



Vore leverandører

Kontakt os

Nohau Danmark A/S



Om Nohau Danmark A/S

Nohau Danmark A/S er et datterselskab af det svenske Nohau Solutions AB.

Vi blev stiftet i 1991 og har dermed mere en 20 års erfaring med udviklingsværktøjer og processer til udvikling af embeddede løsninger.

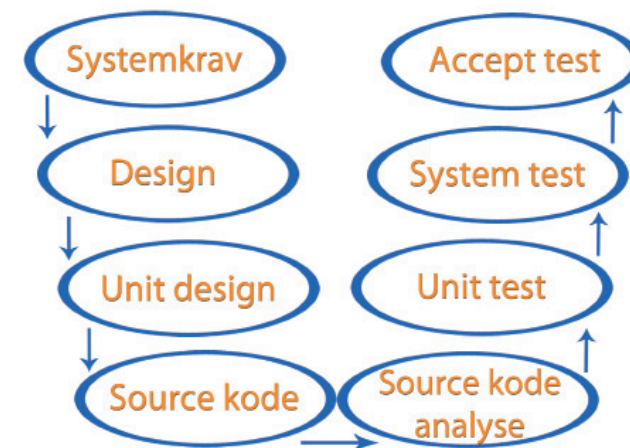
Derfor er vi godt rustet til at hjælpe med at finde løsninger, som sænker omkostningerne og øger produktiviteten i arbejdet med udvikling og test af embeddede løsninger. Det kan være ved opstart af et nyt projekt med fokus på hele processen fra specifikation til test eller blot ved tilpasning og optimering af den nuværende proces – hvad enten det drejer sig om en optimering af økonomien, udviklingstiden eller kvaliteten.

Nohau Danmark A/S
Hørkær 26, Plan 4
DK-2730 Herlev
Denmark

Phone: +45 44 52 16 50
Fax: +45 44 52 16 55

info@nohau.dk - www.nohau.dk

Safety & Security



NOHAU

Nohau tilbyder komplette løsninger

Vores ambitioner er, at hjælpe din organisation med at sænke omkostningerne og samtidig sikre den ønskede kvalitet til den fastsatte tid. Omkostningsoptimering er sjældent opnåelig samtidig med kvalitetsforbedringer og tidsmæssige optimeringer. Men ved et fornuftigt valg af værktøjer og proces, er det i de fleste situationer faktisk muligt, da automatisering kan øge effektiviteten ved samtidig sikring af kvaliteten.

Denne folder fokuserer på de af vores ydelser og produkter, som giver værdi ved udvikling af sikkerhedskritiske produkter med fare for personskaade ved fejl og som kan bidrage til beskyttelse mod Cyber Crimes.

Personal Safety og Security

Kvalitet indbygges i softwareapplikationer igennem specifikation. Vi skelner mellem Safety og Security, som begge på dansk betyder "sikkerhed".

Med Personal Safety mener vi de hensyn, der skal tages under udvikling, installation og brug af et produkt for at sikre, at ingen personer kan komme til skade, hvis et produkt fejler.

Med Security mener vi den robusthed et produkt eller et system skal have for at modstå angreb udefra. Der vil selvfølgelig være sammenfald, hvor en udnyttet Security svaghed, som f.eks. et buffer overflow, kan medføre fare for skader på mennesker også.

Der findes en lang række brancherelaterede standarder, som helt eller delvist kræves overholdt for, at et sikkerhedskritisk produkt kan certificeres. Nogle virksomheder har ikke krav om certificering, men benytter et godkendelsesstempel fra en certificerende myndighed som et kvalitetstegn og dermed som en konkurrenceparameter.

Det kan være meget uoverskueligt første gang et sikkerhedskritisk produkt skal udvikles. Det kan stille store krav til ændringer i udviklingsprocessen og til hvilke værktøjer, der med fordel kan anvendes. Standarderne beskriver oftest kun målene, men ikke hvordan de nås.

