VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS INSTITUTAS

Formalių specifikacijų taikymas projektuojant paskirstytas sistemas

Applying Formal Specifications to Design Distributed Systems

Magistro baigiamasis darbas

Atliko:	Matas Savickis	(parašas)
Darbo vadovas:	Karolis Petrauskas, Doc., Dr.	(parašas)
Recenzentas:	Viačeslav Pozdniakov, Partn. Doc.	(parašas)

Vilnius – 2020

Santrauka

Akcijų ir kitų vertybinių popierių valdymo sistemomis naudojasi daugybė vartotojų ir finansinių institucijų. Šiuose sistemose kasdien yra atliekama daybybė finansinių tranzakcijų. Dėl didelės apkrovos tokių sistemų architektūroje dažniausiai būna taikomi pasiskirtį algoritmai. Tačiau kuriant tokias sistemas ad-hoc būdų lengva padaryti dizaino problemų, kurios išaiškėja tik paleidus sistemą. Klaidos tokio tipo paskirstytoje sistemoje gali reikšti klietų nepasitenkinimą ar net prarastus pinigus. Šiuo darbu sieksime atrasti sistemos klaidas Nasdaq daskirstytoje sistemoje taikydami formalias specifikacijas. Šiame darbe bus naudojama TLA+ formalaus specifikavimo kalba siekant aprašyti sistemą ar bent kai kurias jos dalis formaliais metodais. Darbe tikimasi įrodyti, kad pasirinktos Nasdaq sistemos yra sukurtos korektiškai, arba atrasti su specifikacija nesutinkančias programos dalis ir taip atrasti ir raportuoti klaidas Nasdaq komandai.

Raktiniai žodžiai: Nasdaq, TLA+, Formalios specifikacijos, Paskirstytos sistemos, akcijos

Summary

Equity and other securities management systems are used by many consumers and financial institutions. These systems contain daily waste financial transactions. Due to the high load in the architecture of such systems, separation algorithms are usually applied. However, in the development of such systems, ad-hoc techniques are easy to design, elucidated only at system startup. Errors in this type of distributed system can mean failing to reach customers or even losing money. He is currently working to detect system errors in the Nasdaq distributed system using formal specifications. This work will use the language of the TLA + formal specification, which needs to be described in the system or at least some part of it in a formal method. The paper is expected to prove that the selected Nasdaq systems are designed correctly, or to discover parts of the program that do not agree with the specification and thus to discover and report errors to the Nasdaq team.

TURINYS

Įvadas

Kuriant paskirstytas sistemas dažniausiai būna naudojama architekto arba programuotojo darbo patirtis ir gerosios praktikos. Tačiau net ir geriausia programuotojų komanda kurdama bet kokią sistema gali padaryti klaidų. Šios laidos dažniausiai atsiranda neteisingai užrašius sistemos specifikaciją arba neteisingai implementavus šią specifikaciją. Kai tokios sistemos yra ataskingos už finansus mes bandome siekti, kad mūsų kuriama sistema būtų kuo korektiškesnė ir su kuo mažiaus klaidų. Šio darbo tikslas bus specifikuoti Nasdaq paskirstytą sistemą naudojant TLA+ formalaus specifikavimo kalbą. Darbas yra aktualus nes Nasdaq sistema yra atsakinga už didelių finansinių tranzakcijų kiekį ir tačiau šioje sistemo yra klaidų, kurios atsiranda dėl neaiškių priežasčių. Kaip rodo Amazon praktika, taikant formalius metodus ir TLA+ formalios specifikacijos kalbą yra įmanomas surasti pasislėkusias problemas sistemoje. Šiame darbe bus išanalizuota Nasdaq paskirstyta sistema, identifikuoti sistemos komponentai kurie gali sukelti problemu. Probleminius komponentus specifikuosime TLA+ kalba ir specifikavimo metoda Lineage-driven fault injection. Darbu sieksime surasti paskirstytos sistemos problemas arba įrodyti, kad sistemos komponentai specifikuoti ir implementuoti korektiškai. Tikimasi, kad šis darbas pagerins Nasdaq sistemos veikimą ir atskleis kaikuriuos sistemos paternus kuriuos būtų galima taikyti kitose finansinėse sistemose šiuos paternus specifikuojant TLA+ kalba.

Rezultatai ir išvados

Santrumpos