PATENTOVÝ SPIS

(11) Číslo dokumentu:

308 855

(13) Druh dokumentu: **B6**

(51) Int. Cl.:

H03M 13/09 (2006.01)
H04L 1/00 (2006.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2018-270**
(22) Přihlášeno: **06.06.2018**
(40) Zveřejněno: **18.12.2019**
(Věstník č. 51/2019)
(47) Uděleno: **02.06.2021**
(24) Oznámení o udělení ve věstníku: **14.07.2021**
(Věstník č. 28/2021)

(56) Relevantní dokumenty:
US 2008168323 A; US 2008244361 A; US 2011154159 A; US 9312883 B.

(73) Majitel patentu:
CESNET, zájmové sdružení právnických osob, Praha 6, Dejvice, CZ

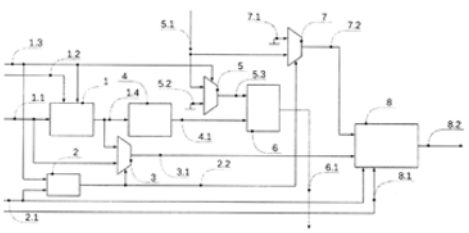
(72) Původce:
Ing. Lukáš Kekely, Ph.D., Praha 6, Dejvice, CZ
Ing. Jakub Cabal, Praha 6, Dejvice, CZ

(74) Zástupce:
Ing. Václav Kratochvíl, Husníkova 2086/22, 158 00 Praha 5, Stodůlky

(54) Název vynálezu:

Zapojení pro rychlý výpočet kontrolního součtu CRC obvodem připojeným přímo ke sběrnici pro přenos datových paketů

(57) Anotace:
Vynález se týká zapojení pro rychlý výpočet kontrolního součtu CRC (Cyclic Redundancy Check, tedy cyklický redundantní součet) obvodem připojeným přímo ke sběrnici pro přenos datových paketů. Hlavním přínosem navrhované architektury je umožnění efektivního výpočtu nezávislých CRC hodnot pro více paketů přenášených na sběrnici paralelně, tedy v jednom datovém slově nebo-li cyklu synchronizačního hodinového signálu. Architektura zapojení je flexibilní a podporuje zpracování obecných datových paketů libovolné variabilní délky, které nemusí být zarovnány na slova sběrnice. Architekturu zapojení je možné beze změny využít pro výpočet CRC součtů libovolné datové šířky popsané libovolným generujícím polynomem.



CZ 308855 B6

Zapojení pro rychlý výpočet kontrolního součtu CRC obvodem připojeným přímo ke sběrnici pro přenos datových paketů

Oblast techniky

Předkládané řešení se týká primárně zpracování datových paketů v počítačových sítích operujících na protokolu Ethernet, řešení je však možné využít i pro řadu jiných typů datových přenosů využívajících CRC pro zajištění integrity, např. vysoko-rychlostní paměti technologie HBM. Data jsou při přenosech náchylná na poškození zavedením náhodných bitových chyb, které je potřebné mít možnost před dalším zpracováním detekovat. Poškozená data pak musí být vyloučena ze zpracování, protože jejich význam – sémantika, mohl být zavedenými chybami výrazně změněn. Jedná se tedy o oblast datových přenosů, telekomunikační techniky a služeb.

Seznam zkratek:

CRC – cyclic redundancy check (cyklický redundantní součet)
FPGA – field-programmable gate array (programovatelná hradlová pole)
HBM – High Bandwidth Memory (vysokovýkonnostní paměť)
HMC – Hybrid Memory Cube

Dosavadní stav techniky

Na zajištění integrity přenášených datových paketů variabilní délky se před jejich odesláním spočítá hodnota kontrolního kódu CRC, který je následně připojen k datům a přenesen společně s nimi. Po přenesení paketů a jejich přijmu druhou komunikující stranou je CRC nad daty spočítáno znovu. Vypočtená hodnota je pak porovnaná na shodu s tou vloženou v paketu od vysílací strany. V případě shody hodnot CRC jsou přijatá data bez poškození, naopak neshoda hodnot poukazuje na zavedení nechtěných změn a nekorektnost přijatých dat. Hodnota CRC musí být vypočtena pro každý jednotlivý paket (transakci) komunikace nezávisle, jen na základě jemu patřících dat.

