Státní závěrečné zkoušky	Akad. rok 2017/2018
Magisterský studijní program:	Inženýrská informatika
Obor:	Počítačové a komunikační systémy

Diagnostika a bezpečnost systémů

Předmět povinně volitelný

1. Metody a způsoby testování číslicových obvodů. Srovnání s metodami u analogových obvodů.
2. Modely poruch při testování číslicových obvodů. Základní skupiny modelů poruch a jejich charakteristika.
3. Strukturní testy, jejich princip a rozdíly ve srovnání s funkčním testem číslicového obvodu. Příklady metod pro odvození strukturních testů a jejich stručná charakteristika.
4. Princip analogové příznakové analýzy a příklady její aplikace při testování číslicových obvodů.
5. Charakteristika funkčních testů číslicových obvodů. Definiční princip Boolovské diference a způsoby jejího odvození.
6. Princip testování poruch pamětí. Možné zdroje poruch a chyb v typické obvodové struktuře pamětí. Rozdíl v testování pa¬mětí ROM a RAM.
7. Spolehlivostní blokové diagramy při hodnocení analytické spolehlivosti systému. Diskutujte možné konfigurace složek systému a vliv této konfigurace na výslednou spolehlivost systému.
8. Význam příznakové analýzy v číslicové technice, princip, základní struktura testovacího řetězce s příznakovým analyzátorem, diskuze o diagnostické spolehlivosti metody.
9. Popis architektury součástek typu hradlová pole. Výhody, které přinášejí zákaznické obvody typu CPLD a FPGA při realizaci číslicových a zejména mikroprocesorových systémů.
10. Základní metodika návrhu číslicových systémů, při použití jazyka VHDL, jaké způsoby simulace modelů obvodů a systémů tato metodika přináší. Výhody použití knihovních buněk a IP (Intellectual Property) při opakovaném návrhu.
11. Popis úrovní abstrakce u modelů pro návrh číslicových obvodů a systémů. Souvislost výstavby hierarchického modelu VHDL s úrovněmi abstrakce popisu modelů. Příklad modelů kombinačních a sekvenčních obvodů a systémů.
12. Kroky návrhu číslicových systémů při dodržení zásad metody návrhu shora dolů (top – down design). Prostředky jazyka VHDL pro tuto metodu.
13. Způsob ověřování pomocí souborů „testbench“ generovaných simulačním prostředím pro verifikaci návrhu. Popis metodiky návrhu zdola nahoru (bottom–up design).
14. Kybernetická bezpečnost a řízení informační bezpečnosti v organizacích. Zákon o kybernetické bezpečnosti, prováděcí vyhlášky a předpisy, norma ISO 27000 (ISO 27001). GDPR.
15. Standard pro řízení a správu služeb ITIL. Rámec nejlepších praktik pro řízení informatiky (IT governance) COBIT.
16. Hašovací funkce, princip symetrické a asymetrické kryptografie, kvalifikované certifikáty, systémové certifikáty a digitální serverové certifikáty, elektronický podpis.
17. Archivace, zálohování a obnova dat, disková pole RAID (1,0,10,5,6). Datové úložiště NAS, konfigurace a využití.
18. Penetrační testování, útoky na počítačové systémy a mobilní technologie. Bezpečnostní rizika virtualizace, hostingu a outsourcingu.

19. Správa identit a přístupů (IAM – Identity and Access Management). Řízení přístupů. Adresářové systémy. Provisioning. Architektura IAM řešení. Pokročilé technologie pro správu identit. Správa identit a přístupů v prostředí Internetu. Budoucnost digitálních identit.
20. Zabezpečení počítačových sítí pomocí firewallů. HW firewall, SW firewall – jednotlivé typy.