CERTIFICATION AND QUALIFICATION OF TOOLS FOR CODE GENERATION IN AUTOMOTIVE INDUSTRY
СЕРТИФИЦИРАНОСТ И КВАЛИФИЦИРАНОСТ НА ПОМОЩНИ ПРОГРАМИ ЗА ГЕНЕРИРАНЕ НА КОД ЗА АВТОМОБИЛНАТА ИНДУСТРИЯ

Dipl. Eng. Nikolay Petev Brayanov
Маг. Инж. Николай Петев Браянов
Department of Microelectronics - Technical University of Sofia

Катедра Микроелектроника – Технически университет София

npb@ecad.tu-sofia.bg

Abstract: *After ISO 26262 was developed as a derivative of IEC 61508 used specially for automotive industry, all software tools used in automotive industry were required to be certified and qualified to assure their compatibility with this safety relevant standard. However the standard does not specify a particular method for tools assessment. It gives a rough frame which allows the each provider of tools to develop custom specification when implementing his solution. This paper identifies approaches, used by different tool suppliers to assure ISO 26262 requirements.*

The paper goes in deep in automotive safety standards, searching for milestones relevant to tools' certification. It describes basic requirement that tools should fulfil and the way it should be implemented and assured. Then behaviours of tools, that is not assessed by ISO 26262, but is part of overall software safety assessment is investigated. Finally the research review how it is implemented in some of the most distinguishable tools' providers – MatLab and IBM.

In conclusion, publication assess how commercial tools correspond to the needs of safety relevant industries and automotive in particular. It gives an answer of the question "Is using of certified and qualified tool enough to assure compliance with safety requirements?". It allocates the issues that are still opened.

Keywords: AUTOMOTIVE, SAFETY, CERTIFIED CODE GENERATION, TOOLS CERTIFICATION

1. Увод

Делът на софтуера в съвременната автомобилна индустрия постоянно нараства. Паралелно с повишения брой на изискванията към софтуера, нараства и желанието за намаляване на времето от начало на разработката до нейното пласиране на пазара и общите разходи. Един от подходите, предложен като отговор на тези нови нужди е автоматизираното генериране на код, а ползите от него са многобройни:

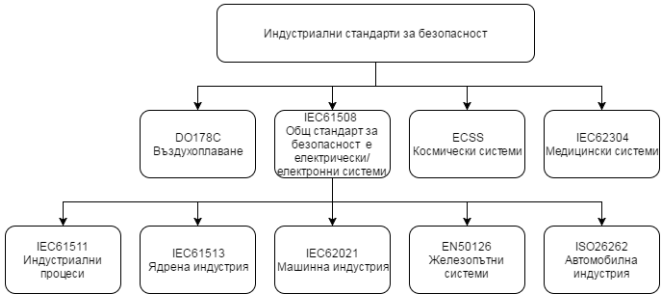
- Проследимост на изискванията в кода
- Консистентност и високо качество на генерирания код, съобразно правилата за безопасност на автомобилна индустрия
- Възможност за повторно използване
- Оптимизиране на цената
- Възможност за симулиране и често прототипиране

Основният проблем при разработки, в контекста на автомобилостроенето, е безопасността. Много нови функционалности - асистенция на водача, подпомагане на спирачната система, динамичен контрол на автомобила, въздушни възглавници и други активни и пасивни системи за сигурност са все по-обвързани с безопасността на автомобила. Разработването и интегрирането им води до нарастваща нужда от сигурен процес на системната разработка и необходимост от представяне на доказателства за изпълнението на целите за безопасност на системата. Това се постига чрез множество измервания, имплементирани в различни технологии и изпълнявани в различни етапи на разработката. В тази връзка възниква нуждата от квалифициране и сертифициране на помощните програми, използвани в индустриите с изисквания за безопасност.

