



בי 1

MICROCOPY RESOLUTION TEST CHART

DAT SEC. F.Y. (LASS CATON Inclassified CAT'S CASS CATON A UNDER SECTION Inclassified CAT'S CASS CATON DOWNGRADNG SCHEDULE Unlimited TORMING ORGANIZATON SEPORT NUMBERSS S VONTORING ORGANIZATON SEPORT NUMBERSS S VONTORING ORGANIZATON SEPORT NUMBERSS S VONTORING ORGANIZATON SECTION AVAILABLITY OF REPORT NUMBERSS S VONTORING ORGANIZATON SECTION AVAILABLE S VONTORING ORGANIZATON S VONTORING ORGANIZATON SECTION AVAILABLE S VONTORING ORGANIZATON S VONTORING ORGANIZATON S DOPESS CR, Stare and JPCORP SONAL AVAILABLE S VONTORING ORGANIZATON S SUBJECT SECTION S S SUBJECT SECTION S S SUBJECT SECTION S S S S S S S S S S S S S S S S S S S		REPORT DOCUM	MENTATION	PAGE			
Inclassified 3 Signal field CLAPT CLASSE CATON DOWNGRADING SCHEDULE 1 Signal field CLASSE CATON DOWNGRADING SCHEDULE Unlimited ECLASSE CATON DOWNGRADING SCHEDULE Unlimited Control C	PORT SEC. R.TY CLASSIE CATION			MARKINGS			
EC.A.1Y CASSP CATON SUMMERS 1 DisTRBUTION AVAILABILITY OF REPORT EC.A.SP CATON DOWNGADING SCHEDULE Unlinited EC.A.SP CATON DOWNGADING SCHEDULE Unlinited STORMING ORGANIZATION REPORT NUMBERS 5 WONJORNG ORGANIZATION REPORT NUMBERS Cornell University TR 85-708 5 WONJORNG ORGANIZATION REPORT NUMBERS Well OF PERFORMING ORGANIZATION 60 OFFICE SYMBOL Walk OF PERFORMING ORGANIZATION 60 OFFICE SYMBOL Walk OF PERFORMING ORGANIZATION 74 WARE OF WONTORING ORGANIZATION Cornell University 75 ADDRESS CIP, State and ZIP Code) Datt of Computer Science 76 DORES CIP, State and ZIP Code) Work OF VIENDAMING ORGANIZATION 74 VAINE Research Office of Naval Research 76 SOURCE OF SUNDING Office of Naval Research 76 SOURCE OF SUNDING VIENDES ODENTIFIC OF SUNDING VIENDES 76 SOURCE OF SUNDING VIENDES MORE OFFICE SWARD, MARK SOURCE OF SUNDING VIENDES 70 SOURCE OF SUNDING VIENDES ODENTIFIC OF SUNDING VIENDES 80 OFFICE SWARD, MARK VIENDES MORE OF VIENDAMING ORGANIZATION 76 SOURCE OF SUNDING VIENDES OFFICE SWARD, VIENDES 80 OFFICE SWARD, MARK VIENDES OTTIGE OF SUNDING VIENDES 80 OFFICE SWARD, MARK VIENDES	Unclassified						
ECLASSFICATION DOWNGRADING SCHEDULE Unlimited SPGRAMING ORGANIZATION REPORT NUMBER(S) 5 MONTORING OPCANIZATION REPORT NUMBER(S) 5 MONTORING OPCANIZATION REPORT NUMBER(S) Cornell University TR 83-708 60 DFFCE SYNBOL 74 NAME OF VONTORING ORGANIZATION Date of Participation 60 DFFCE SYNBOL 74 NAME OF VONTORING ORGANIZATION Dotted I University 0 Office of Naval Research 0 DOTES (G, State and 2P Code) Dotted I University 10 SOURCE Core 800 North Quincy Street Act of explorer Science 800 North Quincy Street Actination, VA 22217-5000 Mage of with Source and 2P Code! 10 SOURCE OF SUND NO NUMBERS 900CRAM Sold Street and 2P Code! 10 SOURCE OF SUND NO NUMBERS 900CRAM Sold Office of Save and 2P Code! 10 SOURCE OF SUND NO NUMBERS 10 SOURCE OF SUND NO NUMBERS Sold Street and 2P Code! 10 SOURCE OF SUND NO NUMBERS 10 SOURCE OF SUND NO NUMBERS Sold Street and 2P Code! 10 SOURCE OF SUND NO NUMBERS 10 SOURCE OF SUND NO NUMBERS Sold Street and 2P Code! 10 SOURCE OF SUND NO NUMBERS 10 SOURCE OF SUND NO NUMBERS Sold Street and 2P Code! 10 SOURCE OF SUND NO NUMBERS 10 SOURCE OF SUND NO NUMBERS Sold Street and 2P Code! 10 SOURCE OF SUND NO NUMBERS 10 SOURCE OF SUND NO NUMBERS Sold Street and 2P Code! 10 SOURCE OF SUND NO NUM	CURITY CLASSIFICATION AUTHORITY		3 DISTRIBUTION	AVAILABILITY C	DF REPORT		
BROWING DRGANZATON REPORT NUMBER(S) S VONTORING ORGANZATON REPORT NUMBER(S) Cornell University TR 85-708 S VONTORING ORGANZATON REPORT NUMBER(S) Cornell University TR 85-708 S VONTORING ORGANZATON OFFICE SYMBOL (If applicable) S VONTORING ORGANZATON REPORT NUMBER(S) Cornell University S DIFFCE SYMBOL (If applicable) S VONTORING ORGANZATON Office of Naval Research 200 North Quincy Street Arlington, VX 22217-5000 Dept. of Computer Science (If applicable) S DOFFCE SYMBOL (If applicable) S VONTORING ORGANZATON VLMBER 200 North Quincy Street 300 North Quincy	ECLASSIFICATION DOWNGRADING SCHEDU		l'nlim	ited			
Cornell University TR 85-708 LAWE OF PERFORMING ORGANIZATION Cornell University Cornell University Diffice of Naval Research Diffice of Naval Research Diffice of Naval Research BOD North Quincy Street AND OF THE Computer Science Cornell University Italian Street BOD North Quincy Street BOD North Oulney Street Street and Diffice Street and Diffice Street without Stuttering Cornell Street The Subject Terms and Merces Street without Stuttering Cornell Street Street without Stuttering Table Street The Subject Terms work of street Street without Stuttering Table Street Street without Street	ERFORMING ORGANIZATION REPORT NUMBE	R(S)	5 MONITORING	ORGANIZATION	REPORT NUN	IBER(S)	