Současná řešení umí realizovat základní výpočet CRC nad daty na relativně vysokých teoretických rychlostech. Jejich hlavním nedostatkem je však chybějící podpora paralelního výpočtu několika hodnot pro více nezávislých paketů přenášených najednou, tj. v jednom slově datové sběrnice. To výrazně omezuje jejich reálně dosažitelnou propustnost zejména na krátkých paketech. Řešení, týkající se částečně dané problematiky jsou popsána například v patentových spisech US 2008168323, US 2008244361, US 2011154159 a US 9312883. Negativní dopad popsaného problému se neustále prohlubuje, protože s rostoucími přenosovými rychlostmi musí být slova datové sběrnice stále širší. Dosažitelná propustnost výpočtu CRC nad přenášenými pakety tak může výrazně omezovat celkovou přenosovou rychlost komunikace.

Podstata vynálezu

Výše uvedené nedostatky odstraňuje zapojení pro rychlý výpočet kontrolního součtu CRC obvodem připojeným přímo ke sběrnici pro přenos datových paketů podle předkládaného řešení. Jeho podstatou je, že datová sběrnice je svými výstupy zapojena k několika - celkově N, pod-obvodům pro výpočet CRC hodnot z přenášených paketů. Počet pod-obvodů je dán šířkou datové sběrnice, respektive maximálním možným počtem ukončených paketů v jednom slově této sběrnice. Každý pod-obvod zajišťuje výpočet CRC hodnoty z přidělené části datového slova a z mezi-výsledků získaných v předchozích pod-obvodech. Vnitřní zapojení každého pod-obvodu umožňuje korektní výpočet CRC při všech platných stavech přidělené části datového slova. V případě začátku paketu je na datový vstup aplikováno vymaskování dat před paketem. Pokud je současně přítomen i konec tohoto paketu, je pomocí multiplexoru vymaskovaný datový vstup

připojen k logice zajišťující výpočet CRC pro konec paketu. Jestliže, je přítomen konec dříve neukončeného paketu, výpočet CRC po konec paketu probíhá z neupraveného datového vstupu a z předchozích mezi-výsledků, výsledek CRC výpočtu je vyveden na výstup pod-obvodu. Pokud započatý paket není současně ukončen, je z vymaskovaných vstupních dat vypočten mezi-výsledek hodnoty CRC vyvedený na výstup pro následující pod-obvod. V případě, že přidělená část datového slova neobsahuje začátek ani konec žádného paketu, je z těchto neupravených vstupních dat vypočtena CRC hodnota a ta je následně akumulována s mezi-výsledkem z předchozích pod-obvodů, výsledek je opět vyveden na výstup pod-obvodu jako mezi-výsledek pro následující pod-obvody. Každý pod-obvod je řízen pouze pomocí řídicích signálů, které poskytuje vstupní datová sběrnice.

Ve výhodném provedení je uvedené zapojení vytvořeno uvnitř čipu technologie FPGA, který slouží k příjmu, zpracování a odesílání datových paketů na počítačové sítí Ethernet nebo vysokorychlostní paměti. Obvod je zpravidla přítomen ve dvou totožných a nezávislých instancích pro každý komunikační port - jedna instance pro vysílací stranu – vložení CRC do paketu a jedna instance pro přijímací stranu - kontrola správnosti CRC.

Výhodou zde předkládaného řešení je zachování velice vysoké rychlosti výpočtu CRC pro libovolné povolené délky přenášených paketů, tedy i pro nejkratší možné. Několik nezávislých hodnot CRC může být vypočteno v každém taktu pracovních hodin FPGA, protože výpočet je rozdělen mezi několik pod-obvodů, které umí pracovat společně na dlouhém paketu nebo nezávisle na několika krátkých. Další výhodou je možnost přizpůsobit strukturu obvodu parametrům konkrétní datové sběrnice i vlastnostem na ní přenášených paketů. Pod-obvody výpočtu CRC jsou zapojeny v pravidelné struktuře a mají jednotné rozhraní, proto změna celkové struktury obvodu není obtížná.

