego rodzaju zmiany z reguły przyczyniają się do powstawania warunków sprzyjających wzrostowi ryzyka występowania poważnych awarii tego samego rodzaju, co nagromadzenia utajonych problemów w organizacjach analizowanych przez Reasona. Bardzo poważne incydenty, które wielokrotnie występowały w siłowniach jądrowych w Japonii w latach 1995, 1996 (Triendl 1999) oraz 1999 (Science et Vie 2000) okazały się ogromnym zaskoczeniem w kraju, w którym sektor jądrowy uważano za

najbezpieczniejszy na świecie ze względu na minimalną liczbę wypadków.

Model bezpieczeństwa ekologicznego przeciwstawiany bywa modelowi optymalizacji. Opiera się na wynikach empirycznych badań zachowań operatorów – zwłaszcza pilotów – w konkretnych sytuacjach. Pokazuje, że celem operatora jest opanowanie sytuacji, czyli zmieszczenie się w granicach dopuszczalnych marginesów bezpieczeństwa przy określonym docelowym poziomie wydajności. Gdy pojawiają się błędy, operator najpierw obniża poziom wydajności, pragnąc je opanować i kontynuować działanie. Zmienną regulującą wydaje się tu więc poczucie panowania nad sytuacją, a nie liczba błędów. Nadmiernie zautomatyzowane rozwiązania prowadzą do ograniczenia orientacji operatora w sytuacji.

Amalberti stawia tezę, że w celu poprawy poziomu bezpieczeństwa lub utrzymania już wysokiego jego poziomu wraz ze wzrostem wydajności, zachodzi konieczność pogodzenia się z drobniejszymi awariami lub błędami, a nie podejmowania prób ich systematycznej eliminacji. Przyczynami są nadmierne zmęczenie i stres, jakie tego rodzaju strategia narzucałaby operatorowi. Stąd dążenie do uzyskania równowagi. System bezpieczny to nie taki, w którym nie występują awarie, lecz taki, w którym operatorzy panują nad awariami i błędami. Podobnie dobrzy operatorzy to nie ci, którzy nie popełniają błędów, lecz ci, którzy potrafią je wykryć i skorygować w taki sposób, aby przywrócić sprawność systemu. Tak więc, chcąc poprawić lub przynajmniej utrzymać obecny niski poziom poważnego ryzyka w systemach o wysokim poziomie bezpieczeństwa, należy się pogodzić z występowaniem ryzyka niższego rzędu.

Na rycinie 1 przedstawiono model zachowania operatorów zainspirowany rozważaniami Amalbertiego. Autor opisuje „kompromis poznawczy", jaki zachodzi między „kosztem poznawczym zdobywania wiedzy specjalistycznej", „kosztem poznawczym działania w czasie rzeczywistym" i docelowym poziomem wydajności (Amalberti 1996, s. 194). Im wyższych poziomów wydajności wymaga się od operatorów, tym wyższe oba są rodzaje kosztów. Odbiegamy nieco od tego modelu, gdyż zamiast kosztami zajmujemy się wzrastającymi poziomami trudności i odróżniamy trudności poznawcze od praktycznych, co jednak nie oznacza, że oba te pojęcia istnieją osobno. Niemniej jednak można się nauczyć obsługi pewnej części systemu, nie posiadając jednocześnie minimalnych praktycznych zasobów potrzebnych do działania w warunkach rzeczywistych. I odwrotnie, można dysponować zasobami praktycznymi, nie mając minimum koniecznej wiedzy. To sytuacja graniczna, w której operator dysponuje pewnymi teoretycznymi podstawami, lecz nie ma żadnych kompetencji praktycznych lub ma pewne doświadczenie empiryczne bez podstaw teoretycznych. Ta sytuacja odpowiada punktowi M na rycinie 2. Kompromis zależy wtedy od trudności poznawczych i praktycznych związanych z określonym poziomem wydajności. Rycina 1 przedstawia oba rodzaje obszarów – wewnątrz i na zewnątrz pięciokąta MNOPQ. Sporządzono ją w czysto heurystycznym celu. Dla uproszczenia linie narysowano symetrycznie względem dwusiecznej. To samo dotyczy linii kropkowanych określających granice obszarów (A), (B) i (C) wewnątrz pięciokąta oraz rozpoczęcia analizy od punktu M – z równych minimalnych poziomów zasobów poznawczych i praktycznych OK i OL.