DAME OF PERFORMING ORGANIZATION 60 05FCE SYMBOL (If splikable) Ta VAME OF VONITORING ORGANIZATION Office of Naval Research DDRESS CR, State and ZMCOde) 05 05FCE SYMBOL (If splikable) 75 ADDRESS CR, State and ZMCOde) DDRESS CR, State and ZMCOde) 75 ADDRESS CR, State and ZMCOde) DDRESS CR, State and ZMCOde) 75 ADDRESS CR, State and ZMCODE (If splikable) DDRESS CR, State and ZMCODE Computer Science Commit Interview 80 North Quincy Street Antination, VA 22217-5000 DDRESS CR, State and ZMCODE (If splikable) 9 PROCEREWEY VSTRUMENT DEVIFICATION VLWBER NO014-86-K-0092 DDRESS CR, State and ZMCODE (If splikable) 10 SOURCE OF SUMENT, VLWBER NO014-86-K-0092 DDRESS CR, State and ZMCODE (If splikable) 10 SOURCE OF SUMENT, VLWBER NO014-86-K-0092 DDRESS CR, State and ZMCODE ARTINET 10 SOURCE OF SUMENT, VLWBER NO014-86-K-0092 DDRESS CR, State and ZMCODE ARTINET 10 SOURCE OF SUMENT, VLWBER NO014-86-K-0092 Safety Withhut Stuttering (ESONAL AU*HOR(S) BOWEN ALPETN, Alan J. Demers, Fred B. Schneider Trace of secont intertim race of secont intertim race of sumentary of address of sumentary safety, invariance under stuttering, temporal logic, concurrent program's, program properties safety, invariance under stuttering, temporal logic, concurrent program's, program properties safety, invariance under stuttering, as well as for properties that are. DDRESS FELE COPY S1 ABSTRACT SECURITY CLASSIFCATION BARE OF RESPONSIBLE ADDRESS FRACT DUNCLASSIFICATI	Cornell University TR 85-708						
Cornell Intersity Office of Naval Research DoPESS Cry, State, and ZPCode) To ADDRESS Cry, State, and ZPCode) Dept. of Computer Science BOD North Quincy Street Artington, VA 128217-5000 Artington, VA 22217-5000 Value Cri, SUNKG SPONSORING Bb DF-CE SYMBOL Make Cri, SUNKG SPONSORING Bb DF-CE SYMBOL ODITION (Mainer Street Artington, VA 22217-5000 T.E. Unifued Security Classification! State and ZPCode) S00 North Quincy Street NO014-86-K-0092 Artington, VA 22217-5000 To Suprescore Finishing Properties Safety without Stuttering State of Suprescore Finishing Properties Safety without Stuttering To Suprescore Finishing Properties Safety without Stuttering To Suprescore Finishing Properties Safety without Stuttering To Suprescore Finishing Properties Safety without Stuttering Supect Teles Safety woration Supect Teles Supect Control of Safety properties is given. The formalization agrees with the informal definition - for properties is given. The formalization agrees with the informal definition - for properties that are. OTT, FILE COPY The Suprescore File Properties Code Properties Summe OF RESPONSignet North Laws Suprescore	AME OF PERFORMING ORGANIZATION	60 OFFICE SYMBOL	7a NAME OF M	ONITORING ORG	ANIZATION		
DDRESS City State and ZIP Code) 75 ADDRESS City State and ZIP Code) Dapt of Computer Science 800 North Quincy Street Arlington, VX 14833 Arlington, VX 22217-5000 WG CR X-NOK SPONSORIG 86 DFFCE SYMBO. May Core X-NOK SPONSORIG 86 DFFCE SYMBO. DOTESSICH, State and ZIP Code) 3 240C.8EWEVT VSTRUMENT DEVIFECATION V_VBER SDDRESS (Cr. State and ZIP Code) 3 240C.8EWEVT VSTRUMENT DEVIFECATION V_VBER SDDRESS (Cr. State and ZIP Code) 3 20014-86-K-0092 SDDRESS (Cr. State and ZIP Code) 3 00014-86-K-0092 SDTESS (Cr. State and ZIP Code) 3 000014-86-K-0092 SDTESS (Cr. State and ZIP Code) 3 000014-86-K-0092 SDTESS (Cr. State and ZIP Code) 3 000014-86-K-0092 SDTEMEUTION: AUXIENT CLASSERCONS WORK JUIT ACCESSION NO COSATI (CODES 13 SUBJECT TERMS (Continue on reverse if necessary and dentify by block number) STEREUTION: AUXIENDER	Cornell University	(ir applicable)	Office o	f Naval Res	earch		
Dept. of Computer Science 800 North Quincy Street Arlington, VX 12853 Steet Symbol. AWE 07.1.VDNG 5PONSORAG Bb OFFCE Symbol. Med 07.1.VDNG 5PONSORAG Bb OFFCE Symbol. Safety without Stuttering Boorn Alpern, Alan J. Demers, Fred B. Schneider TYPE 05 steedat 135 mME COVERD Interim 136 mME COVERD Leptementary votation 136 SubJECT TERMS (Continue on reverse if necessary and identify by block number) Safety, invariance under stuttering, temporal logic, concurrent program 's, program properties Informal ization of safety properties is given. The formalization arees with the informalization of safety	ODRESS City. State, and ZIP Code)	L	75 ADDRESS (Cri	y, State, and ZIF	Code)		
