Schluss mit langen Freigabeprozessen

Effizienzpotentiale bei Safety und Security

Dr. Dominik Holling, ITK Engineering GmbH

Fahrzeugcomputer ermöglichen eine zeitnahe und flexible Aktualisierung der Software. So können neue vernetzte Funktionen in kürzerer Zeit als bisher auf den Markt kommen. Um dies zu erreichen, müssen nicht nur Entwicklungs-, sondern auch Unterstützungsprozesse beschleunigt werden. Besonders bei Safety- und Security-Freigabeprozessen ergeben sich Potentiale, da diese meist mit manuellem Aufwand in langen Zyklen verbunden sind. Durch eine frühzeitige Berücksichtigung von Freigabeaspekten während der Entwicklung und einer Automatisierung der Werkzeugkette in der Absicherung kann dieser Aufwand erheblich reduziert werden. Zudem weist die Absicherung von Safety und Security Potential für Synergien auf (z.B. in der Qualitätssicherung, bei Review- und Testergebnissen), die durch geschickte Prozessgestaltung zur Beherrschung der Komplexität genutzt werden können.

Um Funktionen schneller auf den Markt zum Kunden zu bringen, werden moderne Techniken des Software Engineering wie Continuous Integration (CI), Continuous Delivery (CD) und DevOps nicht nur im Bereich der IT-Systeme, sondern mittlerweile auch im Bereich des Systems Engineering eingesetzt [1]. Die Nutzung dieser Techniken für eingebettete bzw. cyber-physische Systeme ermöglicht dabei die kontinuierliche Auslieferbarkeit der Software, frühe Fehlererkennung und übergreifende Zusammenarbeit zur Beherrschung der gestiegenen Komplexität. Neben Engineering-Prozessen müssen auch die Unterstützungsprozesse angepasst werden, damit die Software bzw. das System fertig gestellt werden kann. Insbesondere die Freigabe und deren Dokumentation ist ein wichtiger Faktor, der ebenfalls an Komplexität gewinnt. Mit den nun kürzeren Release-Zyklen muss die Freigabe genauso getaktet mit der Auslieferung einer komplexen Software oder eines komplexen Systems erfolgen. Andernfalls hat der nachgelagerte Prozess keine Legitimierung zur Nutzung der bereitgestellten Artefakte. An dieser Stelle lassen sich Synergieeffekte aus den Bereichen der Safety und Security sowie Automatisierung der Dokumentationsgenerierung nutzen. Auf diesem Weg kann aus einem langwierigen, manuellen Prozess ein automatisierter und effektiver Prozess der Freigabedokumentation werden.

Freigabeprozess von Safety und Security

Die Freigabe von Software und Systeme erfolgt durch den Nachweis, dass der definierte Prozess entsprechend eingehalten und alle definierten Artefakte mit der angestrebten Qualität erstellt wurden. Damit wird die Einhaltung der Qualitätsziele sowie der regulatorischen Vorgaben, besonders aus den Bereichen Safety und Security, sichergestellt. Zusätzlich besitzt jede Freigabe einen Geltungsbereich, der sich auf Software(-teile) bzw. System(-teile) bezieht. Es können beispielsweise Freigaben für Softwarekomponenten bestehen, welche für die Integration benötigt werden, die daraufhin wieder eine Freigabe des Gesamtsystems nach sich zieht. Durch die hohe Anzahl an Auslieferungen in CI, CD und DevOps werden Freigaben für die gesamte Software oder auch nur Teile davon häufig benötigt und bieten durch ihre Komplexität die größten Potentiale zur Optimierung. Im Folgenden wird insbesondere auf zwei dieser Potentiale eingegangen: Synergieeffekte bei Freigabeaspekten aus den

Bereichen Security und Safety sowie bei der Erzeugung und Ablage der Freigabedokumentation.