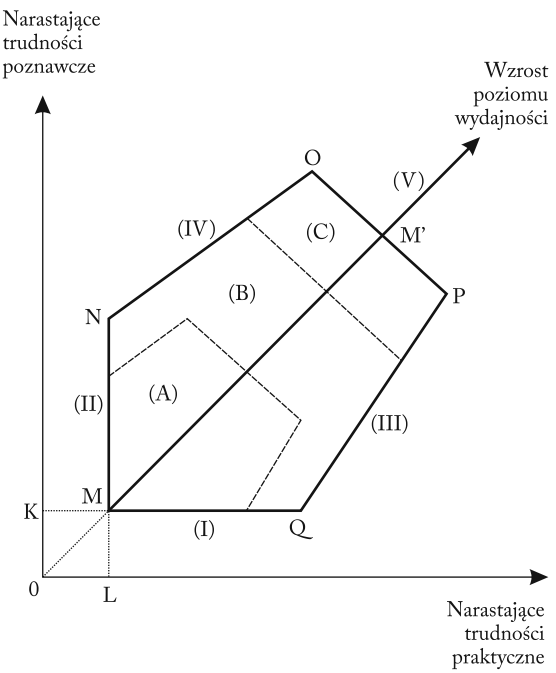
Kompromis osiąga się wewnątrz pięciokąta, a na zewnątrz leżą obszary poza granicami kompromisu. Dla przypomnienia – kompromis określa warunki, w których operator może zachować panowanie nad sytuacją. W obszarze (A) istnieje margines pozwalający na poprawę. To obszar „komfortu". Marginesy te można wykorzystać w obszarze (B) do zwiększenia wydajności dzięki bodźcom i lepszej motywacji. To obszar „motywacji". Samoograniczaniu wydajności poprzez wykrywanie błędów i przywracanie sprawności przeciwdziałają wzrastające wymagania w zakresie wydajności. W tym obszarze narastają więc zmęczenie i stres.

Obszar (C) przedstawia sztuczny zakres dostępny tylko w przypadku zastosowania sztucznych środków pomocniczych. Wymagają one obniżenia ogólnej liczby awarii, co umożliwi zwiększenie wydajności. Towarzyszy temu ryzyko wzrostu liczby niewykrytych błędów, po których nie przywrócono systemu do właściwego stanu. To obszar „sztuczny". Wymuszenie wyjścia systemu poza punkt graniczny M' lub poza OP zaburza sztuczny kompromis i stwarza

warunki sprzyjające wystąpieniu poważnej awarii. OP reprezentuje wtedy swego rodzaju barierę bezpieczeństwa stworzoną przez nacisk na zwiększanie wydajności w warunkach ograniczonych zasobów poznawczych i praktycznych operatora.

Obszary od I do V symbolizują sytuację braku lub utraty panowania nad sytuacją. W obszarze I brak panowania nad sytuacją spowodowany jest brakiem minimalnej wiedzy. W obszarze II przyczyną utraty panowania jest brak minimalnych zasobów praktycznych. Obszar III odpowiada przeciążeniu pracą: utratę panowania powoduje niepełne dostosowanie praktyczne. Podobnie utrata panowania w obszarze IV wynika z braku wiedzy spowodowanej przeciążeniem poznawczym. I wreszcie obszar V symbolizuje utratę panowania nad sytuacją z powodu namnożenia się niewykrytych błędów oraz zarówno niepełnego dostosowania praktycznego, jak i niepełnej wiedzy.

