

Bezpieczeństwo systemów

Konwersatorium 1

Jarosław Szkoła

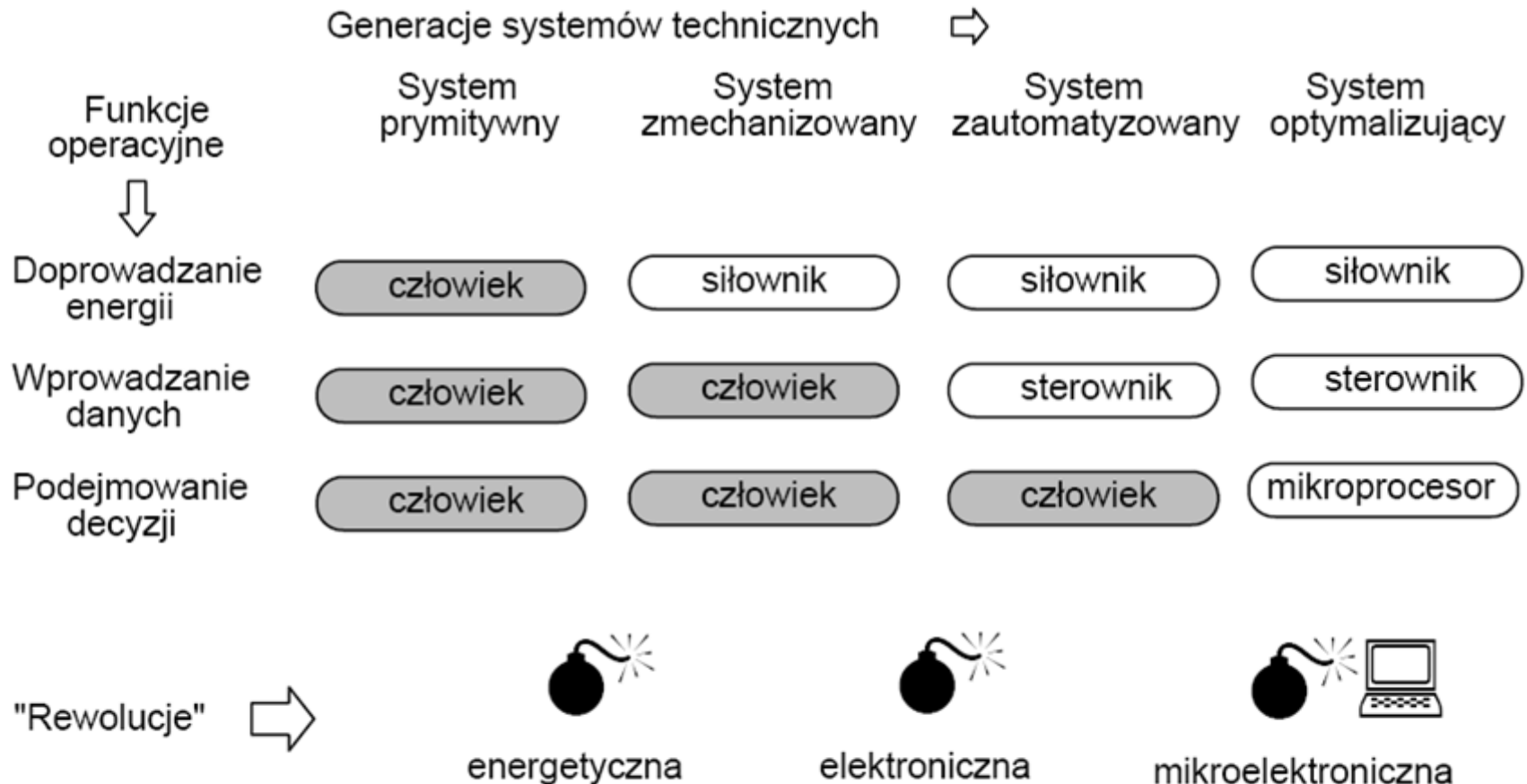
Powstawanie układów mechatronicznych

- produkty oparte na czysto mechanicznej zasadzie działania
- pojawianie się produktów, w których występują układy elektroniczne, ale nie mają wpływu na podstawowe działanie produktu
 - samochód → radio, wyświetlacze elektroniczne, sterowniki klimatyzacji
 - samolot → radio, radar, wspomaganie, nawigacja