В настоящия труд се разглеждат стандарта DO-178C използван във въздухоплаването, IEC61508 – главен стандарт за електрически и електронни системи и ISO26262, изработен на база IEC61508 и ориентиран към нуждите на автомобилостроенето. Разглежда се приложението на описаната методология, според практиката на два от най-големите доставчици на помощни програми за автомобилната индустрия, отчитайки преимуществата и недостатъците на методите и на приложението им съобразно стандарта. Разглеждат се алтернативни варианти за квалификация на вериги от помощни програми. В резултат се дава отговор на поставения въпрос и са анализирани преимуществата и недостатъците на стандарта от гледна точка сертификация и квалификация на помощи програми, както и възможностите за подобряването му.

2. Предпоставки и начини за разрешаване на проблема

Създадени са стандарти, описващи методите за разработване и оценка безопасността за индустриите, имащи отношение към безопасността(фиг. 1).



Фиг. 1 *Стандарти за индустриите с изисквания за безопасност*

Всеки стандарт за безопасност поставя различни критерии за квалификация и сертификация на помощните програми.

DO-178C ясно дефинира методите за квалифициране на помощни програми [1]. Стандартът разглежда квалифицирането като процес, необходим за достигане на нужното ниво на сертифициране на дадена помощна програма в контекста на конкретно въздухоплавателна система. DO-178C разделя помощните програми на такива за разработване и такива за проверка. Разликата между тях е отговора на въпроса „Резултата от изпълнението на помощната програма част ли е от въздухоплавателният софтуер?“. Ако отговора на въпроса е да, помощната програма следва да бъде сертифицирана като такава за разработване. В противен случай тя се класифицира като програма за проверка, което значително улеснява сертификацията и. Според стандарта, когато помощната програма се използва за разработване, процесът при които е разработена тя трябва да удовлетворява процеса, нужен за текущата разработка на софтуер за въздухоплаването. Нивото на безопасност на продуктовия код е еквивалентно на това на използваната помощна програма. Стандартът дава възможност

за доказване на по-високо ниво на надеждност, чрез прилагане на допълнителни проверки. При квалифицирането на помощна програма за проверка, нещата са доста опростени. Необходимо е да бъде доказано че помощната програма работи коректно в контекста на употребата и. На практика това може да бъде постигнато чрез документиране на методите и ограниченията на работа.

IEC61508 дава концепция за сертифицирана помощна програма и препоръчва употребата им при изработване на проекти с изисквания за гарантирано ниво на безопасност [2]. Предлага се помощните програми да бъдат сертифицирани чрез продължителни тестове и проверка на резултатите или, алтернативно, чрез нарастване на доверието в следствие на продължителна употреба. На практика, на процеса на сертифициране се гледа като на измерване, необходимо в случаите когато не може да бъде доказано голямо доверие породено от употреба. Поради тази причина формалното сертифициране се счита за ненужно и утежняващо. Стандарта препоръчва да се сертифицират вериги от помощни приложения.

IEC61508 разделя помощните програми на онлайн и офлайн. Като онлайн се определят помощни програми, които могат да укажат пряко влияние на вградените системи с изисквания за безопасност, докато офлайн помощните програми не могат. Офлайн програмите са типизирани:

- резултатите от тип T1 не участват по никакъв начин в изпълнимия код
- тип T2 са отговорни за проверката на дизайна или изпълнимия код(в такива случаи в резултат от изпълнението не може да бъде променена работата на изпълнимия софтуер, но е възможно да не бъдат открити грешки)
- резултатите от тип T3 могат директно или индиректно да участват в изпълнимия код на система с изисквания за ниво на безопасност.

На база тази класификация, автоматизираното генериране на код е тип T3 на офлайн помощните програми. Сертификацията на програма от тази категория, изисква доказателства че тя отговаря на спецификацията си и инструкциите за употреба.