Objasnění výkresů

Podstata nového řešení je dále vysvětlena a popsána na základě připojených výkresů. Řešení je možné realizovat ve dvou provedeních - sériovém nebo paralelním. obr. 1 znázorňuje blokové schéma sériové varianty základního pod-obvodu pro výpočet CRC a obr. 2 pak znázorňuje sériové zapojení několika pod-obvodů do celkové architektury. Obr. 3 znázorňuje blokové schéma paralelní varianty realizace základního pod-obvodu a obr. 4 pak znázorňuje paralelní zapojení několika pod-obvodů do celkové architektury.

Příklady uskutečnění vynálezu

Předmětem nového řešení obecně jsou dvě varianty zapojení obvodu, který slouží k rychlému výpočtu cyklicky redundantního součtu (zkratka CRC) pro několik, maximálně N, datových paketů za jeden takt, které jsou přenášené na široké datové sběrnici. Celé zapojení obvodu je rozděleno do N pod-obvodů, na přiloženém obr. 1 je vyznačeno obvodové řešení sériové varianty jednoho pod-obvodu.

V zapojení podle obr. 1 je obvod 1, který upravuje vstupní slovo datové sběrnice o zvolené šířce R_w tak, aby výpočet CRC začal správně od začátku paketu, který může být umístěn na různých pozicích ve slově. Obvod 1 je opatřen datovým vstupem 1.1 připojeným přímo ke sběrnici pro přenos datových paketů, vstupem 1.2 určujícím pozicí začátku paketu, povolovacím vstupem 1.3 na určení přítomnosti platného začátek paketu v aktuálním datovém slově, a podle polohy začátku správně upraveným datovým výstupem 1.4. Úprava dat obvodem 1 ze vstupu 1.1 na výstup 1.4 zajišťuje nezávislost výpočtu CRC na datech přenášených sběrnicí v aktuálním slově před samotnými daty paketu. Jinak řečeno, jde o vymaskování dat před paketem.

Druhý obvod 2 rozhoduje o pokračování nebo dokončení výpočtu CRC pro paket v tomto slově. Druhý obvod 2 je opatřen povolovacím vstupem 1.3 určujícím polohu začátku paketu v aktuálním datovém slově, vstupním signálem 2.1 označujícím přítomnost konce paketu na datové sběrnici a výstupním signálem 2.2 na určení pokračování paketu z předchozího slova. Výstupní signál 2.2 je využíván k řízení multiplexoru 3, který slouží pro výběr neupraveného datového vstupu 1.1 pro pokračující paket z předešlého pod-obvodu - taktu hodin, nebo upraveného datového výstupu 1.4 pro konečný výpočet CRC jednoho paketu celého obsaženého v datovém vstupu 1.1. Základní obvod 4 pro výpočet CRC poskytuje na svém výstupu 4.1 vypočítané CRC z celého datového slova přivedeného vstupním signálem na datovém výstupu 1.4. Výpočet probíhá nezávisle na poloze či přítomnosti začátků nebo konců paketů, ošetření těchto situací řeší jiné části architektury, např. obvod 1 úpravou dat na datovém vstupu 1.1 na datový výstup 1.4. Druhý multiplexor 5 je řízen signálem přítomnosti začátku paketu - vstupním signálem na povolovacím vstupu 1.3, který vybírá mezi prvním vstupem 5.1 s průběžnou hodnotou CRC vypočtenou z předchozích dat pokračujícího paketu a druhým vstupem 5.2 s inicializační hodnotou CRC při začátku výpočtu pro zcela nový paket. Třetí obvod 6 slouží ke sloučení CRC hodnoty na výstupu 4.1 vypočítané z aktuálního datového slova a CRC hodnoty z prvního výstupu 5.3 druhého multiplexoru 5. Jeho výstupní signál na výstupu 6.1 poskytuje průběžný mezi-výsledek CRC od posledního začátku paketu, detekovaného v tomto pod-obvodě nebo v minulých, až po konec aktuálního datového slova. Třetí multiplexor 7 je řízen výstupním signálem 2.2, pokud je v aktuálním datovém slově pokračování ještě nedokončeného paketu, třetí multiplexor 7 vybere vstupní signál prvního vstupu 5.1 s mezi-výsledkem CRC pro předchozí data tohoto paketu, jinak vybere další vstupní signál 7.1 s inicializační CRC hodnotou. Další výstup 7.2 třetího multiplexoru 7 je připojen ke čtvrtému obvodu 8, který realizuje finální dopočtení CRC hodnoty pro paket, který končí v aktuálním datovém slově. Čtvrtý obvod 8 je dále opatřen dalším datovým vstupem 3.1, vstupním signálem 2.1, dalším vstupem 8.1 s pozicí konce paketu a dalším výstupem 8.2 poskytujícím finální výsledek výpočtu CRC pro zde končící datový paket.

