Professoren und
wissenschaftliche Mitarbeiter des
Forschungsprojektes Programmverifikation
der Universitäten
Karlsruhe und Kaiserslautern

Karlsruhe, den 31.10.1983

Sehr geehrte(r) Abgeordnete(r) des Deutschen Bundestages,

im Zusammenhang mit der Nachrüstung wird in letzter Zeit immer häufiger von einem möglichen Atomkrieg infolge von Computerfehlern gesprochen. Da das Ziel unserer Forschungsarbeit in der Entwicklung von Hilfsmitteln zur Erstellung sicherer Computerprogramme besteht, möchten wir aus fachlicher Sicht zu diesem Punkt Stellung nehmen.

In der Informatik ist allgemein bekannt, daß Computerprogramme, insbesondere große und komplexe Programmsysteme, stets Fehler enthalten. Die Beseitigung von Fehlern nach der Inbetriebnahme ist in der Industrie oft ein größerer Kostenfaktor als die Erstellung dieser Programme.

Zur Überprüfung der korrekten Funktionsweise eines Computerprogramms gibt es grundsätzlich zwei Möglichkeiten:
1. Test: Mit ausgewählten Eingabedaten wird der Ablauf des Programms simuliert.
2. Verifikation: Die Korrektheit des Programms wird in Form von mathematischen Beweisen nachgewiesen.

Bisher wird die Korrektheit eines Programms fast ausschließlich durch Testen überprüft, da sich die Methoden zur Verifikation erst in der Entwicklung befinden. Das Testen eines Programms kann grundsätzlich nur die Anwesenheit einzelner Fehler nachweisen, nicht aber deren Abwesenheit. Ab einer gewissen Komplexität enthält ein Programm stets Fehler, die nicht alle durch Testen entdeckt werden können. Bei Programmen mit hohen Zuverlässigkeitsanforderungen ist deshalb eine formale Verifikation nötig.

Die Forschungen auf dem Gebiet der Programmverifikation haben zum Ziel, Methoden zum formalen Nachweis der Korrektheit zu entwickeln, mit deren Hilfe die Fehlerwahrscheinlichkeit in Computerprogrammen drastisch verringert werden kann.
Selbst die Verifikation kann keine 100 %ige Sicherheit garantieren, unter anderem weil sie keine Aussagen über technische Defekte der zugrundeliegenden Geräte machen kann.

Aufgrund unserer eigenen Arbeiten und der Zusammenarbeit mit anderen führenden Forschungsgruppen (vor allem in den USA) sowie mit namhaften deutschen Industriefirmen können wir den weltweiten Stand der Technik in der Programmverifikation (und damit der Computersicherheit) recht gut beurteilen.

Die Grundlagenforschung auf diesem Gebiet ist im Moment noch nicht abgeschlossen, und auch für die theoretisch geklärten Teilprobleme sind erste prototypische Systeme gerade erst in der Entwicklung. Die Verifikation von hochkomplexen Softwarepaketen ist in absehbarer Zeit unrealistisch.

Die Computerprogramme der Frühwarnsysteme gehören zu den größten überhaupt bestehenden Softwareprodukten, bei denen die angedeuteten Sicherheitsprobleme deshalb in besonderem Maße bestehen (die Fehlerhäufigkeit wächst überproportional mit der Größe und Komplexität eines Programms). Wie solche Systeme in einer unvorhergesehenen Ausnahmesituation reagieren, ist im Grunde unbekannt. Dies belegen die zahlreich bekannt gewordenen und dokumentierten Fehlalarme in amerikanischen Frühwarnsystemen.

Die kurzen Vorwarnzeiten und die höhere Treffsicherheit der neuen Raketengenerationen führen dazu, daß das Verhalten der politischen und militärischen Führungsspitze immer mehr von Computeranalysen abhängig wird. Die wenigen zur Verfügung stehenden Minuten sind kaum ausreichend, um dabei zwangsläufig auftretende Fehler als solche zu erkennen. Auch für eine Bestätigung der eventuell fehlerhaften Computerdaten durch andere Quellen fehlt dem Politiker im Ernstfall die Zeit.

Es spricht einiges dafür, daß diese Computerabhängigkeit durch die Qualität der neuen westlichen Raketen auch auf sowjetischer Seite verstärkt wird.
Können wir uns darauf verlassen, daß dann die sowjetischen Politiker oder Militärs bei einem Alarm, der zwar durch einen Computerfehler ausgelöst aber nicht als solcher erkannt wurde, stillhalten und nicht reagieren, bevor sie einen Einschlag auf ihrem Territorium registrieren?
Sollen wir darauf vertrauen, daß die Sowjetunion angesichts der hohen Treffsicherheit der westlichen Raketen die vermeintliche Vernichtung eines großen Teils der eigenen Waffen zuläßt, ohne diese vorher zu einem Gegenschlag zu nutzen?
Solche Spekulationen erscheinen als äußerst riskantes und makabres Spiel mit dem Leben fast aller in Europa lebenden Menschen.

Sicher sind die sowjetischen SS20-Raketen für uns eine schlimme Bedrohung. Aber was nützt uns ein Gegengewicht zu diesen Raketen und immer größere Abschreckung, wenn dies zum Atomkrieg durch Computerfehler führen kann?
Die Wahrscheinlichkeit dafür wächst mit jeder neuen, insbesondere schnelleren und treffsichereren Rakete ganz drastisch.

Wir empfinden es als unsere besondere Pflicht, Sie nachdrücklich auf diese Situation hinzuweisen. Wir bitten Sie, die Ihnen übertragene Verantwortung zu nutzen und alles zu tun, um einen drohenden Atomkrieg durch Computerfehler zu verhindern.

Dieser Brief wird gemeinsam von allen am Projekt beteiligten Wissenschaftlern getragen.