Въпреки че ISO26262 се базира на IEC61508, те имат доста различни подходи към квалификацията на помощни програми. Според стандарта, за всяка използвана помощна програма следва да бъдат анализирани и документирани случаите на употреба[3]. Анализа следва да удостовери, дали грешка при изпълнението на помощната програма или случайно генериран резултат, би довел до нарушение на изискванията за безопасност. Въздействието на помощната програма(TI – tool impact), има две стойности: TI1 – грешката не оказва въздействие; TI2 – грешката въздейства. В допълнение следва да бъде оценена вероятността такъв тип грешки да бъдат открити и премахнати. На база на този анализ се установява нужното ниво на доверие на помощната програма(tool confidence level (TCL), Таблица 1).

Таблица 1: *Установява нужното ниво на доверие към помощната програма*

		Вероятност за откриване на грешките на помощната програма		
		TD1 голяма	TD2 средна	TD3 други
Въздействие на помощната програма	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

На база пресметнатия TCL и нивото на осигурена безопасност(Automotive Safety Integrity Level (ASIL)) се избира нужния метод са квалифициране на помощната програма(таблица 2).

Таблица 2: *Избор на методи за квалификация на помощна програма*

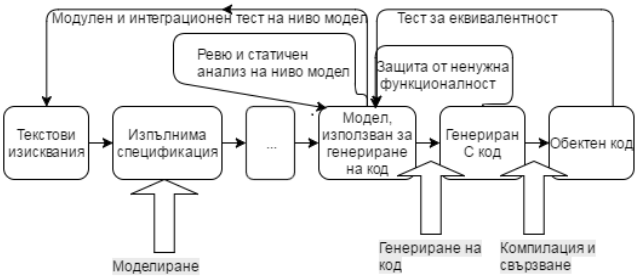
Методи	Препоръчани методи	
	за TCL2	за TCL3
1. Доверие, придобита от употреба	ASIL A, B и C	ASIL A и B
2. Проверка на процеса на разработване на помощната програма	ASIL A, B и C	ASIL A и B
3. Валидация на софтуера на помощната програма	ASIL D	ASIL C и D
4. Разработване на помощната програма според стандартите за безопасност за които се прилага	ASIL D	ASIL C и D

Метода „Доверие, придобито от употреба“ се възприема и от този стандарт. Както се вижда обаче, при по-голяма вероятност от неоткриваема грешка, той не е достатъчен.

3. Решение на проучения проблем

Публикацията [4] описва подхода, използван от MathWorks за квалифициране и сертифициране, чрез орган със сериозна акредитация в областта сертифициране/квалифициране на помощни програми - TÜV SÜD Automotive GmbH. За целта те използват вече създадените за IEC 61508 сертифициращи пакети и квалифициращите функционалности за DO-178C, които са били налични към този момент, както и подходите им за сертификация/квалификация.

Следващата фигура демонстрира процеса на проверка и валидация на модели и генериран код, създадени чрез „Simulink“ среда за моделиране и „Real-Time Workshop Embedded Coder“ генератор на С код.



Фиг.2: *Последователност на проверка и валидация реализирани за квалифициране на Simulink“ и „Real-Time Workshop Embedded Coder“*

Описаните проверки и валидация целят да откриват или предпазват резултата от грешки при изпълнение на помощните програми или други спонтанни такива. Според доклада за сертификация, прилагането на описания процес води до висока вероятност потенциалните грешни резултати на код генератора могат да бъдат открити или премахнати, т.е. TD1, което води до ниво на доверие към помощната програма TCL1. Според тази оценка генератора на код , приложен чрез този процес, е квалифициран и няма нужда от допълнителна квалификация и проверка.

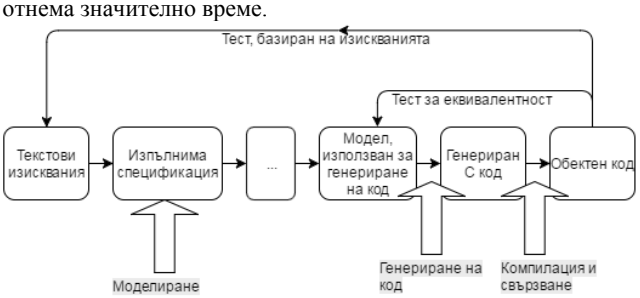
За да направят помощната програма гъвкава и приложима в нестандартни вериги от помощни програми, разработката предвижда и случаи в които вероятността за откриване на грешка е средна(TD2) и съответно е необходима ниво на доверие към помощната програма TCL2. В този случай е необходима допълнителна сертификация на база таблица 2. Помощната програма за проверка на C/C++ код „PolySpace“ също е класифицирана на ниво TCL2.