Ichaca, NY 14833 Arlington, VA 22217-5000 AWE OF FLYD VG SPONSORING (MaxWar ON) BD OFFCE SYMBOL (Mappicable) 3 PROCREWENT VSTRUMENT DENTIFCATION NUMBER NO014-B6-K-0092 DSRESS(CN, State, and ZP Code) BD OFFCE SYMBOL (Mappicable) 16 SOURCE OF FLYDING NUMBERS PROCREWENT VSTRUMENT DENTIFCATION NUMBER NO014-B6-K-0092 SOPESS(CN, State, and ZP Code) BD OFFCE SYMBOL (Mappicable) 16 SOURCE OF FLYDING NUMBERS PROCREWENT VSTRUMENT DENTIFCATION NUMBER NO014-B6-K-0092 Safety without Stuttering BROGRAM PROCREWENT NO NO Task NO Safety without Stuttering Bowen Alpern, Alan J. Demers, Fred B. Schneider Task NO NO Safety without Stuttering IB NUBLECT TERMS (Continue on reverse if necessary and identify by block number) safety, invariance under stuttering, temporal logic, concurrent program 's, program properties 18 SUBLECT TERMS (Continue on reverse if necessary and identify by block number) safety, invariance under stuttering, temporal logic, concurrent program 's, program properties IsstRACT (Continue on reverse if necessary and identify by block number) Safety properties is given. The formalization agrees with the informal definition - that a safety property stipulates that some "bad thing" doesn't happen during execution - for properties that are not invariant under stuttering, as well as for properties that are. DTRC FILE COPY I ABSTRACT SECURITY CLASSIFICATION NAME OF RESPONSIBLE NONVIDUAL Fred B. Schneider I DDTC USERS	Dept. of Computer Science Cornell University		800 Nort	h Quincy St	reet		
AME OF S. NONG SPONSORING (If applicable) Bb OFFCE SYMBOL (If applicable) P SOC.REMENT INSTRUMENT DENTIFICATION NUMBER NO0014-86-K-0092 DOPESSION, State and /PCode) 10 SOURCE OF SUNDING NUMBERS NO0014-86-K-0092 NO014-86-K-0092 DOPESSION, State and /PCode) 10 SOURCE OF SUNDING NUMBERS S00 North Quincy Street Arlington, VA 22217-5000 10 SOURCE OF SUNDING NUMBERS Safety without Stuttering TeleMoude Security Classification) Safety None Alpern, Alan J. Demers, Fred B. Schneider Safety of apport Interim 13b TIME COVERD Costati COOES 14 Date OF REPORT (Year, Month, Day) Is PAGE COUNT 4 COSATI COOES 18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Safety, invariance under stuttering, temporal logic, concurrent program 's, program properties BSTRACT (Continue on reverse if necessary and identify by block number) Safety properties is given. The formalization agrees with the Informal definition - that a safety property stipulates that some Toad thing'' doesn't happen during execution - for properties that are not invariant under stuttering, as well as for properties that are. Image: Safety CLASSIFICATION DISTRIBUTION, AVAILABILITY OF ABSTRACT JUNCLASSIFIEDUNUMERD SABAPE edition may be used until eshausted Al other editions are dospied 21 ABSTRACT SECURITY CLASSIFICATION oF THIS PAGE SIAPP edition may be used until eshausted Al other editions are dospied SECURITY CLASSIFICATION OF THIS PAGE <td>Ithaca, NY 14853</td> <td></td> <td>Arlingto</td> <td>n, VA 222</td> <td>17-5000</td> <td></td> <td></td>	Ithaca, NY 14853		Arlingto	n, VA 222	17-5000		
Office of Naval Research N00014-86-K-0092 ODPRESSION, State. and JPCOde) 10.5004EC OF SUNDING VUMBERS S00 North Quincy Street PROJECT Arlington, VA 22217-5000 PROJECT T.E. Unclude Security Classification) Safety without Stuttering Safety without Stuttering PROJECT "FSONAL AU"-OR(S) Bowen Alpern, Alan J. Demers, Fred B. Schneider "Voc OF REPORT 13b TIME COVERED Interim 13b TIME COVERED Interim 13b TIME COVERED Safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) safety properties is given. The formalization agrees with the informal definition - that a safety property stipulates that some "bad thing" doesn't happen during execution - for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY It ABSTRACT SECURITY CLASSFECATION NAME OF RESONSIBE (NONUDUAL Fred B. Schneider 22 7 0 8 0 DISTRIBUTION/AVAILABILITY OF ABSTRACT DITIC USERS DITIC USERS 21 ABSTRACT SECURITY CLASSFECATION NAME OF RESONSIBE (NONUDUAL Fred B. Schneider 21 ABSTRACT SECURITY CLASSFECATION (CASSFECATION FINIS PAGE All other editions ar	IAME OF FUNDING SPONSORING DRGANIZATION	8b OFFICE SYMBOL (If applicable)	9 PROCUREMEN	T NSTRUMENT (DENTIFICATIO	N NUMBER	
COPRESSICITY, State and 2/P Code: 10 SQUECE OF =:VIQ:MC NUMBERS BOD North Quincy Street PROJECT Arlington, VA 22217-5000 PROJECT Tel: (Include Security Classification) Safety without Stuttering "ESONAL AUTOPS) Bowen Alpern, Alan J. Demers, Fred B. Schneider Type OF REPORT Table Time Covered Interim "Sold Covered COSATI CODES "Stafe Y, invariance under stuttering, temporal logic, concurrent program's, program properties Safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) Safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) A new formalization of safety properties is given. The formalization agrees with the informal definition - that a safety property stipulates that some? "bad thing?" doesn't happen during execution - for properties that are. DTIC, FILE COPY Image: safety report (cassification) NAME OF REPORTIES that are. 21 ABSTRACT SECURITY (Cassification) NAME OF REPORTIES that are. 21 ABSTRACT SECURITY (Cassification) DINC, FILE COPY 21 ABSTRACT SECU	Office of Naval Research		N00014-8	6-K-0092		<u> </u>	