Kompromis ekologiczny odpowiada obszarom (A) i (B), w których operator dostosowuje poziom wydajności do własnych zdolności poznawczych i praktycznych w czasie rzeczywistym. W przypadku dostrzeżenia ryzyka zakłóceń obniża poziom wydajności w celu przywrócenia równowagi i zrozumienia sytuacji, a następnie podejmuje próby zwiększenia wydajności. Mamy tu więc do czynienia z kompromisem między wydajnością i bezpieczeństwem. Stanowi to uzupełnienie modelu utajonych problemów Reasona: występują one zwłaszcza w obszarze (C) – sztucznego kompromisu, oraz poza punktem M', poza którym wzrasta ryzyko zaistnienia poważnej awarii, gdyż operator nie panuje już nad sytuacją. Na poziomie operatora można więc zidentyfikować trzy operacyjne źródła nieredukowalności wypadków w obszarach III, IV i V. W ten sposób kontekst behawioralny także endogenizuje nieredukowalność ryzyka, podobnie jak wyżej wspomniane systemowe i organizacyjne punkty widzenia.




Ryc. 1. Teoretyczny operator i kompromis między wydajnością a bezpieczeństwem

Zaprezentowany model pokazuje, dlaczego ograniczanie ryzyka może nie poddawać się optymalizacji. Inżynieryjne i techniczne tymczasowe środki zaradcze zmniejszają co prawda ryzyko wystąpienia bieżących awarii i zwiększają wydajność, lecz przyczyniają się także do wzrostu liczby utajonych problemów sprzyjających występowaniu poważnych awarii. Model ten sugeruje wprost, że sama tylko optymalizacja i eliminacja błędów nie stanowią odpowiednich strategii ze względu na niemożność zredukowania ryzyka wystąpienia poważnych awarii w systemach o wysokim poziomie bezpieczeństwa. Nie istnieje liniowy związek między drobnymi i poważnymi wypadkami. Model Amalbertiego mówi nam, że sposobem na ograniczenie liczby poważnych awarii jest odwołanie się do kompromisów, co zwykle praktykują wyszkoleni operatorzy. Ilustruje on również, jak badanie warunków granicznych (tu: ryzyka wystąpienia poważnej awarii) wywiera zwrotny wpływ na bieżące działanie systemu, jest więc niezbędny do zrozumienia codziennego nim zarządzania.

## 5. Zasada ostrożności

Kierując się zasadą ostrożności, zarządzamy ryzykiem na poziomie władz publicznych, lecz nie ogranicza się ona do dziedziny regulacji. Zasada ostrożności może wymagać podjęcia decyzji o działaniu lub powstrzymaniu się od niego. Natomiast decyzja o działaniu może

obejmować zarówno działania regulacyjne, jak i finansowanie badań oraz informowanie społeczeństwa o potencjalnych zagrożeniach.

Zasada ostrożności jest szczególnie interesująca z punktu widzenia celu naszych rozważań, ponieważ rozszerza pojęcie akceptowalnego ryzyka z ostatniej części na sytuacje, które nie ograniczają się do systemów o wysokim poziomie bezpieczeństwa ani do nowoczesnych systemów technologicznych. Dzięki temu oferuje sposobność bardziej szczegółowego zbadania procesu określania akceptowalnego ryzyka na poziomie społeczeństwa. Ponieważ zasada ostrożności zasadza się na istnieniu luki między wiedzą i ryzykiem w określonej sytuacji, samo pojęcie dopuszczalnego ryzyka to inna nazwa progu ryzyka, powyżej którego nie jest już ono akceptowalne.