Приложени са методи за квалификация 2 и 3, с което се покриват всички нива на безопасност от ASIL A до ASIL D.

В допълнение се предлага „Пакет за Квалифициране на Помощни Програми“, който предоставя подход и бланки за квалифициране на вериги от помощни програми базирани на ISO/DIS 26262-8, както и независимата оценка на TÜV SÜD.

Описаният метод се опитва да предложи гъвкавост. Резултат от това е обемен и съответно бавен и скъп процес. Приложението му в малки проекти би било трудно, поради статичността му и нуждата от закупуване на допълнителен пакет за сертифициране.

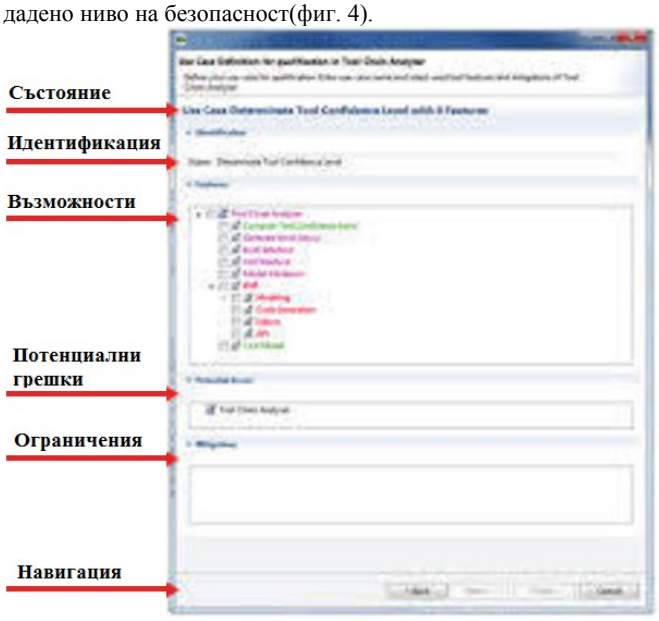
В публикация [5] се предлага сертифицирана и оптимизирана верига от помощни програми. Подобрението спрямо предходния метод е, че няма нарочна проверка на модела(фиг. 3). Според авторите, въпреки липсата на тази проверка в процеса, тя все пак се извършва косвено чрез проверка на резултата от автоматичната генерация на код, изпълнявайки тестове, базирани на изискванията. Недостатък на този тип проверка на ниво код е факта че в случай на грешка, анализа и трябва да бъде извършен на ниво код, а не на моделно ниво. След като проблема бъде идентифициран на ниво код, следва да бъдат направени релевантните промени на ниво модел, което евентуално ще коригира проблемите на ниво код. Един такъв подход не е никак рутинен, а и понякога отнема значително време.



Фиг. 3: *Последователност на проверка и валидация реализирани за квалифициране на IBM помощна програма, оптимизирана чрез премахване на проверките за модела*

В този случай опита на доставчиците за оптимизиране на процеса води до едно усложняване и необходимост от специфични умения. Все пак този метод е приемлив и може да бъде използван, макар и с не еднозначен резултат.

Други доставчици предлагат възможността потребителя сам да избере веригата от помощни програми, както и специфичните функционалности, които да използва[6]. В резултат от автоматичен анализ на риска, на потребите се предоставят избор от допълнителни тестове, които следва да бъдат извършени, за квалификацията на веригата спрямо дадено ниво на безопасност(фиг. 4).