Powstawanie układów mechatronicznych

- pojawianie się produktów w których układy elektroniczne są ściśle połączone z realizowaniem podstawowych zadań
 - samochód -> elektroniczny zapłon
 - obrabiarka numeryczna -> sterownik
 - robot -> sterownik

Rozwój systemów technicznych



Rozwój elektroniki

- 1943-46 – komputer ENIAC
- 1947 – tranzystor - Bell Telephone Lab.
- 1961 – manipulator UNIAMTE w Ewing Township (GM)
- 1969 – sterowniki PLC w GM
- 1971 – mikroprocesor 4004
- 1976 – video VHS – JVC
- 1982 – płyty CD
- 1997 – płyty DVD
- 2002 – płyty BlueRay (2008) – HD-DVD
- 2006 – TV HD w Polsce – platforma N
- 2012 – naziemna TV cyfrowa DVB (mpeg4)
- 2018 – kart graficzne Nvidia RTX – Ray Tracing i uczenie maszynowe

Rozwój mikroprocesorów Intela

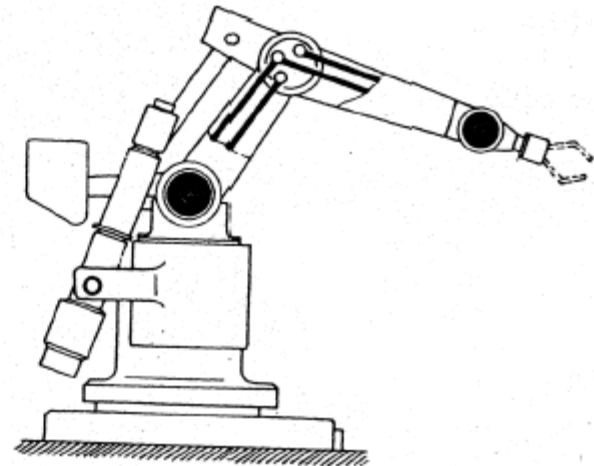
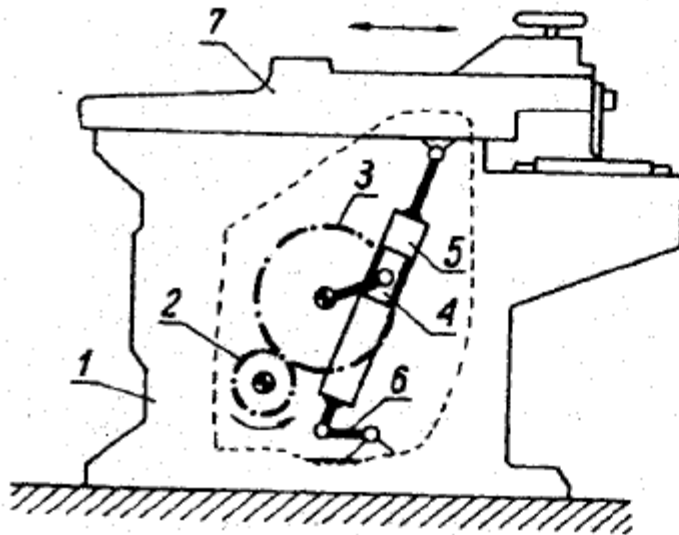
- 1971 – intel 4004 (4 bitowy do kalkulatorów)
- 1972 – intel 8008 (8 bitowy)
- 1974 – intel 8080 (8 bitowy)
- 1978 – intel 8088/8086 (16 bitowy) – IBM PC
- 1982 – intel 80286 – IBM PC AT
- 1985 – intel 386 (32 bitowy)
- 1989 – intel 486
- 1993 – intel Pentium
- 1997 – intel Pentium II
- 1999 – intel Pentium III
- 2000 - intel Pentium 4
- 2002 - intel Dual Core
- 2023/24 - AMD Ryzen Threadripper z 96 rdzeniami