OUD AUCH VULLEY SELECT Arlington, VA 22217-5000 PROJECT ELEMENT VO TASK VORK JUT VORK	DDRESS (City, State, and ZIP Code)	10 SOURCE OF	UNDING NUMBE	RS			
T.E (Include Security Classification) Safety without Stuttering TEFSONAL AUTHOR(S) Bowen Alpern, Alan J. Demers, Fred B. Schneider TVPE OF REPORT 13b TIME COVERED 14 DATE OF REPORT (Year, Month, Day) 15 Page COUNT UPPLEMENTARY NOTATION COSATI CODES 18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) A new formalization of safety properties is given. The formalization agrees with the informal definition – that a safety property stipulates that some bad thing ¹¹ doesn't happen during execution – for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY DITC STRIBUTION/AVAILABILITY OF ABSTRACT DUNCLASSIFICOUNLIMITED SAME AS RPT DOTIC USERS 21 ABSTRACT SECURITY CLASSIFICATION NAME OF REPONSIBLE ANDIVUDUAL Fred B. Schneider 607-255-9221 SECURITY CLASSIFICATION OF THIS PAGE All other edutions are obsolete	Arlington, VA 22217-5000		ELEMENT NO	PROJECT NO	NO	WOF	rk unit Ission no
Safety without Stuttering Safety without Stuttering Solver Authors Bowen Alpern, Alan J. Demers, Fred B. Schneider Type OF REPORT 13b TIME COVERED 14 DATE OF REPORT (Year. Month. Day) 15 PAGE COUNT UPPLEMENTARY NOTATION COSATI CODES 18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number) safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) A new formalization of safety properties is given. The formalization agrees with the informal definition - that a safety property stipulates that some "bad thing" doesn't happen during execution - for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY 21 ABSTRACT SECURITY CLASSIFICATION DAME OF RESPONSIBLE INDIVIDUAL 21 ABSTRACT SECURITY CLASSIFICATION ZUNCLASSIFIED UNLIMITED SAME AS RPT Dotic users 21 ABSTRACT SECURITY CLASSIFICATION ZAME OF RESPONSIBLE INDIVIDUAL 21 ABSTRACT SECURITY CLASSIFICATION NAME OF RESPONSIBLE INDIVIDUAL 21 ABSTRACT SECURITY CLASSIFICATION OF THIS PAGE All other edutions are obsolvere 22 OFFICE SYMBOL 607-255-9221 <t< th=""><th></th><th></th><th>L</th><th><u>L</u></th><th><u> </u></th><th></th><th></th></t<>			L	<u>L</u>	<u> </u>		
UPPLEMENTARY NOTATION COSATI CODES SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) A new formalization of safety properties is given. The formalization agrees with the informal definition - that a safety property stipulates that some?" bad thing" doesn't happen during execution - for properties that are not invariant under stuttering, as well as for properties that are. DTTC, FILE COPY DDISTRIBUTION / AVAILABILITY OF ABSTRACT OUNCLASSIFIED/UNLIMITED SAME AS RPT OTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Pred B. Schneider BECURITY CLASSIFICATION OF THIS PAGE All other editions are obsolice	Bowen Alpern, TYPE OF REPORT 13b TIME CO	Alan J. Demers, DVERED	Fred B. Sch	neider RI_(Year, Month	, Day) 15 F	AGE COUN	r
COSATI CODES 18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Safety, invariance under stuttering, temporal logic, concurrent program's, program properties A new formalization of safety properties is given. The formalization agrees with the informal definition – that a safety property stipulates that some bad thing'' doesn't happen during execution – for properties that are not invariant under stuttering, as well as for properties that are. DTDC, FILE COPY Image: Copy of abstract DUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC GRESONSIBLE (NDIVIDUAL Fred B. Schneider 21 ABSTRACT SECURITY CLASSIFICATION OF THIS PAGE AME OF RESPONSIBLE (NDIVIDUAL Fred B. Schneider 83 APR edition may be used until exhausted All other editions are obsolete	interim FROM	01	October	1985		4	
EFELD GROUP SUB-GROUP safety, invariance under stuttering, temporal logic, concurrent program's, program properties NBSTRACT (Continue on reverse if necessary and identify by block number) A new formalization of safety properties is given. The formalization agrees with the informal definition – that a safety property stipulates that some? bad thing''' doesn't happen during execution – for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY Image: Copy of the second state of t	INTERIM FROM	TO	October	1985		4	
Concurrent program's, program properties Concurrent program's concurrent prog	INTERIM FROM	18 SUBJECT TERMS (October Continue on revers	e if necessary ar	nd identify by	4 y block num	1ber)
A new formalization of safety properties is given. The formalization agrees with the informal definition – that a safety property stipulates that some "bad thing" doesn't happen during execution – for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE NDIVIDUAL Fred B. Schneider BLACK Schneider BLACK SCHNEICE STUDE SCHNEICE SCHNEIC	INTERIM FROM		October Continue on revers ariance unde	e if necessary ar r stutterin	nd identify by g, tempor	4 y block num cal logic	iber)