Фиг.4:*TI предлага готова конфигурация за да улеснят клиентите си*

Решението е доста гъвкаво, просто и олекотяващо процеса. Като недостатък може да се посочи че такъв тип софтуери дават възможност за създаване на вериги, използвайки само един доставчик. Това ограничава избора, както поради причината че не дава възможност да се използва най-доброто предложение за всеки тип операции, така и заради потушаването на конкуренцията.

Алтернативата публикувана в [7] предлага моделно базирана помощна програма „Tool Chain Analyzer“, която може да оценява нестандартно изградени вериги от помощни програми. Недостатък в съчетаването на различни помощни програми е, че те трудно се синхронизират, защото имат различни интерфейси, а понякога се налага и добавяне на допълнителни проверки, което води до утежняване на процеса и допълнителна нужда от квалификация.

За последния проблем има решение в тази публикация [8]. Авторите предлагат метод за оптимизиране на броя на необходимите проверки. Според статията, приложението на метода успява да намали нужните помощните приложения, квалифицирани на ниво TCL3 от 7 до 0 и TCL2 от 4 на 1. В резултат от това те намаляват времето, необходимо за квалифициране на нужната верига от помощни програми с 50%, от 120 дни на 60. Резултатите са доста добри. За прилагане на метода обаче, се изискват някои специфични знания и умения.

4. Резултати и дискусия;

ISO26262 е един от най-добре дефинираните стандарти за безопасност. Той дава методология за оценка на помощните програми, използвани в автомобилната индустрия. Добре описани са подходите чрез които те могат да бъдат квалифицирани и сертифицирани. За разлика от други стандарти ISO26262 дефинира еднакви изисквания за квалификация за програмите за разработване и тези за валидация. Мнението ми е, че това е гаранция за процес, гарантиращ константно ниво на безопасност. Реално, статистически винаги има вероятност за допускане на грешка и много важно е проверката да се извършва с реципрочното ниво на достоверност. Изследването доказа, че е достатъчно да бъдат използвани сертифицирани и квалифицирани помощни програми за осигуряване на съвместимост с нормите на безопасност.

Този факт не е достатъчен за да убеди индустрията в смисъла от използването на автоматизирани методи за създаване на софтуерни приложения и конкретно автоматично генериране на код. Целта на всеки бизнес е да оптимизира процесите си с цел редуциране на разходите и осигуряване на нужното качество и безопасност на продукта. В този смисъл, и в контекста на съвременния текст на стандарта, използването на автоматизираните системи за генериране на код е спорно.

Основен недостатък е, че квалифицирането и сертифицирането на вериги от помощни програми са бавни, специфични и не на последно място скъпи процедури. Това ги прави нерентабилни за малки проекти и фирми. На база опита, мнението ми е, че това е голяма пречка за широкото разпространение на автоматизираните методи за генерация на код, което води до по-бърз, евтин, качествен и безопасен резултат. Изхождайки от позицията че този тип помощни програми са нужният инструмент за оптимизиране на разработките, считам, че е нужна оптимизацията на стандартите за безопасност, както следва:

- Квалификацията и сертификацията да бъдат извършвани върху веригите от помощни програми. Оптимално е квалификацията на помощни програми да бъде извършвана за всяка отделна верига, минимизирайки нужните проверки, според необходимото ниво на безопасност. Проучването установи, че квалифицирането на помощни програми в частност, е излишен процес, тъй като сертификацията на помощната програма сама по себе си не носи облекчения на процеса на сертифициране на веригата, който е задължителен. Следва да се извършват

промени в стандарта за безопасност в частта си за квалификация и сертификация на помощни програми, с цел премахване на сертифицирането на единични помощни програми и подробно дефиниране и улесняване на квалифицирането на вериги.

- Хармонизиране на подходите за оценка и квалификация, дефинирани в различните стандарти. Това ще доведе до концентриране на ресурси и обединена работа на доставчиците на помощни програми, работещи в различни индустрии с изисквания за безопасност.