## 5.1. Definicja

Ostrożność rozumiana jako zasada ostrożności wywodzi się z zaniepokojenia zanieczyszczeniem środowiska w latach 70. XX w. Zawarta w 1972 r. konwencja z Oslo na temat zapobiegania zanieczyszczeniu mórz i Londyński Akt Końcowy z 1987 r. dotyczący ochrony Morza Północnego stanowią decydujące kroki, za którymi poszły deklaracje ministrów środowiska krajów OECD (Organizacji Współpracy Gospodarczej i Rozwoju) w 1991 r. Zasadę ostrożności uznano na Konferencji Organizacji Narodów Zjednoczonych na temat Środowiska i Rozwoju (UNCED) w Rio de Janeiro w 1992 r. Uwzględniono ją także jako zasadę 15. tzw. Deklaracji z Rio (czerwiec 1992 r.) wymienioną wśród ogólnych praw i obowiązków władz poszczególnych krajów:

> Wszystkie państwa powinny szeroko zastosować podejście zapobiegawcze w celu ochrony środowiska, mając na uwadze ich własne możliwości. Tam gdzie występują zagrożenia poważnymi lub nieodwracalnymi zmianami, brak całkowitej pewności naukowej nie może być powodem opóźniania efektywnych działań, których realizacja prowadziłaby do degradacji środowiska (CEC: Komisja Wspólnot Europejskich 2000, s. 26).

Zasadę tę stopniowo wcielono do międzynarodowego prawodawstwa w zakresie ochrony środowiska i stała się odtąd ogólną zasadą prawa międzynarodowego. Porozumienia WTO (Światowej Organizacji Handlu) potwierdzają to spostrzeżenie ze względu na związki między handlem zagranicznym i ochroną środowiska, chociaż termin „zasada ostrożności" jako taki nie został w nich użyty.

Zasada ta znalazła także swój wyraz w przepisach prawnych kilku krajów. Przykładowo, francuski przepis z 1995 r. stwierdza: „Brak pewności w odniesieniu do dowodów naukowych i technicznych istniejących w danej chwili nie może opóźniać podejmowania skutecznych i proporcjonalnych decyzji mających na celu zapobieganie ryzyku powstania znacznych i nieodwracalnych szkód dla środowiska przy gospodarczo dopuszczalnych kosztach". Zasadę tę wcielono do konstytucji Republiki Francuskiej w 2005 r.

Komisja Wspólnot Europejskich oświadczyła, że „w ślad za przykładem innych Członków WTO Wspólnota upoważniona jest do określenia poziomu ochrony, zwłaszcza w odniesieniu do środowiska naturalnego i zdrowia ludzi, zwierząt i roślin, jaki uzna za stosowny", a w tym celu „oparcie na zasadzie ostrożności stanowi zasadniczy element jej polityki" (CEC 2000, s. 12). Komisja Wspólnot Europejskich wprowadziła tutaj nowy przepis, ponieważ traktat Unii Europejskiej nie definiuje wyraźnie zasady ostrożności i przewiduje jedynie ochronę środowiska naturalnego. Komisja podkreśliła, że zakres zasady ostrożności jest w praktyce o wiele szerszy niż środowisko naturalne i obejmuje zdrowie ludzi, zwierząt i roślin. Ponadto stwierdza, że „Wspólnota, podobnie jak inni członkowie WTO, ma prawo określić poziom ochrony (…), jaki uzna za stosowny" (ibidem, s. 3).

## 5.2. Zakres stosowania

Odwołamy się tutaj do komunikatów Komisji Europejskiej, ponieważ definiują one zakres stosowania zasady ostrożności, który sprawia, że jest ona szczególnie istotna dla decydentów, zwłaszcza władz publicznych, mających za zadanie zarządzanie ryzykiem.

Odwołanie się do zasady ostrożności powinno, po pierwsze, rozpoczynać się od identyfikacji „potencjalnie niebezpiecznych skutków zjawisk,

produktów lub procesów", a po drugie, obejmować zaprezentowanie dowodów, że „ocena naukowa nie pozwala na określenie ryzyka z wystarczającą pewnością" (CEC 2000, s. 4).