Nohau tilbyder derfor flere kurser, der sammen vores store udbud af værktøjer og middleware kan bidrage til, at lette udviklingsarbejdet og en eventuel certificeringsproces.

Kravhåndtering og design/modellering

I en certificeringsproces vil man altid blive mødt med kravet om - og dokumentation for - at funktionaliteten er valideret og verificeret. Det gælder ikke blot den primære funktionalitet, men også opførslen i kendte fejlsituationer. For at kunne teste dette, er man nødt til at have nogle krav og tænkte scenarier at teste op imod.

Nohau har flere produkter fra bl.a. Visure Solutions, Borland/Microfocus og IBM Rational til kravdefinition og -håndtering samt modellering og design. Sporbarhed fra krav til test er let at opretholde med de rigtige værktøjer.

Implementering og debugging

UML/SysML værktøjerne IBM Rational Rhapsody kan automatisk generere kode, som hermed altid er i fuld overensstemmelse med modellen.

Nohau forhandler en række af de førende compilere fra ARM, Keil og Tasking til de mest benyttede cpu-arkitekturer. Alle kommer med integreret udviklingsmiljø med mulighed for både kodeimplementering og debugging. De fleste kan leveres med Qualification Kit, der letter certificeringsprocessen markant.

Enkelte af compilerne kan endda leveres i en præ-certificeret udgave med long term maintenance. Dvs. ingen unødvendige opgraderinger og re-certificeringer.

Debuggerne fra Keil og Lauterbach kan i realtid lave code coverage analyse, hvorved kodedækningen under test kan dokumenteres.

PikeOS fra SysGo er et sikkerhedsgodkendt RTOS med tilhørende virtualiseringsplatform. Der kan således køre flere operativsystemer på samme CPU samtidig, og sikkerhedskritiske dele kan effektivt separeres fra mindre kritiske dele. SysGo har også certificerbare netværksstakke og filsystemer.



Statisk kodeanalyse

Unittest validerer de funktionelle krav. Med statisk kodeanalyse sikrer man, at applikationen bliver så robust, og dermed sikker, som mulig. Statisk kodeanalyse benyttes til at finde uventede fejl og farlige kodestrukturer, sikre overholdelse af kodningsregler, som f.eks. MISRA, HIC++, JSF m.fl. samt at finde security sårbarheder og arkitektur-problemer.

PRQA fra Programming Research er markedsledende med hensyn til regeltjek. CodeSonar fra Grammatech er et af de mest præcise bug-detection tools. Det er samtidig det lettest anvendelige. PC-Lint fra Gimpel Software er et kosteffektivt værktøj med lavere præcision.

Validering og test

Unittest-værktøjet CANTATA fra QA-Systems genererer automatisk testcases ud fra den C- eller C++ -kode, der skal testes. Kriterier for code coverage målinger sættes op, og parametre til og fra funktioner kan styres og kontrolleres. En komplet "Test Harness" med main rutine til afvikling af testcases på target eller host genereres - ligesom testrapporter til certificeringsformål - også automatisk.

Firewalls

For at beskytte embeddede applikationer og systemer mod Cyber Attacks, anbefales brug af statisk kodeanalyse for at mindske sårbarheden. Sikkerheden kan igen øges ved at indbygge embeddede firewalls i de enkelte enheder eller beskytte og segmentere installationer med dedikerede industrielle firewalls. En sådan firewall kender - til forskel fra almindelige IT-firewalls - til industrielle protokoller og busser.

Med produkterne fra Icon Labs' "Floodgate Security Framework" (Secure Boot, Secure Update, Firewall ...) er man altid sikker med netværksopkoblede enheder.

Kræves certificering kan man med Wurdtech's "Archilles" produkter få dokumenteret sikkerhed mod angreb.

Kurser

Nohau udbyder altid en lang række kurser indenfor safety og security onrødet. Se vores hjemmeside for aktuelle tilbud.