В допълнение, в стандарта липсва обосновка на добри практики, които да бъдат използвани по време на оценката на нивото на доверие към помощната програма. При следваща редакция, е препоръчително да бъдат добавени такива, осигурявайки еднозначното тълкуване по време на процеса на оценка.

5. Заключение

В настоящия труд бяха разгледани стандартите за безопасност и методите по които те квалифицират и/или сертифицират помощни програми, и в частност тези за генериране на кода за вградени системи в автомобилната индустрия. Спряхме се подробно на ISO26262, който е един от най-добре дефинираните стандарти в това отношение. Той се отнася до системи с изисквания за безопасност в автомобилната индустрия и описва процеса при оценката на ниво на доверие към помощната програма(TCL), както и следващите стъпки за квалификация на помощната програма във връзка с нивото на осигурена безопасност(ASIL) необходимо на изгражданата система.

Разгледахме решенията на този проблем, предложени от два от най-големите доставчици на помощни програми MathWorks и IBM, анализирайки преимуществата и недостатъците им. Анализа показа, че подходите им са оптимални и отговарят на стандарта. Недостатък беше посочен в невъзможността за квалифицирано ползване на част от веригата.

Конкуренцията, в лицето на TI, предлага подход за динамично квалифициране, в които потребителя може да избере кои функционалности да използва, след което полуавтоматично да квалифицира така създадената верига. В този случай, обаче, е невъзможно създаването на верига от помощни програми, използвайки конкурентни доставчици.

Бяха разгледани и решения за квалифициране на верига, съставена от различни помощни програми, както и оптимизиране на такъв тип вериги, заявяващи доста добри резултати. Многостранната работа върху този проблем е доказателство за неговата важност и за това че все още той е неразрешен.

Обобщават се и се обсъждат резултатите, изхождайки от позицията, че помощните програми за автоматично генериране на код са част от решението за повишения брой на изискванията към софтуера, съвместно с нуждата от намаляване на времето от начало на разработката до нейното пласиране на пазара и общите разходи. В резултат от проучването, се обоснова извода, че използването на сертифицирана и квалифицирана помощна програма е достатъчно условие за осигуряване на съвместимост с нормите на безопасност. В допълнение беше достигнат извода, че стандартите, в текущата им форма, значително усложняват процеса на разработката. Възможен подход за справяне с този проблем е стандартите за безопасност да бъдат хомогенизирани, обединявайки доставчиците от различните индустрии с цел безопасност на продуктите им. От друга страна основен недостатък на стандарта е, че предлага подход насочен към квалифициране на помощните програми, а не към веригите. Опита показва че квалифицирането на помощни програми сами по себе си е ненужно. Поради тази причина се предлага промяна на стандарта, улесняване и задаване на насоки за квалифициране на вериги от помощни програми.

Изследването е извършено с финансовата подкрепата на НИС при ТУ - София по проект №162ПД0022-03 на тема "Изследване на възможностите за моделно базирана разработка на вграден код съгласно изискванията в автомобилната индустрия"

6. Литература.

[1] Software Considerations in Airborne Systems and Equipment Certification, DO-178C, RTCA Inc./EUROCAE, 2011

[2] Functional safety of E/E/PE safety-related systems, IEC 61508:2010, IEC.

[3] Road Vehicles – Functional safety– ISO26262:2011.

[4] Mirko Conrad, Patrick Munier, Frank Rauch Qualifying Software Tools According to ISO 26262

[5]IBM Rational Rhapsody Reference Workflow Guide Version 1.9

[6] Dr. Oscar Slotosch, Dr. Marcel Beemster Model-Based Tool Qualification of the TI C/C++ ARM® Compiler

[7] Oscar Slotosch Model-Based Tool Qualification The Roadmap of Eclipse towards Tool Qualification

[8] Oscar Slotosch, Martin Wildmoser, Jan Philipps, Reinhard Jeschull, Rafael Zalman ISO 26262 - Tool Chain Analysis Reduces Tool Qualification Costs