Początki mechatroniki

- Charakterystyka produktów uzyskanych na drodze projektowania mechatronicznego:
 - podstawowe funkcje można zrealizować tylko przez współdziałanie komponentów mechanicznych, elektronicznych i informatycznych,
 - występuje w tych układach przemieszczenie funkcji z mechaniki w kierunku, elektroniki i przetwarzania informacji,
 - właściwości takich produktów są w dużej mierze określone przez elementy niematerialne (oprogramowanie)

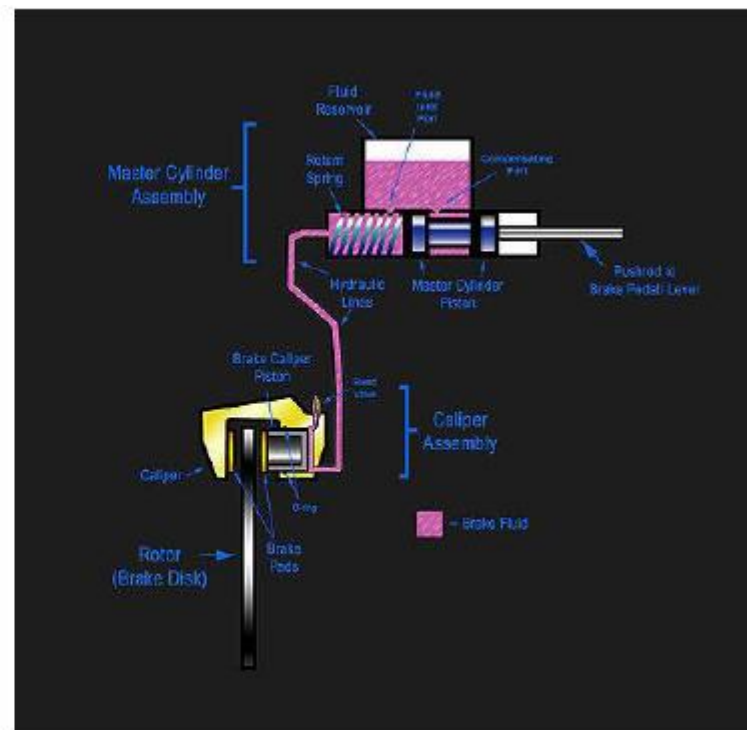
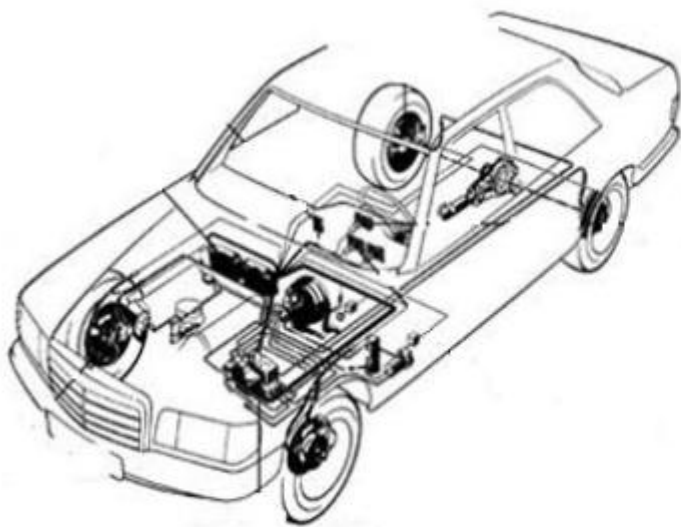
Mechatronika - przykłady