Potential 1: Synergieeffekte der Freigabedokumentation
Verantwortlichkeiten für Safety und Security liegen typischerweise an verschiedenen Stellen der Organisation mit bedingter Möglichkeit des Austauschs. Dennoch ergeben sich Synergieeffekte der Freigabedokumentation aus gemeinsamen Aspekten, die für das Qualitätsmanagement, Safety und Security benötigt werden. Diese bestehen aus Metriken, welche die entsprechenden Prozesse bewerten und die Qualität der dazugehörigen Artefakte erfassen. Es ist auch möglich, Zusammenfassungen basierend auf Textbausteinen anhand des Werts einer Metrik zu erstellen. Dabei werden im Allgemeinen folgende Metriken erhoben bzw. Zusammenfassungen erstellt:

- Status der Anforderungen
- Status des Change- / Problem-Tickets
- Status der Verfolgbarkeit auf allen Ebenen
- Ergebnisse der Qualitätssicherung, Reviews und Tests

Zusätzlich existieren für die Bereiche Safety und Security jeweils Zusammenfassungen bzw. Metriken entlang der Safety bzw. Security Engineering-Prozessen für:

- Status der Risikoanalyse(n)
- Status der Konzept(e)
- Ergebnisse der Restrisikoanalyse(n) und Source-Code-Analyse(n)

Im Bereich Safety existieren u.a. zusätzlich Ergebnisse zur Toolqualifikation, die in die Freigabedokumentation einfließen. Für den Bereich Security werden zusätzlich u.a. die Ergebnisse des Penetration Testings berücksichtigt.

Potential 2: Automatisierung der Freigabedokumentation
Die Erstellung der Freigabedokumentation kann einen Flaschenhals darstellen, falls viele manuelle fehleranfällige Schritte benötigt wird. Hierdurch ist das Potential Automatisierung diese Aufgabe automatisch und zuverlässig durchzuführen. Benötigt werden dafür eine sorgfältige Planung bezüglich des Prozesses zur Erzeugung (1) und der Ablageorte (2) der Artefakte sowie die verwendeten Werkzeuge. Um das Potential maximal auszuschöpfen, sollte diese Planung vor Projektbeginn durchgeführt werden. Da die benötigten Informationen bei dieser Herangehensweise automatisiert erstellt und abgeholt werden, müssen die verschiedenen Werkzeuge in einer Toolchain automatisiert ineinandergreifen. Bei der Erzeugung der Artefakte hilft es, Techniken wie CI und CD so zu erweitern, dass Informationen automatisch erstellt und für die Dokumentation zur Verfügung zu gestellt werden. Dies kann zum Beispiel über eine automatische Erstellung der Problem-Tickets bei fehlgeschlagenen Tests oder automatischen Prüfungen der Verfolgbarkeit auf allen Ebenen bei der Softwareentwicklung erfolgen. Darüber hinaus ist es bei der Abholung von Artefakten sinnvoll, diese in einem umfassenden Anwendungsmanagement (ALM) zu speichern. Dieses zentralisiert die benötigten Informationen und erstellt mittels Berichtsfunktion die entsprechende Freigabedokumentation. Alternativ können beispielsweise auch Interoperabilitätsstandards verwendet werden [2], um die benötigten Informationen zu sammeln und zusammenzustellen. In der Praxis zeigt sich jedoch, dass diese Art der Zusammenstellung fehler- und wartungsanfällig ist. Allerdings lässt sie

sich zumeist nicht umgehen, da nicht alle Informationen in einem ALM-System abbildbar sind und so für gewöhnlich ein hybrider Ansatz aus ALM und Skripten für die Interoperabilität gewählt wird.

Abkürzungsverzeichnis

CI: Continuous Integration

CD: Continuous Delivery

ALM: Anwendungsmanagement

Literatur- und Quellenverzeichnis

[1] Pranav Ashar, Shifting Mindsets: Static Verification Transforms SoC Design at RT Level– https://www.eetimes.com/author.asp?section_id=36&doc_id=1325932
[2] Frédéric Loiret, Interoperability Specifications (IOS) v1 – http://www.crystal-artemis.eu/fileadmin/user_upload/Deliverables/CRYSTAL_D_601_021_v1.0.pdf

Autor

Dr. Dominik Holling arbeitet im Bereich Testmethodik und Entwicklungsprozesse bei der ITK Engineering GmbH. Sein Fokus liegt auf Software Engineering und Softwaretest. Dies beinhaltet das Zusammenbringen von Entwicklung und Qualitätssicherung sowie der frühen Aktivitäten des Requirements Engineering und der Software Architecture. Sein Hauptinteresse gilt dabei den Themen Continuous Integration, Continuous Delivery sowie SysDevOps für eingebettete / cyber-physische Steuergeräte. Holling studierte Informatik mit Fokus auf Security an der TU Kaiserslautern und hat an der Technischen Universität München am Lehrstuhl Software Engineering zum Thema wissensbasierte Testmethodik promoviert.

Kontakt

Internet: www.itk-engineering.de
Email: dominik.holling@itk-engineering.de