A new formalization of safety properties is given. The formalization agrees with the informal definition - that a safety property stipulates that some "bad thing" doesn't happen during execution - for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY DISTRIBUTION / AVAILABILITY OF ABSTRACT DUNCLASSIFIED/UNLIMITED SAME AS RPT OTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR B3 APR edition may be used until exhausted All other editions are obsolete Structure of the second	INTERIM FROM	TO 18 SUBJECT TERMS (safety, inv concurrent	October Continue on revers ariance unde program's, p	1985 e <i>if necessary ar</i> r stutterin rogram prop	nd identify by g, tempor erties	4 y block num al logic	1ber) 2 ,
And the for properties that are not invariant under stuttering, as well as for properties that are. DTIC, FILE COPY DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR BIAPP edition may be used until exhausted All other editions are obsolete ALL DATE DATE DATE DATE DATE DATE DATE DATE	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary)	TO TB SUBJECT TERMS (safety, inv concurrent and identify by block of	October Continue on revers ariance unde program's, p	1985 e <i>if necessary an</i> r stutterin rogram prop	nd identify by g, tempor erties	4 / block num al logic	1ber) 2 ,
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DITIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR B3 APR edition may be used until exhausted All other editions are obsolete All other editions are obsolete ALL AND ALL AND	INTERIM FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a	TO 18 SUBJECT TERMS (safety, inv concurrent and identify by block of y properties is safety property	October Continue on revers ariance unde program's, p number) given. The stipulates	e if necessary and r stutterin rogram prop formalization	nd identify by g, tempor erties on agrees	4 <i>block num</i> cal logic s with the "doesn'	iber) 2, he
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR BAR AS RPT BAR AS RPT BAR AS RPT SCHEME (Include Area Code) BAR AS RPT BAR AS RPT SCHEME (Include Area Code) BAR AS RPT BAR AS RPT SCHEME (Include Area Code) BAR AS RPT BAR AS RPT SCHEME (Include Area Code) BAR AS RPT SCHEME (Include Area Code)	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for	TO TO TO Safety, inv concurrent and identify by block of properties is safety property properties tha	October Continue on revers ariance unde program's, p humber) given. The stipulates t are not in	e <i>if necessary ar</i> r stutterin rogram prop formalizati that some ^{2 of} variant und	nd identify by g, tempor erties on agrees bad thing er stutte	4 , block num ;al logic ; with th ;"`doesn' ering, as	nber) 2 , ne 1 t 5
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED / UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR B3 APR edition may be used until exhausted All other editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a	TO B SUBJECT TERMS (safety, inv concurrent and identify by block of y properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary ar r stutterin rogram prop formalizati that some variant und	nd identify by g, tempor erties on agrees bad thing er stutte	y block num al logic with th g"'doesn' ering, as	iber) 2, 1e 1t 5
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR B3 APR edition may be used until exhausted All other editions are obsolete All other editions are obsolete	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a	TO B SUBJECT TERMS (safety, inv concurrent and identify by block of properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary and r stutterin rogram prop formalization that some ^{2 off} variant und i	nd identify by g, tempor erties on agrees bad thing er stutte	4 s with the state of the stat	iber) 2, ne 't 3
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR B3 APR edition may be used until exhausted All other editions are obsolete All other editions are obsolete All other editions are obsolete B. Schneider B. Schne	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a	TO TO TO Safety, inv concurrent and identify by block of properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary ar r stutterin rogram prop formalizati that some variant und	on agrees bad thing er stutte	y block num al logic s with th g" doesn' ering, as CTE	iber) 2, 1e 1 5