Układ mechaniczny i mechatroniczny



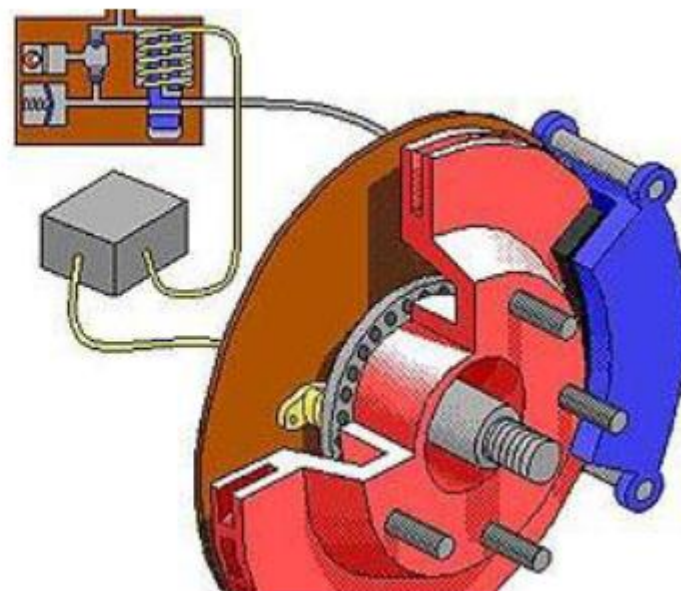
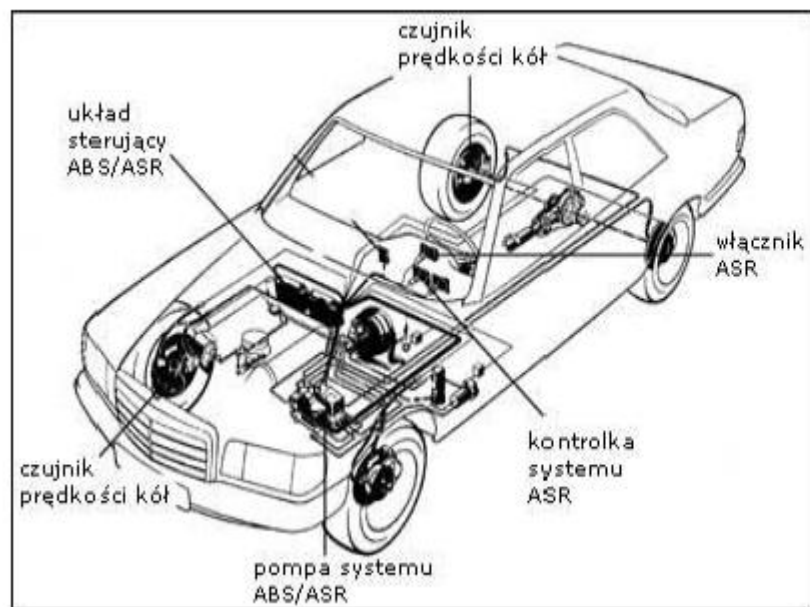
Mechatronika - przykłady

Samochód – mechaniczny układ hamulcowy



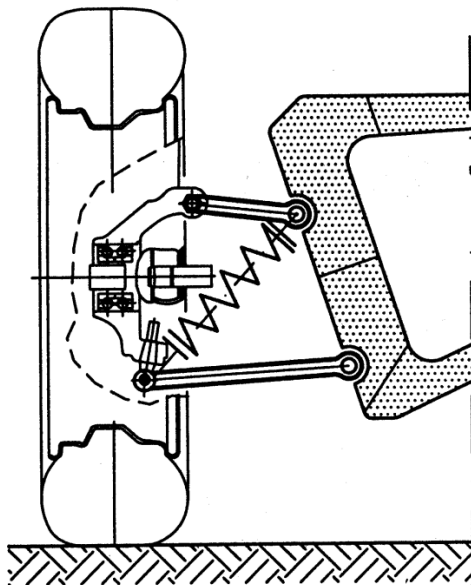
Mechatronika - przykłady

Samochód układy hamulcowe – ABS, ASR, ESP



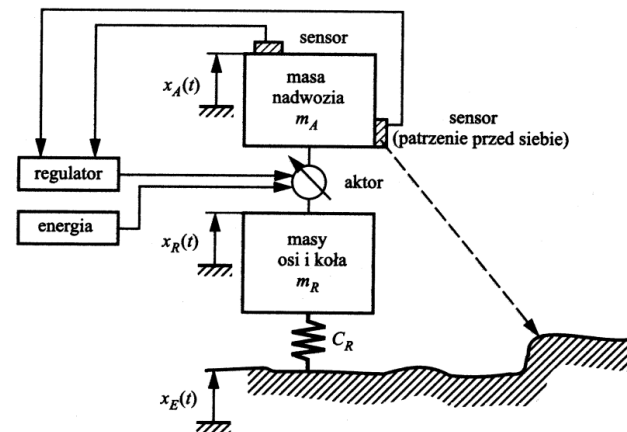
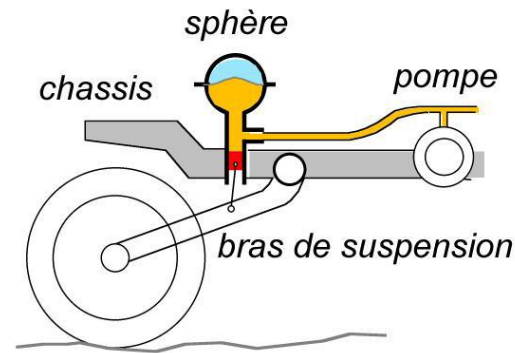
Mechatronika - przykłady