V zapojení podle obr. 2 je zobrazeno zapojení N sériových pod-obvodů 9, které byly zobrazeny v obr. 1 a popsány výše. Každý pod-obvod 9 je opatřen vstupem 9.1 z datové sběrnice, jehož součástí jsou i řídicí signály o poloze/přítomnosti hranic paketů připojeny na vstup 1.2, povolovací vstup 1.3, datový výstup 1.4, vstupní signál 2.1, další vstup 8.1 a část datového slova o šířce R_w připojena na neupravený datový vstup 1.1. Datová šířka celého slova vstupní sběrnice tak je $D_w = N * R_w$. Dalším vstupem 9.2 připojeným na vstup 5.1 každého pod-obvodu 9 je mezi-výsledek CRC z předchozího pod-obvodu 9 v sekvenci. Výstup 9.3 připojený z výstupu 8.2 poskytuje vypočítané CRC pro paket končící v odpovídající části datového slova. Nakonec konečný výstup 9.4 připojený z výstupního signálu 6.1 poskytuje mezi-výsledek výpočtu CRC následujícímu pod-obvodu 9. V případě N-tého – posledního, pod-obvodu 9 je konečný výstup 9.4 připojen do registru 10, který jeho hodnotu uchová do následujícího hodinového taktu. Výstup registru 10 je pak přiveden na další vstup 9.2 prvního pod-obvodu 9, korektně tak může pokračovat výpočet pro další datové slovo sběrnice.

V zapojení podle obr. 3 je zobrazena paralelní varianta zapojení pod-obvodu z obr. 1. Většina zapojení součástí pod-obvodu zůstává beze změny. Avšak, na rozdíl od zapojení zobrazeného na obr. 1 je na výstup tohoto zapojení vyveden signál výstupu 4.1. Druhý multiplexor 5 je v tomto zapojení přítomen M-krát, kde M odpovídá pořadí zapojení pod-obvodu v celkové architektuře. Na první vstupy 5.1 druhého multiplexoru 5 jsou přivedeny vypočtené CRC hodnoty z jednotlivých předchozích datových slov. Všechny druhé vstupy 5.2 druhého multiplexoru 5 jsou zapojeny na inicializační CRC hodnotu. Každý z M druhých multiplexorů 5 je řízen odpovídajícím signálem 5.4, který určuje přítomnost začátku paketu v tom kterém datovém slově. M prvních výstupů 5.3 z druhých multiplexorů 5 je zapojeno do třetího obvodu 6, který v tomto zapojení slučuje všech M vypočtených CRC hodnot z předchozích datových slov a CRC vypočtené z aktuálního datového slova na výstupu 4.1. Třetí obvod 6 je opět opatřen výstupem 6.1, který je vyveden na výstup tohoto zapojení. Třetí multiplexor 7 je řízen výstupním signálem 2.2, pokud je v aktuálním datovém slově pokračování paketu z předchozího slova, třetí multiplexor 7 vybere vstupní signál 7.3 s mezi-výsledkem výpočtu hodnoty CRC z předchozího datového slova, který odpovídá signálu na

výstupu 6.1 z předchozího datového slova, jinak vybere další vstupní signál 7.1 s inicializační CRC hodnotu. Další výstupní signál 7.2 je opět připojen do čtvrtého obvodu 8, který realizuje finální výpočet CRC pro paket, který končí právě v aktuálním datovém slově.