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR 83 APR edition may be used until exhausted All other editions are obsolete All other editions are obsolete DIC USERS 21 ABSTRACT SECURITY CLASSIFICATION B 2 27 080 22 0FFICE SYMBOL SECURITY CLASSIFICATION OF THIS PAGE	INTERIM FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a	TO 18 SUBJECT TERMS (safety, inv concurrent and identify by block of properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary and r stutterin rogram prop formalization that some ^{2 of} variant und that some ^{2 of}	on agrees bad thing er stutte FEB 2	y block num al logic with th " doesn' ering, as CTE 7 1986	1ber) 2, 1e 1 t 3
DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR 83 APR edition may be used until exhausted All other editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE	INTERIM FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a OTTIC, FILE COPY	TO TO Safety, inv concurrent and identify by block in properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary and r stutterin rogram prop formalization that some ² variant und that some ²	nd identify by g, tempor erties on agrees bad thing er stutte FEB 2	y block num cal logic s with th grindoesn's cring, as creation 7 1986	iber) 2, 1e 1t 3
DISTRIBUTION / AVAILABILITY OF ABSTRACT 21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED/UNLIMITED SAME AS RPT DTIC USERS NAME OF RESPONSIBLE INDIVIDUAL Fred B. Schneider FORM 1473, 84 MAR 83 APR edition may be used until exhausted All other editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE	INTERIM FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition – that a happen during execution – for well as for properties that a	TO B SUBJECT TERMS (safety, inv concurrent and identify by block of y properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary ar r stutterin rogram prop formalizati that some variant und t i i	on agrees bad thing er stutte FEB 2	4 s with th g"'doesn' ering, as CTE 7 1986	iber) 2, 1e 1t 3 D
NAME OF RESPONSIBLE INDIVIDUAL 22b TELEPHONE (Include Area Code) 22c OFFICE SYMBOL Fred B. Schneider 607-255-9221 22c OFFICE SYMBOL FORM 1473, 84 MAR 83 APR edition may be used until exhausted SECURITY CLASSIFICATION OF THIS PAGE All other editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE	INTERIM FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP SUB-GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a DTNC, FILE COPY	TO	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary and r stutterin rogram propi formalization that some ^{2,47} variant und 2,47 () () () () () () () () () () () () ()	nd identify by g, tempor erties on agrees bad thing er stutte FEB 2 2	4 s with th s with th s with th s with th s as c t c 7 1986 3 2 7	1ber) 2, 1e 1t 3 0 8 0
FORM 1473, 84 MAR 83 APR edition may be used until exhausted SECURITY CLASSIFICATION OF THIS PAGE All other editions are obsolete	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a DISTRIBUTION / AVAILABILITY OF ABSTRACT DUNCLASSIFIED/UNLIMITED SAME AS F	TO 18 SUBJECT TERMS (safety, inv concurrent and identify by block of properties is safety property properties that are.	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in	e if necessary ar r stutterin rogram prop formalizati that some ² variant und i i i i i i i i i i i i i i i i i i i	on agrees bad thing er stutte FEB 2 CATION	4 s with th s''' doesn' sring, as CTE 7 1986 3 27	1ber) 2, 1e 1t 3 0 8 0
All other editions are obsolete	interim FROM SUPPLEMENTARY NOTATION SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a DISTRIBUTION / AVAILABILITY OF ABSTRACT DUNCLASSIFIED/UNLIMITED SAME AS F NAME OF RESPONSIBLE INDIVIDUAL Erood B Same as F	TO 18 SUBJECT TERMS (safety, inv concurrent and identify by block of properties is safety property properties that are.	October Continue on revers ariance unde program's, p pumber) given. The stipulates t are not in ,	e if necessary ar r stutterin rogram prop formalizati that some variant und i i variant und i i curity classifi finclude Area Coo	nd identify by g, tempor erties on agrees bad thing er stutte FEB 2 FEB 2 CATION	4 s with th s"'doesn' ering, as CTE 7 1986 3 27 CE SYMBOL	1ber) 2, 1e 7t 3 0 8 0
	interim FROM SUPPLEMENTARY NOTATION COSATI CODES FIELD GROUP ABSTRACT (Continue on reverse if necessary A new formalization of safety informal definition - that a happen during execution - for well as for properties that a DISTRIBUTION / AVAILABILITY OF ABSTRACT JUNCLASSIFIED/UNLIMITED SAME OF RESPONSIBLE (NDIVIDUAL Fred B. Schneider	TO	October Continue on revers ariance unde program's, p number) given. The stipulates t are not in ,	e if necessary and r stutterin rogram prop formalization that some ² variant und variant und that some ² curity classifie (Include Area Coo 221	on agrees bad thing er ties DI agrees bad thing er stutte FEB 2 FEB 2 2 CATION	4 s with th s with t	1ber) 2, 1e 1t 3 0 8 0