Samochód zawieszenia koła klasyczne



Schemat ideowy układu zawieszenia samochodu

Samochód zawieszenia aktywne



Zasada aktywnego zawieszenia dla „ćwiartki pojazdu”

Mechatronika - przykłady

Waga – klasyczna i elektroniczna



Powstawanie mechatroniki

- Przyczyny rozwoju mechatroniki:
 - zastosowanie układów półprzewodnikowych (tranzystory, diody...) zamiast układów lampowych,
 - opracowanie i rozwój układów scalonych,



Powstawanie mechatroniki

Przyczyny rozwoju mechatroniki cd.:

- rozwój i zastosowanie w przetwarzaniu sygnałów technik cyfrowych,
- powstanie układów programowalnych,
- powstanie i rozwój technik mikroprocesorowych

Powstawanie mechatroniki

- 1969 – pojęcie MECHATRONICS zostało zdefiniowane przez firmę Yasakwa Electric Corporation
- 1971 – 1982 - chronione jako nazwa handlowa
- 1982 – dostępne dla wszystkich
- 1987 – mechanotronika – pierwsza polska próba definicji
- **MECHAnika+elekTRONIKA**
- 1995 – przyjęcie oficjalnej definicji Komisji Unii Europejskiej
- 2006/7 – utworzenie kierunku studiów mechatronika

Mechatronika - definicje

1. Integracja naturalnie różnych systemów konstrukcyjnych: mechanizmów, obwodów elektrycznych i oprogramowania. Ta konieczność integracji jest jasno widoczna w robotach. [ISHII 1983]
2. Zastosowanie mikroelektroniki w inżynierii mechanicznej. [Oryginalna definicja Japońskiego Ministerstwa Przemysłu i Handlu (MITI)]
3. System, w którym rozwinięty ruch i rozwinięte sterowanie łączone są systematycznie w celu otrzymania systemu o wysokiej wartości, który może wykonywać rozwinięte funkcje zamierzone. [KAJITANI 1986]
4. Interdyscyplinarny obszar nauk inżynierskich, który wspiera się na klasycznych dyscyplinach budowy maszyn, elektrotechniki i informatyki. Typowy system mechatroniczny odbiera sygnały, przetwarza je i wydaje sygnały, które z kolei przetwarza np. w siły i ruchy. [SCHWEITZER 1989]
5. Programowalne urządzenia i systemy mechaniczne z sensoryką, aktoryką i komunikacją. [HANSON 1994]

Mechatronika - definicje

6. Synergiczna integracja inżynierii mechanicznej z elektroniką i inteligentnym sterowaniem komputerowym w projektowaniu i wytwarzaniu produktów i procesów. [komisja Wspólnoty Europejskiej, wg KING 1995]
7. Projektowanie i wytwarzanie produktów i systemów wykazujących zarówno funkcjonalność mechaniczną jak i zintegrowane sterowanie algorytmiczne. [HEWIT 1995, KING 1995]
8. Projektowanie maszyn inteligentnych. [HEWIT 1995]

Mechatronika - definicje

- **Mechatronika jest interdyscyplinarna i obejmuje następujące dziedziny:**
 - mechanikę (mechanikę techniczną, budowę maszyn, mechanikę precyzyjną)
 - elektronikę/elektrotechnikę (mikroelektronikę, elektronikę siłową, technikę pomiarów, aktorykę)
 - informatykę (teorie systemów, przetwarzanie informacji, przetwarzanie danych procesowych, sztuczną inteligencję)

Układ Mechatroniczny

Układ (system) mechatroniczny zbudowany jest z systemów częściowych:

- systemu podstawowego – mechanicznego
 - Aktory (siłowników),
 - sensorów,
 - układu sterowania (procesory i oprogramowanie).
-
- System mechatroniczny rejestruje sygnały (sensory), przetwarza je (układ sterowania) i wydaje sygnały, które przetwarza w siły i ruchy (aktory), które poprzez układ mechaniczny wpływają na realizowany proces techniczny.