V zapojení podle obr. 4 je zobrazeno zapojení N paralelních verzí pod-obvodů 19, které byly zobrazeny v obr. 3. Každý pod-obvod 19 je opatřen vstupem 19.1 z datové sběrnice, jehož součástí jsou řídicí signály o poloze/přítomnosti hranic paketů připojeny na vstup 1.2, povolovací vstup 1.3, vstupní signál 2.1, odpovídající signál 5.4, další vstup 8.1 a část datového slova o šířce R_w připojena na datový vstup 1.1. Propojení na datovou sběrnici a datová šířka celého slova tak zůstává stejná, mění se zde jen propojení a distribuce mezi-výsledků výpočtů CRC mezi jednotlivými pod-obvody 19. Další vstup 19.2 připojený z vstupního signálu 7.3 přivádí mezi-výsledky výpočtu CRC z dat od posledního začátku paketu, na rozdíl od sériové varianty pod-obvodu slouží tento mezi-výsledek pouze k výpočtu CRC pro paket končící v odpovídající části datového slova, které je poskytované výstupem 9.3 připojeným z výstupu 8.2 čtvrtého obvodu 8. Další výstup 19.4 připojený z výstupu 6.1 třetího obvodu 6 poskytuje tento mezi-výsledek výpočtu CRC následujícímu pod-obvodu 19. V případě N-tého, tj. posledního, pod-obvodu 19 je další výstup 19.4 připojen do druhého registru 20, který jeho hodnotu uchová do následujícího hodinového taktu. Výstup 20.1 druhého registru 20 je pak přiveden na další vstup 19.2 prvního pod-obvodu 19 a také do prvního z M vstupů 19.5 každého dalšího pod-obvodu 19, korektně tak může pokračovat výpočet pro další datové slovo sběrnice. Na rozdíl od sériové varianty obsahuje pod-obvod 19 ještě další výstup 19.6 připojený z výstupu 4.1 základního obvodu 4, který poskytuje mezi-výsledek výpočtu CRC pouze z odpovídající části datového slova. Každý další výstup 19.6 je pak připojen do jednoho z M vstupu 19.5 každého následujícího pod-obvodu 19.

Průmyslová využitelnost

Zapojení pro rychlý výpočet kontrolního součtu CRC obvodem připojeným přímo ke sběrnici pro přenos datových paketů podle uvedeného řešení je průmyslově využitelné v obvodech proudového či dávkového zpracování a kontroly dat rozdělených na menší nezávislé datové celky - pakety nebo transakce. Ve srovnání s běžně používanými řešeními umožňuje paralelní zpracování více těchto paketů v jednom hodinovém taktu - datovém slově sběrnice, čímž zvyšuje celkovou reálně dosažitelnou rychlost zpracování a kontroly dat i při velice širokých datových sběrnicích. Může být vytvořeno pro výpočet a kontrolu CRC hodnot datových paketů síťové komunikace jako je protokol Ethernet a obdobné a pro výpočet a kontrolu CRC hodnot pro potřeby komunikace s vysoko-rychlostními pamětmi, jako jsou technologie HBM, HMC a obdobné.