Komisja Europejska stwierdza, że „braku dowodów naukowych na istnienie związku przyczynowo-skutkowego dającej się kwantyfikować relacji dawka–odpowiedź lub ilościowej oceny prawdopodobieństwa powstawania szkodliwych wpływów po ekspozycji nie należy używać do uzasadnienia bezczynności" (ibidem, s. 17). Zasada ostrożności obejmuje te okoliczności, w których „dowody naukowe są niedostateczne, nieprzekonywujące lub niepewne, lecz istnieją wskazania na bazie wstępnych obiektywnych ocen naukowych, że są uzasadnione podstawy do obaw, iż potencjalnie niebezpieczny wpływ na środowisko naturalne, zdrowie ludzi, zwierząt lub roślin może być niezgodny z wybranym poziomem ochrony" (ibidem, s. 10). W tym miejscu pojawiają się prawdziwe trudności. Po pierwsze, „obiektywna" ocena naukowa nie wyklucza podziału wśród naukowców i grup specjalistów. Właśnie to istnienie rozbieżnych poglądów wyznawanych przez kompetentnych naukowców na temat konkretnego zagadnienia może wskazywać lub nawet zwiększać stan niepewności naukowej. Po drugie, większą część odpowiedzialności przesuwa się na osąd decydentów: „Osąd tego, co stanowi «dopuszczalny» poziom ryzyka dla społeczeństwa to decyzja o charakterze wybitnie politycznym. Osoby podejmujące decyzje, stojąc w obliczu nieakceptowalnego ryzyka, naukowej niepewności i obaw społeczeństwa, mają obowiązek znaleźć odpowiedzi" (ibidem, s. 4).

Oprócz decyzji o podjęciu lub powstrzymaniu się od działania związanej z dwoma wyżej wspomnianymi czynnikami wzbudzającymi – identyfikacją niebezpieczeństwa i naukową niepewnością na temat ryzyka – pojawia się pytanie, jak działać. Decyzja o niepodejmowaniu żadnych działań może stanowić odpowiedź samą w sobie, gdyż ciążący na decydentach obowiązek zareagowania na sytuację niekoniecznie oznacza konieczność podejmowania jakichkolwiek działań. Komisja podkreśla, że odpowiednia odpowiedź stanowi wynik decyzji politycznej, „funkcję poziomu ryzyka, które zostaje uznane za «akceptowalne» dla społeczeństwa, którego dotyczy" (ibidem, s. 16). Kluczową kwestią jest legitymacja środków, które umożliwiają osiągnięcie tego, co społeczeństwo uważa za dopuszczalny poziom ryzyka lub odpowiednio dostateczny poziom ochrony środowiska lub zdrowia. Rozwiązanie Komisji stanowi, że wszystkie zainteresowane strony powinny zaangażować się „w jak najpełniejszym stopniu w badanie różnych dających się przewidzieć możliwości zarządzania ryzykiem" (ibidem, s. 17).

## 6. Podsumowanie. Nieredukowalność poznawcza i praktyczna

W tekście chcieliśmy wyjaśnić, na jakiej podstawie uznajemy, że trudność związana z wykonaniem określonego zadania ma charakter złożony lub niezłożony. Musieliśmy więc jasno sprecyzować zachowania operatora. Mając nadzieję znaleźć właściwości, które mogłyby się okazać przydatne do tego celu, postanowiliśmy zająć się dziedziną, w której czynniki te odgrywają zasadniczą rolę i były badane od wielu lat, tj. nauką o bezpieczeństwie i zarządzaniu bezpieczeństwem.