Zastosowania urządzeń mechatronicznych

- zastępowanie konwencjonalnych urządzeń mechanicznych,
- •dołączanie elektronicznych urządzeń sterowniczych do maszyn konwencjonalnych,
- •tworzenie nowych rozwiązań układów mechatronicznych,

Mechatronika – obszar zastosowania

- produkty techniczne (zegarki, komputery, telefony, agd, rtv, samochody, samoloty, ...)
- urządzenie wytwórcze (obrabiarki numeryczne, roboty, systemy wytwórcze, systemy magazynowe,...)
- zespoły i elementy maszyn (sensory, silniki, elektryczne, elementy pomiarowe, wyświetlacze,...)

Powody stosowania Mechatroniki w maszynach

- Poszerzenie charakterystyk (konstrukcja mech. bez zmian – nowe sterowanie – lepsza wydajność, dokładność, szybkość, elastyczność, niezawodność – np. silnik samochodowy)
- Uproszczenie złożonych mechanizmów (modułowy układ mechatron. zastępuje kilka złożonych mechanizmów - np. obrabiarka numeryczna, maszyny offsetowe drukarskie,...)
- Inowacyjność (możliwość tworzenia układów, które bez elektroniki byłyby niemożliwe – układy analizy wizji, sztuczna inteligencja ...)

Wybrane aspekty bezpieczeństwa systemów mechatronicznych i informatycznych

- Podatność / odporność na występowanie zakłóceń w układach zasilania
- Podatność / odporność na ataki związane z protokołami komunikacyjnymi
- Podatność / odporność na przekroczenie dopuszczalnych parametrów pracy czujników i układów sterownia
- Występowanie luk bezpieczeństwa w oprogramowaniu systemowym (exploit)
- Znajomość / metody zabezpieczeń przed znanymi błędami lub słabymi punktami sprzętowych układów sterowania (sterowniki PLC / FPGA / Mikrokontrolery / Przetworniki A/D, D/A i inne)
- Odporność / podatność na celowe szkodliwe działania mające wywołać niepożądane zachowanie (np. przegrzewanie układów logiki sterowania, przekraczanie norm obciążenia siłowników, wprowadzanie zakłóceń w układach zasilania, itp.)

Luki bezpieczeństwa w układach mikroprocesorowych

- Podatność na atak typu Meltdown and Spectre procesorów Intel, AMD, ARM
 - Meltdown przełamuje najbardziej podstawową izolację pomiędzy aplikacjami użytkownika a systemem operacyjnym. Atak ten umożliwia programowi dostęp do pamięci, a tym samym do informacji dotyczących innych programów i systemu operacyjnego.

Luki bezpieczeństwa w układach mikroprocesorowych

- Podatność na atak typu Meltdown and Spectre procesorów Intel, AMD, ARM
 - Spectre przełamuje izolację pomiędzy różnymi aplikacjami. Pozwala atakującemu oszukać bezbłędne programy, które działają zgodnie z najlepszymi praktykami, w celu ujawnienia ich sekretów. W rzeczywistości kontrole bezpieczeństwa wspomnianych najlepszych praktyk zwiększają powierzchnię ataku i mogą sprawić, że aplikacje będą bardziej podatne na Spectre

Luki bezpieczeństwa w układach mikroprocesorowych

- Najnowsze procesory Intel, AMD z poprawioną architekturą są również podatne na ataki nowego typu - Spectre-BHB
- Problem dotyczy również architektury ARM, za sprawą ataku typu Spectre-BHB (CVE-2022-23960)

Jak się zabezpieczać przez exploitami

- Sprawdzać na bieżąco w ogólnie dostępnych bazach dane o podatności na ataki np.
- <https://www.exploit-db.com/>
- Korzystać z rozwiązań sprzętowych pozbawionych znany luk bezpieczeństwa
- Jeśli nie jest możliwa wymiana podatnego na ataki sprzętu – zastosować łatki bezpieczeństwa lub inne zabezpieczenia, minimalizujące ryzyko ataku (patche, firewalle, specjalne tryby pracy itp.)

