Fredrik Asplund
Risks Related to the Use of Software Tools when Developing Cyber-Physical Systems - A Critical Perspective on the Future of Developing Complex, Safety-Critical Systems

Abstract

The increasing complexity and size of modern Cyber-Physical Systems (CPS) has led to a sharp decline in productivity among CPS designers. Requirements on safety aggravate this problem further, both by being difficult to ensure and due to their high importance to the public.

Tools, or rather efforts to facilitate the automation of development processes, are a central ingredient in many of the proposed innovations to mitigate this problem. Even though the safety-related implications of introducing automation in development processes have not been extensively studied, it is known that automation has already had a large impact on operational systems. If tools are to play a part in mitigating the increase in safety-critical CPS complexity, then their actual impact on CPS development, and thereby the safety of the corresponding end products, must be sufficiently understood.

An survey of relevant research fields, such as *system safety*, *software engineering* and *tool integration*, is provided to facilitate the discussion on *safety-related implications of tool usage*. Based on the identification of industrial safety standards as an important source of information and considering that the risks posed by *separate* tools have been given considerable attention in the *transportation domain*, several high-profile safety standards in this domain have been surveyed. According to the surveyed standards, automation should primarily be evaluated on its reliable execution of separate process steps independent of human operators. Automation that only supports the actions of operators during CPS development is viewed as relatively inconsequential.

A *conceptual model* and a *reference model* have been created based on the surveyed research fields. The former defines the entities and relationships most relevant to safety-related risks associated with tool usage. The latter describes aspects of tool integration and how these relate to each other. By combining these models, a risk analysis could be performed and properties of tool chains which need to be ensured to mitigate risk identified. Ten such *safety-related characteristics of tool chains* are described.

These safety-related characteristics provide a systematic way to narrow down what to look for with regard to tool usage and risk. The hypothesis that a large set of factors related to tool usage may introduce risk could thus be tested through an empirical study, which identified safety-related weaknesses in support environments tied both to high and low levels of automation. The conclusion is that a broader perspective, which includes more factors related to tool usage than those considered by the surveyed standards, will be needed.

Three possible reasons to disregard such a broad perspective have been refuted, namely requirements on development processes enforced by the domain of CPS itself, certain characteristics of safety-critical CPS and the possibility to place trust in a proven, manual development process. After finding no strong reason to keep a narrow perspective on tool usage, arguments are put forward as to why the future evolution of support environments may actually increase the importance of such a broad perspective.

Suggestions for how to update the mental models of the surveyed safety standards, and other standards like them, are put forward based on this identified need for a broader perspective.

Sammanfattning

Den ökande komplexiteten och storleken på Cyber-Fysiska System (CPS) har lett till att produktiviteten i utvecklingen av CPS har minskat kraftigt. Krav på att CPS ska vara säkra att använda förvärrar problemet ytterligare, då dessa ofta är svåra att säkerställa och samtidigt av stor vikt för samhället.

Mjukvaruverktyg, eller egentligen alla insatser för att automatisera utvecklingen av CPS, är en central komponent i många innovationer menade att lösa detta problem. Även om forskningen endast delvis studerat säkerhetsrelaterade konsekvenser av att automatisera produktutveckling, så är det känt att automation har haft en kraftig (och subtil) inverkan på operationella system. Om verktyg ska lösa problemet med en ökande komplexitet hos säkerhetskritiska CPS, så måste verktygens påverkan på produktutveckling, och i förlängningen på det säkra användandet av slutprodukterna, vara känd.

Den här boken ger en översikt av forskningsfronten gällande *säkerhetsrelaterade konsekvenser av verktygsanvändning*. Denna kommer från en litteraturstudie i områdena *systemsäkerhet*, *mjukvaruutveckling* och *verktygsintegration*. Industriella säkerhetsstandarder identifieras som en viktig informationskälla. Då riskerna med användandet av *enskilda* verktyg har undersökts i stor utsträckning hos producenter av produkter relaterade till *transport*, studeras flera välkända säkerhetsstandarder från denna domän. Enligt de utvalda standarderna bör automation primärt utvärderas utifrån dess förmåga att självständigt utföra enskilda processteg på ett robust sätt. Automation som stödjer operatörers egna handlingar ses som tämligen oviktig.

En *konceptuell modell* och en *referensmodell* har utvecklats baserat på litteraturstudien. Den förstnämnda definierar vilka entiteter och relationer som är av vikt för säkerhetsrelaterade konsekvenser av verktygsanvändning. Den sistnämnda beskriver olika aspekter av verktygsintegration och hur dessa relaterar till varandra. Genom att kombinera modellerna och utföra en riskanalys har egenskaper hos verktygskedjor som måste säkerställas för att undvika risk identifierats. Tio sådana *säkerhetsrelaterade egenskaper* beskrivs.

Dessa säkerhetsrelaterade egenskaper möjliggör ett systematiskt sätt att begränsa vad som måste beaktas under studier av risker relaterade till verktygsanvändning. Hypotesen att ett stort antal faktorer relaterade till verktygsanvändning innebär risk kunde därför testas i en empirisk studie. Denna studie identifierade säkerhetsrelaterade svagheter i utvecklingsmiljöer knutna både till höga och låga nivåer av automation. Slutsatsen är att ett brett perspektiv, som inkluderar fler faktorer än de som beaktas av de utvalda standarderna, kommer att behövas i framtiden.

Tre möjliga orsaker till att ett bredare perspektiv ändå skulle vara irrelevant analyseras, nämligen egenskaper specifika för CPS-domänen, egenskaper hos säkerhetskritiska CPS och möjligheten att lita på en beprövad, manuell process. Slutsatsen blir att ett bredare perspektiv är motiverat, och att den framtida utvecklingen av utvecklingsmiljöer för CPS sannolikt kommer att öka denna betydelse.

Baserat på detta breda perspektiv läggs förslag fram för hur de mentala modellerna som bärs fram av de utvalda säkerhetstandarderna (och andra standarder som dem) kan utvecklas.