PATENTOVÉ NÁROKY

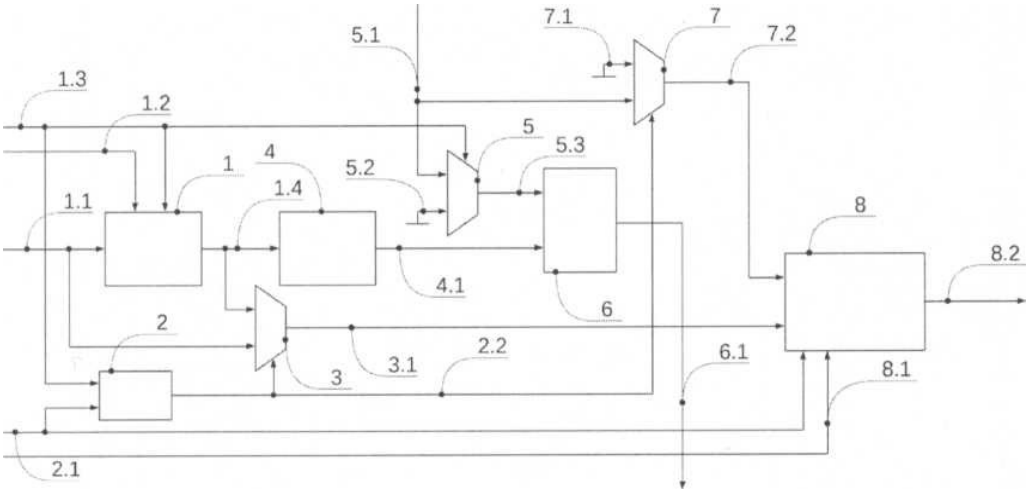
1. Zapojení pro rychlý výpočet kontrolního součtu CRC obvodem připojeným přímo ke sběrnici pro přenos datových paketů, **vyznačující se tím**, že obsahuje alespoň dva obvody (1) připojené k datovým a řídicím signálům vstupní sběrnice datovým vstupem (1.1), vstupem (1.2) určujícím pozicí začátku paketu, povolovacím vstupem (1.3), čtvrtý obvod (8) připojený k upravenému datovému signálu dalšího datového vstupu (3.1) a mezi-výsledku CRC na dalším vstupu (7.2) přes multiplexor (3) a třetí multiplexor (7) řízené výstupním signálem na výstupu (2.2) druhého obvodu (2) pro konce paketů a třetím obvodem (6) společně s druhými multiplexory (5) pro správnou agregaci a distribuci mezi-výsledků CRC výpočtů na výstupu (4.1), prvním vstupu (5.1), výstupu (6.1) na úrovni každého pod-obvodu (9, 19), pro dokončení výpočtu nezávislých CRC hodnot na výstupu (9.3, 19.3) pro až N datových paketů současně přítomných v jednom slově připojené sběrnice, přičemž datová sběrnice je propojena svými datovými výstupy s N pod-obvody (9, 19) pro výpočet CRC hodnoty pro dané části slova sběrnice na vstupu (9.1, 19.1), jejichž počet N je dán maximálním počtem přenášených paketů v jednom slově sběrnice a pro distribuci mezi-výsledků výpočtů CRC mezi jednotlivými pod-obvody (9) signály na dalším výstupu (9.2) a konečném výstupu (9.4) a přes registr (10) v sériové variantě zapojení a/nebo mezi pod-obvody (19) signály z dalšího vstupu (19.2), dalšího výstupu (19.4), M vstupu (19.5), dalšího výstupu (19.6) a přes druhý registr (20) v paralelní variantě zapojení pro zpracování jedné části slova datové sběrnice odděluje samotný základní výpočet CRC hodnoty bez ohledu na hranice datových paketů základního obvodu (4) od úpravy tohoto výpočtu pro vyřešení korektního chování pro pokračující, začínající nebo končící datové pakety.

2. Zapojení podle nároku 1, **vyznačující se tím**, že je vytvořeno uvnitř obvodu FPGA.

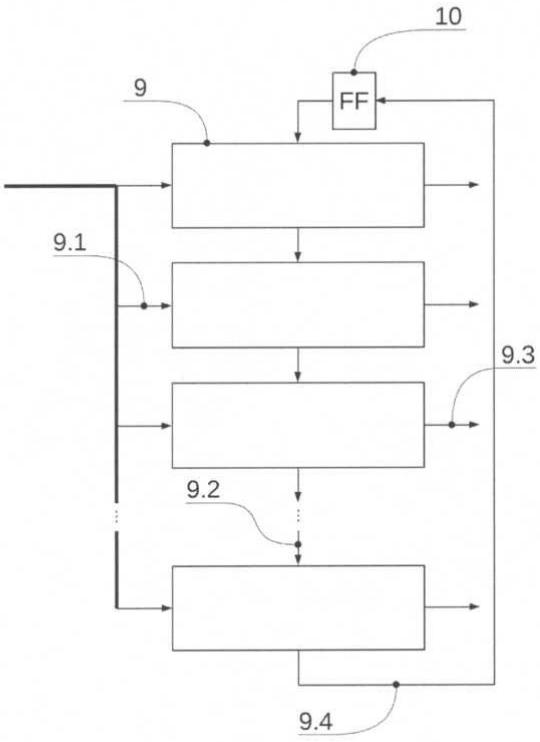
3. Zapojení podle nároku 1, **vyznačující se tím**, že je vytvořeno pro výpočet a kontrolu CRC hodnot datových paketů síťové komunikace.

4. Zapojení podle nároku 1, **vyznačující se tím**, že je vytvořeno pro výpočet a kontrolu CRC hodnot pro potřeby komunikace s vysoko-rychlostními pamětmi.