Ataki na protokoły komunikacyjne i usługi sieciowe

Typy ataków:

1. Atak typu „odmowa usługi” (DoS).

Atak DoS przytłacza sieci, systemy lub usługi nadmiernym ruchem lub żądaniami, czyniąc je niedostępnymi dla legalnych użytkowników.

2. Atak typu man-in-the-middle (MitM).

Podczas ataku MitM napastnicy przechwytyują i podsłuchują komunikację sieciową między dwiema stronami, co pozwala im przechwycić poufne informacje lub manipulować przesyłanymi danymi.

3. IP Spoofing Attack

Atak polegający na fałszowaniu adresów IP. Podszywanie się pod adres IP to technika polegająca na tym, że osoba atakująca fałszuje źródłowy adres IP w pakiecie IP, aby sprawiał wrażenie, jakby pochodził z innego źródła niż rzeczywisty nadawca.

Ataki na protokoły komunikacyjne i usługi sieciowe

4. ARP Spoofing ARP

Atak polegający na fałszowaniu protokołu, znany również jako zatrucie pamięci podręcznej ARP, to atak, podczas którego osoba atakująca manipuluje protokołem rozpoznawania adresów (ARP) w celu przechwycenia lub manipulowania ruchem sieciowym.

5. Privilege Escalation Attack

Atak na eskalację uprawnień Ataki polegające na eskalacji uprawnień polegają na wykorzystaniu luk w zabezpieczeniach lub słabości systemu w celu uzyskania wyższego poziomu dostępu lub uprawnień niż pierwotnie przyznane, co zazwyczaj umożliwia atakującym wykonanie nieautoryzowanych działań lub uzyskanie dostępu do wrażliwych zasobów.

Najważniejsze rodzaje zakłóceń pochodzących z sieci zasilającej

- Zanik napięcia
- Chwilowe wahania amplitudy napięcia
- Udary napięciowe i przepięcia łączeniowe
- Długotrwałe obniżenie napięcia

Najważniejsze rodzaje zakłóceń pochodzących z sieci zasilającej

- Długotrwałe podwyższenie napięcia
- Szumy
- Zakłócenia impulsowe, wahania częstotliwości
- Odkształcenia harmoniczne

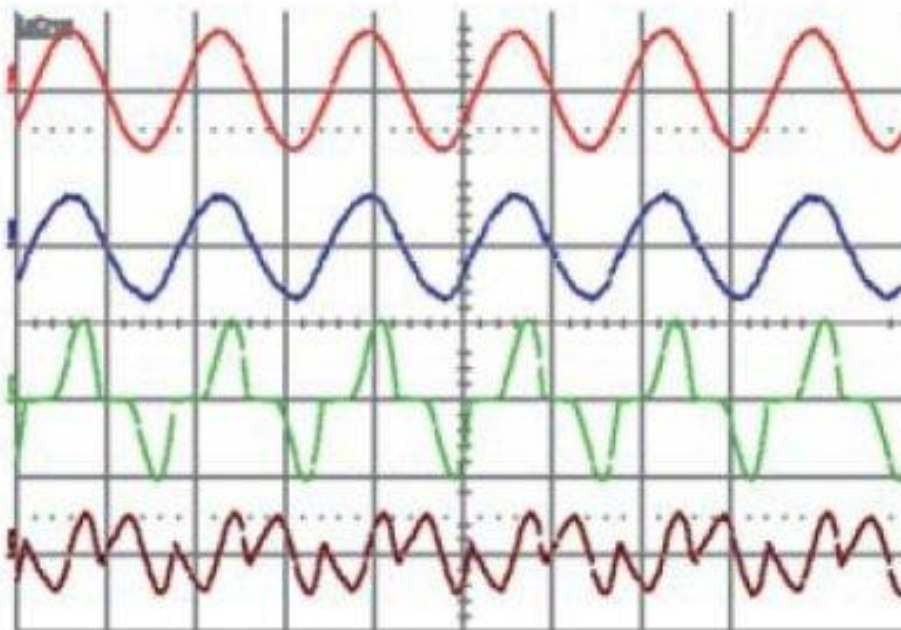
Przykładowy przebieg napięcia odkształconego

napięcie zasilające

prąd po stronie źródła zasilania
THDi=4.31%
DPF=1.0
PF=1.0

prąd pobierany przez obciążenie
THDi=51.89%
DPF=0.87
PF=0.77

prąd generowany przez aktywny
filtr harmonicznego (APF)