Istnieje wiele podejść do zarządzania bezpieczeństwem obejmujących kilka poziomów: od obsady pierwszej linii, przez poziomy człowiek–maszyna, miejsce pracy (inżynieria, ergonomia poznawcza), poziom organizacyjny, poziom systemowy, poziom regulacyjny i wreszcie poziom społeczny. Skoncentrowaliśmy się na czterech perspektywach związanych z kilkoma spośród wyżej wymienionych poziomów. Od nieredukowalności dotyczącej wypadków systemowych (zwyczajnych) przeszliśmy do nieuchronnej nieprzezroczystości i utajonych problemów odnoszących się do wypadków w organizacjach. Następnie podkreśliliśmy nieredukowalność do zera ryzyka resztkowego wystąpienia poważnego wypadku w systemach o wysokim poziomie bezpieczeństwa. Kwestią tą zajmują się najpełniej aktualne prace poświęcone zasadzie ostrożności. Zmierzają one do syntezy wszystkich jej aspektów, o których wspomnieliśmy, z nieodłącznym naciskiem na społeczny poziom kwestii akceptowalnego poziomu ryzyka.

Komisja Europejska podkreśla proceduralny charakter tego, co stanowi akceptowalne ryzy-

ko. Jest ono akceptowalne, jeżeli jest uprawnione, co oznacza udział wszystkich zainteresowanych stron w badaniach nad różnymi opcjami zarządzania nim, które można sobie wyobrazić, „gdy wyniki oceny naukowej oraz/lub wyniki oceny ryzyka udostępnia się w toku możliwie przejrzystych procedur" (CEC 2000, s. 17).

Zasada ostrożności ilustruje proces poszukiwania i kształtowania ogólnych wytycznych do działania w kontekście radykalnej niepewności, w którym gra toczy się z uwzględnieniem wysokiego i nieodwracalnego ryzyka dla środowiska naturalnego, zdrowia ludzi, zwierząt i roślin. Wiąże się z tymi samymi rodzajami trudności co te, które zaobserwowaliśmy podczas analizy ryzyka resztkowego wystąpienia poważnego wypadku w systemach o wysokim poziomie bezpieczeństwa. We wszystkich tych dziedzinach chodzi o uniknięcie wszelkich poważnych wypadków. Wiadomo, że celu tego nie da się osiągnąć ze względu na nieredukowalność poznawczą, co jednak nie przeszkadza nam korzystać z tych technologii. Czy rzeczywiście oznacza to społeczną akceptację związanego z tym ryzyka? Odpowiedzi na to pytanie są różne w zależności od dziedziny – większe rozbieżności opinii panują na temat siłowni jądrowych niż lotnictwa pasażerskiego. Fakt, że technologie te są w sposób ciągły i normalny wykorzystywane w większości krajów, można potraktować jako wskaźnik praktycznej akceptacji poziomu towarzyszącego im ryzyka.

Ze względu na ogólny poziom aspiracji do unikania wszelkich poważnych wypadków jesteśmy zmuszeni zaakceptować fakt istnienia luki między tym celem a dostępną nam wiedzą. Ta luka poznawcza charakteryzuje sytuację poznawczo niedostatecznie dobrą (*non-satisficing*). Niemniej samo pojęcie dopuszczalnego ryzyka można interpretować, wychodząc z praktycznego punktu widzenia. Skoro ludzie akceptują pewien poziom ryzyka, oznacza to, że uznają je w jakimś sensie za zadowalający lub wystarczająco dobry – zaspokajający nasze potrzeby w dostatecznym stopniu. A to z kolei sugeruje sytuację wystarczająco dobrą z praktycznego punktu widzenia.

Wyżej wspomniani „ludzie" mogą reprezentować grupy liczące od kilku osób do całej populacji i społeczeństwa. Podział wystąpi prawdopodobnie na poziomie populacji i osób bezpośrednio zainteresowanych akceptowalnością ryzyka w wybranych dziedzinach: niektórzy zaakceptują pewien poziom ryzyka, a inni nie, co często bywa źródłem kontrowersji. Może nawet pojawić się większość lub dominująca grupa okazująca praktyczne niezadowolenie, nie wyrażając zgody na dany poziom ryzyka. Paralele między tym spostrzeżeniem i przedstawionym powyżej tokiem naszej argumentacji stają się oczywiste, gdy zastąpimy kilka warunków postawionych przez Komisję Europejską własnymi: „odpowiedni poziom ochrony" – poziomem aspiracji, „niewystarczające dowody naukowe" – niezaspokojeniem aspiracji kognitywnych w wystarczającym stopniu, „określenie, co stanowi dopuszczalny poziom ryzyka dla społeczeństwa" oraz „zaangażowanie zainteresowanych stron" – działaniami zmierzającymi do zaspokojenia w wystarczającym stopniu aspiracji praktycznych i poznawczych.