¥ -

Safety without Stuttering*

Bowen Alpern Alan J. Demers Fred B. Schneider

> TR 85-708 October 1985

Department of Computer Science Cornell University Ithaca, NY 14853

 This work is supported, in part, by NSF Grant DCR-8320274 and a grant from the Office of Naval Research.

Current address: Xerox Palo Alto Research Center, 3030 Covoto Hill Road, Palo Alto, CA 94304.

Safety without Stuttering

Bowen Alpern Alan J. Demers Fred B. Schneider

Department of Computer Science Cornell University Ithaca, New York 14853

October 22, 1985

ABSTRACT

A new formalization of safety properties is given. The formalization agrees with the informal definition—that a safety property stipulates that some "bad thing" doesn't happen during execution—for properties that are not invariant under stuttering, as well as for properties that are.

This work is supported, in part, by NSF Grant DCR-8320274 and a grant from the Office of Naval Research.

1. Introduction

Informally, a safety property stipulates that some "bad thing" doesn't happen during execution [Lamport 77]. Examples of safety properties include mutual exclusion, deadlock freedom, and partial correctness. In *mutual exclusion*, the proscribed "bad thing" is two processes executing in critical sections at the same time. In *deadlock freedom*, it is deadlock. In *partial correctness*, it is terminating in a state not satisfying the postcondition when execution is started in a state that satisfies the precondition.

A formal definition of safety is given in [Lamport 85]. While that definition correctly captures the intuition for an important class of properties—those invariant under stuttering it is inadequate for safety properties that are not invariant under stuttering. This note gives a formal definition of safety that is independent of stuttering.

Section 2 of the paper reviews some notation for describing properties. Section 3 gives our new formalization of safety and relates it to the one in [Lamport 85]. Finally, section 4 puts our work into perspective.

2. Properties

An execution of a concurrent program can be described by an infinite sequence of states $\sigma = s_0 s_1 \dots$

which we call a history. Each state after s_0 results from executing a single atomic action in the preceding state. For a terminating program execution, an infinite sequence is obtained by repeating the final state. This corresponds to the view that a terminating execution is the same as a non-terminating execution in which after some finite time (once the program has terminated) the state remains fixed.

A property is a set of histories. We write $\sigma \vdash P$ to denote that history σ is a member of property P. A property is usually defined by a characteristic predicate on histories rather than by enumerating the histories themselves. Temporal logic provides a suitable formalism for this purpose [Lamport 83].

The following notation is used in the remainder of the paper. S is the set of states, S[•] the set of finite sequences of states, and S^{ω} the set of histories. For a history $\sigma = s_0 s_1 \dots$, define

 $\sigma[i] = s_i$

 $\sigma[...i] = s_0 s_1 ... s_i$

 $\sigma[i..] = s_i s_{i+1} \dots$

We use superscripts to denote repetition. Thus, for α in S^* , α^n is the finite sequence obtained by repeating α n times and α^{ω} is the history obtained by repeating α indefinitely. We use juxtaposition to denote catenation of state sequences.

3. Formalizing Safety

If a "bad thing" happens in a history, then it must do so in some finite prefix of that history. Based on this, Lamport [Lamport 85] formalized a safety property as any property P satisfying

 $SP_L(P): \quad (\forall \sigma: \ \sigma \in S^{\omega}: \ \sigma \models P \Leftrightarrow (\forall i: \ 0 \le i: \ \sigma[..i]\sigma[i]^{\omega} \models P))$

Thus, a safety property P is satisfied by a history σ if and only if every prefix of σ —extended to an infinite sequence by repeating its last state—also satisfies P. Extension of a finite sequence ($\sigma[...i]$) to an infinite one is necessary because only a history can satisfy a property; repetition of the last step is one of a number of ways to perform this extension.

For some properties, extending a finite sequence by repeating the final state causes problems. Consider property CP stipulating that a variable *clock* is increased for every instruction executed. Using the temporal logic notation "O" for the "next-time" operator, this is given by

CP: $(clock = N) \Rightarrow \bigcirc (clock > N)$.