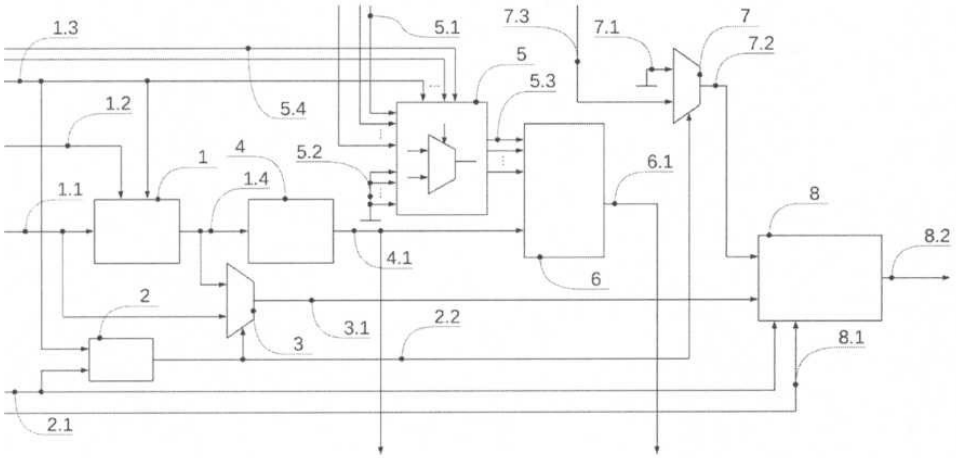
2 výkresy


5.1
7.1
7
7.2
1.3
1.2
5
5.3
1
4
5.2
1.1
1.4
8
8.2
4.1
6
2
2.2
3.1
3
6.1
8.1
2.1

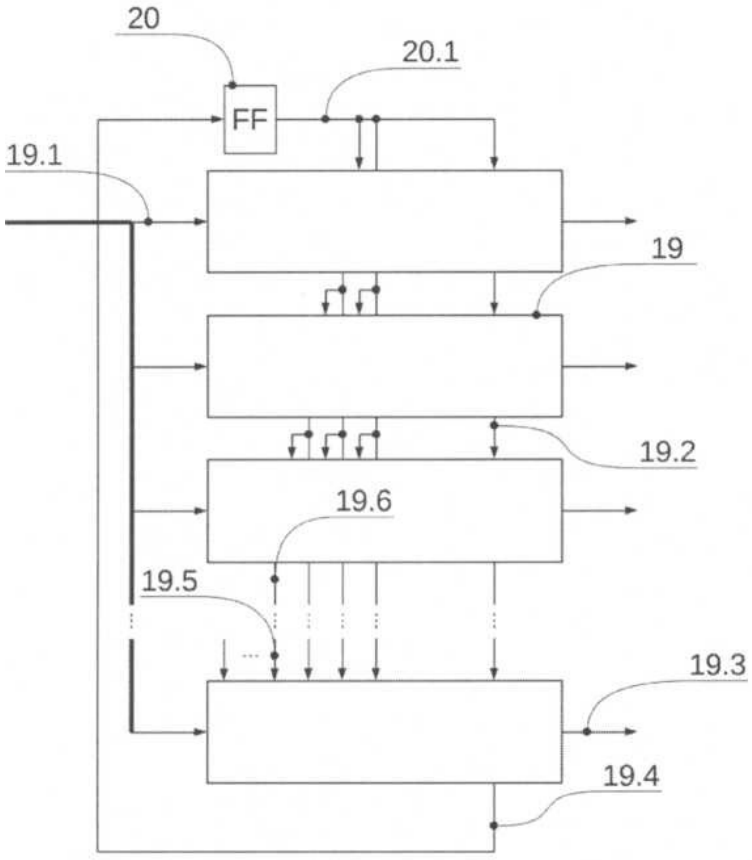
Obr. 1


10
FF
9
9.1
9.3
9.2
9.4

Obr. 2


1.3
5.1
7.3
7.1
7
7.2
5
5.3
1.2
5.4
1
4
5.2
6.1
1.1
1.4
8
8.2
4.1
6
2
3.1
2.2
3
8.1
2.1

Obr. 3


20
20.1
FF
19.1
19
19.2
19.6
19.5
19.3
19.4

Obr. 4