Pora na garść uwag uzupełniających. Na pierwsze miejsce, jak zauważyliśmy wyżej, wysuwa się wystarczająco dobre zaspokojenie aspiracji poznawczych, a następnie praktycznych, w przypadku gdy nie można osiągnąć tych pierwszych.

Po drugie, nasze odniesienie do zaspokajania aspiracji praktycznych nieco upraszcza proces, w którym obecny jest również aspekt poznawczy. Ten ostatni odgrywa ważną rolę w poglądach A. Marshalla i J.M. Keynesa oraz w koncepcji systemu doceniającego (*appreciative system*) G. Vickersa (1995). Ponieważ naszym celem na tym etapie jest odróżnienie wystarczająco dobrego zaspokojenia aspiracji poznawczych (*cognitive satisficing*) od innych, usprawiedliwiona wydaje się decyzja o zaliczeniu tych drugich do grupy wystarczająco dobrego spełniania aspiracji praktycznych (*practical satisficing*) bez względu na stopień i rodzaj zaangażowanego aspektu poznawczego.

Ponadto fakt wystarczająco dobrego zaspokojenia lub niezaspokojenia aspiracji praktycznych stanowi najczęściej wynik debaty i ewolucji opinii publicznej na temat akceptowalności ryzyka. Wywodzi się on ze społeczeństwa i nie jest subiektywny w zwykłym znaczeniu tego słowa. Podlega ewolucji, wiąże się z doświadczeniem oraz z procesem uczenia się. Poszukiwanie wystarczająco dobrej realizacji aspiracji praktycznych

nie jest więc zjawiskiem rozłącznym od wiedzy. W tym sensie sformułowania użyte dotąd w celu odróżnienia od siebie tych dwóch rodzajów spełnienia aspiracji mogą wprowadzać czytelnika w błąd, sugerując, że wystarczająco dobre spełnienie aspiracji praktycznych nie wiąże się z żadnymi treściami poznawczymi. Usprawiedliwione byłoby określenie ich odpowiednio jako wystarczająco dobrego spełnienia aspiracji poznawczo-praktycznych, by odróżnić je od zastosowanego na początku wystarczająco dobrego spełnienia aspiracji wyłącznie poznawczych.

Bez względu jednak na stopień wzajemnego splątania wiedzy i praktyki, przedstawiona powyżej dyskusja sugeruje, że przydatne jest zachowanie rozróżnienia między tymi dwoma rodzajami wystarczająco dobrego spełnienia aspiracji. Dla uproszczenia lepiej będzie pozostać przy terminach „wystarczające spełnienie aspiracji poznawczych" oraz „wystarczające spełnienie aspiracji praktycznych" oznaczających odpowiednio „nieredukowalność poznawczą" i „nieredukowalność praktyczną", w przypadku niewystarczającego spełnienia jednej z nich. Próg niezłożoność–złożoność stanowi więc część ram behawioralnych łączących przeanalizowane powyżej komponenty złożoności i dlatego sam ulega endogenizacji.

## Bibliografia


Amalberti R. (1996). *La conduite de systèmes à risques.* Paris: Presses Universitaires de France.

Amalberti R. (1997). *Notions de sécurité écologique: le contrôle du risque par l'individu et l'analyse des menaces qui pèsent sur ce contrôle. Approche psycho-ergonomique*. Monographie du Séminaire du Programme Risques Collectifs et Situations de Crise. Paris: CNRS, listopad.

Amalberti R. (1999). „Les effets pervers de l'ultrasécurité", *La Recherche*, nr 319, s. 66–70.