Intuitively, CP is a safety property: the "bad thing" is *clock* not increasing in two successive states. However, CP does not satisfy the formal definition of safety given above. $SP_L(CP) = false$ because for no history σ —even if $\sigma \models CP$ —will the value of *clock* change after the *i*th state in $\sigma[...i]\sigma[i]^{\omega}$.

This difficulty arises only for properties that are not invariant under stuttering. A property is *invariant under stuttering* if and only if whenever a history satisfies the property, the history with every state repeated zero or more times also satisfies the property, and vice versa. More formally, any property P satisfying

 $STR(P): \quad (\forall f: f \in \mathbb{N} \to \mathbb{N}: \sigma \models P \Leftrightarrow \sigma[0]^{f(0)+1} \dots \sigma[i]^{f(i)+1} \dots \models P)$

is invariant under stuttering. Properties that are invariant under stuttering are well suited for hierarchical specification and verification [Lamport 83]. By permitting states to be repeated, meaningful statements can be made about the system at various levels of abstraction. For example, execution of a higher-level operation that is implemented by a sequence of lowerlevel operations can be viewed as a sequence of repeated, identical, higher-level states where there is one state for every lower-level instruction executed but the last, which produces a new higher-level state.

We now give a formalization of safety that agrees with SP_L for properties invariant under stuttering and that agrees with the informal definition of safety for properties (like CP) that are not. If a safety property P does not hold for a history σ , then some "bad thing" must have happened during σ . This "bad thing" must be irremediable, because a safety property requires that the "bad thing" never happen. Thus, if $\neg(\sigma \models P)$, there is some prefix of σ (that includes the "bad thing") for which no extension to a history will satisfy P. Taking the contrapositive of this, P is a safety property if it satisfies

 $SP_{ADS}(P): \quad (\forall \sigma: \ \sigma \in S^{\omega}: \ \sigma \models P \Leftrightarrow (\forall i: \ 0 \le i: \ (\exists \beta: \ \beta \in S^{\omega}: \ \sigma[..i] \beta \models P))).$

 SP_{ADS} differs from SP_L in the way prefixes are extended to form histories. SP_{ADS} permits extension using any history β , while SP_L requires extension by replicating the last state of the prefix. Note that $SP_{ADS}(CP) = true$, so CP is a safety property according to this formalization.

The relationship between SP_L and SP_{ADS} is given in the following two theorems. The first theorem states that safety properties under SP_L are also safety properties under SP_{ADS} .

Theorem: For any property P, $SP_L(P) \Rightarrow SP_{ADS}(P)$.

Proof: Assuming $SP_{L}(P)$, we must show $\sigma \models P \Leftrightarrow (\forall i: 0 \le i: (\exists \beta: \beta \in S^{\omega}: \sigma[..i]\beta \models P))$.

(∀*i*: 0≤*i*: (∃β: β∈S^ω: σ[..*i*]β⊨P))

 $\Leftrightarrow \quad (\forall i: \ 0 \le i: \ (\exists \beta: \ \beta \in S^{\omega}: \ \sigma[..i] \sigma[i]^{\omega} \models P)) \quad SP_L(P), \text{ since } \sigma[..i] \beta \models P$

 $\Leftrightarrow (\forall i: 0 \le i: \sigma[..i]\sigma[i]^{\omega} \models P) \quad \text{by Predicate Logic}$

 $\Leftrightarrow \sigma \models P \quad \text{by } SP_L(P).$

The second theorem states that every safety property according to SP_{ADS} that is invariant under stuttering is also a safety property according to SP_L .

Theorem: For any property P, $(SP_{ADS}(P) \land STR(P)) \Rightarrow SP_L(P)$.

Proof: Assuming $SP_{ADS}(P)$ and STR(P), we must show:

(1) $\sigma \models P \Rightarrow (\forall i: 0 \le i: \sigma[..i]\sigma[i]^{\omega} \models P)$

(2) $(\forall i: 0 \le i: \sigma[..i]\sigma[i] = P) \Rightarrow \sigma \models P$

First, we prove (1):

Next, we prove (2):

4. Discussion

It has been argued that properties invariant under stuttering are the only ones of real interest in program verification [Lamport 83]. We agree. This, however, is a religious issue. A formalization of safety should serve many faiths. This note presents a definition of safety that can be applied to any property.

Acknowledgments

Suggestions by D. Gries led to improvements in the clarity of the proofs.

References

- [Lamport 77] Lamport, L. Proving the correctness of multiprocess programs. IEEE Transactions on Saftware Engineering SE-3,2 (March 1977), 124-143.
- [Lamport 83] Lamport, L. What good is temporal logic? Information Processing 83, R.E.A Mason, ed., (1983), North Holland, Amsterdam.
- [Lamport 85] Lamport, L. Logical Foundation. In Distributed Systems—Methods and Tools for Specification, Lecture Notes in Computer Science, Vol 190. M. Paul and H.J. Siegert, eds. (1985), Springer-Verlag, New York.

Accession For NTIS CEARL DTIC TAS Unaphoundrd Jostificall. Distribution/ Availability Codes Avail and/or Special Dist

FILMED

END

4-86

DTIC