Współczynnik mocy a efektywność przekazywania energii

- Współczynnik mocy lub rzeczywisty współczynnik mocy (PF lub TPF) to wartość uwzględniająca obecność wyższych harmonicznych.
- W przypadku układów sinusoidalnych jest on równy współczynnikowi mocy przemieszczenia (DPF). Zatem DPF jest miarą przesunięcia fazowego pomiędzy podstawowymi składowymi napięcia i prądu.
- W przypadku obciążenia czysto rezystancyjnego (w układzie jednofazowym) moc pozorna jest równa mocy czynnej (wartościowo), a moc bierna równa zero, więc takie obciążenie w pełni wykorzystuje potencjał energetyczny źródła i współczynnik mocy wynosi 1.

Sposoby poprawy jakości układów zasilania

- Zastosowanie dedykowanych zasilaczy oraz falowników,
- Zastosowanie aktywnych układów korekty współczynnika mocy
 - Pasywne Passive PFC, PPFC
 - Niektóre zasilacze i ładowarki przenośne
 - Aktywne Active PFC, APFC
 - np. zasilacze komputerowe, przetwornice napięcia, falowniki),

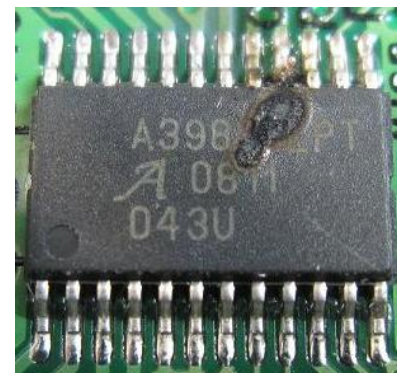
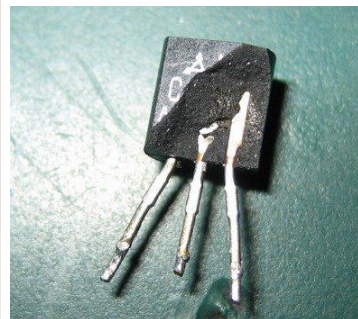
Zagrożenia bezpieczeństwa na poziomie oprogramowania

- Występowanie luk bezpieczeństwa w popularnych systemach operacyjnych Windows, Linux, MacOS, Android
- Występowanie błędów w bibliotekach programistycznych i kompilatorach
- Celowe wstrzykiwanie kodu lub podmiana zastosowanych bibliotek na specjalnie spreparowane wersje z tylnymi furtkami
- Niedoskonałość protokołów komunikacyjnych i ich podatność na manipulację (GSM, LTE, TCP/IP, RS232, IIC)

Zagrożenia dotyczące warstwy sprzętowej

- Obsługa urządzeń zewnętrznych niezgodnie z zaleceniami producenta
 - Przeciążanie urządzeń,
 - Sterowanie, zasilania odbiegające od zaleceń producenta
- Wprowadzanie własnych modyfikacji zmieniających charakterystykę urządzenia na inną niż zakładał producent
 - Zmiany mechaniczne
 - Zmiany elektryczne/elektroniczne

Przykładowe uszkodzenia urządzeń zewnętrznych



Dobre praktyki w zakresie użytkowania i projektowania systemów mechatronicznych i informatycznych

- Nie należy przekraczać maksymalnych parametrów pracy urządzeń, zgodnie z zaleceniami producenta,
- Dla projektowanych układów stosować przynajmniej 20% margines bezpieczeństwa w zakresie maksymalnych prądów, napięć, częstotliwości, mocy
- Dla projektowanych układów przewidywać wystąpienie sytuacji wyjątkowych, i odpowiednio na wystąpienie takich sytuacji wprowadzić zabezpieczenia,

Dziękuję za uwagę