Amalberti R. (2001). „The paradoxes of almost totally safe transportation systems", *Safety Science*, nr 37, 2–3, s. 109–126.

Bainbridge L. (1987). „Ironies of automation", w: J. Rasmussen, K. Duncan, J. Leplat (red.), *New Technology and Human Error*. Chichester: Wiley, s. 271–283.

Billings C. (1997). *Human Centred Aviation Automation*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Commission of the European Communities (CEC) (2000). *Communication on the Precautionary Principle*. Brussels: COM 1, luty.

Durand N., Alliot J.-M. (1999). „Peut-on supprimer le contrôle au sol?", *La Recherche*, s. 319, kwiecień, s. 57–61.

Fischhoff B. (1975). „Hindsight ≠ foresight: The effect of outcome knowledge on judgment under uncertainty", *Journal of Experimental Psychology: Human Cognition and Performance*, nr 1, 3, s. 288–299.

Fischhoff B., Lichtenstein S., Slovic P., Derby S., Keeney R. (1981 [1999]). *Acceptable Risk* (wyd. 2). Cambridge: Cambridge University Press.

Hollnagel E. (2004). *Barriers and Accident Prevention*. Aldershot: Ashgate.

Paté-Cornell M.E. (1993). „Learning from the Piper Alpha Accident: A postmortem analysis of technical and organizational factors", *Risk Analysis*, nr 13, 2, s. 215–232.

Perrow C. (1999a). *Normal Accidents. Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.

Perrow C. (1999b). *Organisations à hauts risques et „normal accidents"*. Monographie du Séminaire du Programme Risques Collectifs et Situations de Crise. Paris: CNRS, czerwiec.

Rasmussen J. (1997). „Risk management in a dynamic society: A modelling problem", *Safety Science*, nr 27, 2/3, s. 183–213.

Rasmussen J., Jensen A. (1974). „Mental procedures in real life tasks. A case study of electronic troubleshooting", *Ergonomics*, nr 17, s. 293–307.

Rasmussen J., Svedung I. (2000). *Proactive Risk Management in a Dynamic Society*. Karlstad, Sweden: Swedish Rescue Services Agency.

Reason J. (1993). *L'erreur humaine*. Paris: Presses Universitaires de France.

Reason J. (1998). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.

Science et Vie (2000). „Tokaimura: accident impossible en France?", *Science et Vie*, styczeń, s. 102–109.

Triendl R. (1999). „Les déboires du plutonium japonais", *La Recherche*, nr 319, s. 30–32.

Vaughan D. (1996). *The Challenger Launch Decision, Risky Technology, Culture and Deviance at NASA*. Chicago, IL: University of Chicago Press.

Vickers G. (1995). *The Art of Judgment, A Study of Policy Making*. London: Sage.

Villiers J. (1998). „Le mur de l'automatisation", w: Académie Nationale de l'Air et de l'Espace (red.), *La relation homme-machine dans l'aéronautique.* Toulouse: Teknea, s. 205–237.

# Irreducibility Endogenised

The author of the present work, which constitutes an excerpt from his book Deep Complexity and the Social Sciences. Experience, Modelling and Operationality, offers a detailed analysis of an intrinsic irreducibility of risk of accidents in complex systems. Drawing on the works of authors such as Charles Perrow, he argues that the fundamental reason behind such events is the unpredictability of interactions between individual components of these systems. He goes on to outline the concept of defences-in-depth and criticises it on the grounds of the ever-growing distance between operators and the systems that they are supposed to supervise, and the occurrence of the so-called latent problems. The selected fragment of the book concludes with a presentation of different points of view on the subject of defining socially acceptable levels of risk and its optimisation with reference to the theoretical model of compromise between risk and performance proposed by James Reason, along with a discussion of the practical application of the precautionary principle.

Key words: complex systems, latent problems, acceptable level of risk, risk optimisation, precautionary principle.