n pro ee n s n or Con eren eon nte te Des n ro ess e no o D Aust n s De e er
e not ress to t e ent e ro ess ro equ re ents to ste Ar te tures n

T T T A A

D D T C J
D

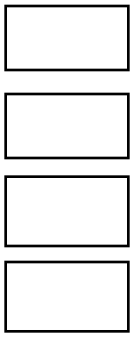
oo
A A o, tware esearc Lab

t e eve oper re ar s t e I a ent as an a y n t e e ort to pro uce qua ty so tware t en t e con ct can be avo e _I t ey re ar t e I a ent as an ene y put t ere to n au t w t t e r wor k t e con ct beco es centra to t e r re at ons p_

C B D C

Dur n t e 9 ks an 9 ks so tware ca e to p ay an portant ro e n enab n A A s eve op ent o ar er an ore co p ex spacecra t_ n ortunate y A A s cu ture o prototype an test not carry over we to t e so tware o a n]_A nu ber o actors a k so tware s n cant y erent an n erent y ess sa e_B u] sts t e co p ex ty o so tware h re at on to ts s e so tware as no up cate co ponents t e ac ko a abr cat on sta e so tware s pure y a es n an c aot c be av or u e c an es n be av or n response to nor c an es n nput _In a t on to t ese so tware s seen as ore a eab e t an ar ware because o t e ac ko a abr cat oh sta e ost en neers be eve t at t s eas er to a ter so tware t an ar ware n response to c an n requ re ents_

A t ou so tware was not p cate n t e C a en er acc ent n 9 t e subsequent nqu ry o ere a c ance to assess a aspects o A A s eve op ent processes_ e o ers co ss on ent e a ac ko n epen ent overs t o eve op ent processes as a s n cant actor n t e C a en er acc ent_ ere was no process or ea n w t prob e s t at arose n t e en neer n processes an n part cu ar a ac ko n epen ent r s k assess ent_ s k were accepte n t e ace o sc e u e pressures w e t e ro e o separate sa ety pane s was re uce _ wo subsequent C reports warne t at so tware s un er represente n A A s sa ety pro ra s an t at any o t e sa e sta k s t at contr bute to t e C a en er acc ent are now be n repeate w t respect to so tware]_ ese reports reco en e t at A A a opt so tware I or s utt e an or a uture



approac be a opte or a suc requ re ents_

Hav n pro uce a c earer representat on t e I tea t en procee e to ent y propert es o t e spec cat on t at s ou o t s cons stent an co p ete_A cons stency property s t at t ere s ou be no co b nat on o con t ons or w c two erent a ure recovery act ons are spec e _A co p eteness property s t at every poss b e co b nat on o a ure con t ons s ou ave so e recovery act on spec e or t_ ese propert es were teste by convert n t e tabu ar representat ons nto a or a o e n t s case C] an us n a too to test or t ese propert es_A s n cant nu ber o cohs stency errors were oun t ere were co b nat ons o con t ons or w c ore t an one recovery act on was spec e _ ese were trace to a prob e w t t e or er n o t e requ re ents_ e correct unct on n o t e FDI so tware epen s on t e tests escr be n t ese requ re ents be n carr e out n t e or er t at t e requ re ents are ven_However t s s not state exp c t y_ s n n con r e an ear er n or a observat on by t e I tea _

At t s po nt t e I tea wou ave one on to c ec k t e va ty o t e requ re ents a a nst a a ure o es an e ects ana ys s o t e bus arc tecture_ However at t s po nt n t e case stu y t e I tea oun out t at t s sect on o t e requ re ents was be n substant a y re wr tten_ Hence t ey e aye urt er ana ys s unt t e new vers on beca e ava ab e_

s case stu y ustrates two nterest n po nts about t e wor ko an I a ent_F rst t e I ana ysts o ten create t e r own representat on or exa p e a of a o e o t e eve oper s spec cat on_However t ese a ternat ve representat ons are never ven to t e eve op ent tea to use n p ace o t e or na spec cat ons_ s s to uar a a nst t e an er o t e I tea be n rawn nto eve op ent wor k an poss b y os n t e r n epen ence on subsequent ana yses o t ese co ponents_

econ t e I tea ave t e r own scret on on ow uc ana ys s to per or _For exa p e t e ana ys s oes not stop w en t e rst error s encountere _I t ere s an obv ous x to t e error t a es sense or t e I tea to assu e t s x w be a e an procee w t ot er types o ana ys s_However t ere s a po nt beyon w c urt er ana ys s a s tt e extra va ue or exa p e w en a or errors are encountere or w en as n t s case a re wr te s un erway_

T D C

Hav n escr be t e bas c I process an ustrate t w t a case stu y we now scuss so e o t e cu t es ace by I n carry n out t e r ro e_ ur current researc s nvest at n t ese prob e s an see k ways o overco n t e _

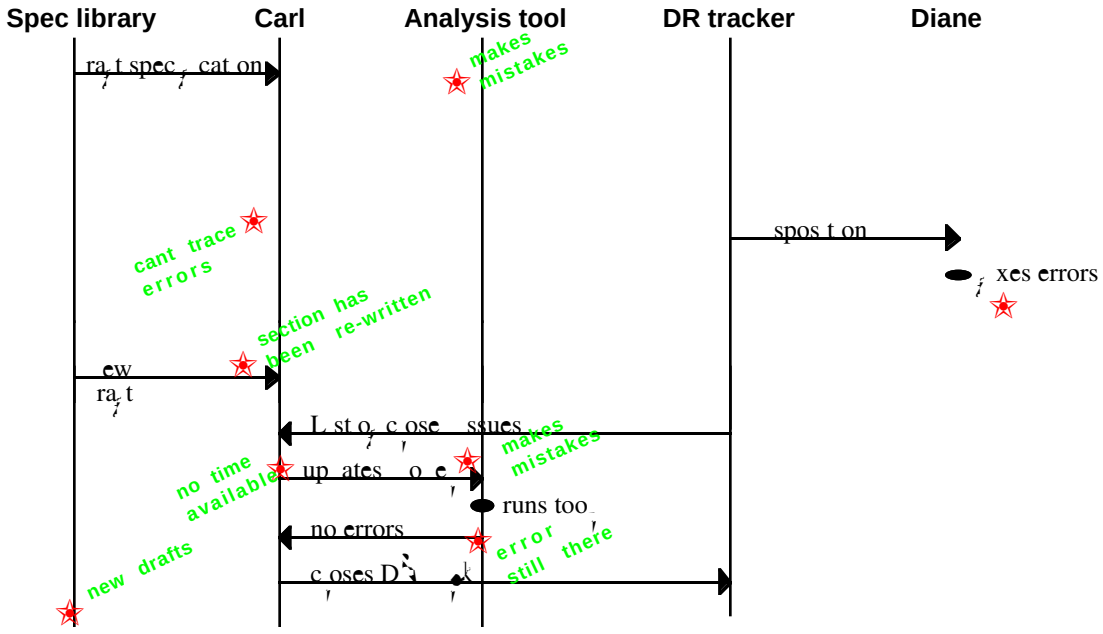
e o ow n cu t es are n erent n t e re at ons ps between t e eve oper custo er an I a ent_ o e o t ese ar se as a rect resu t o t e con ct n oa s o I an eve oper ot ers are to o w t resource pressures an t e nee or t e y resu ts

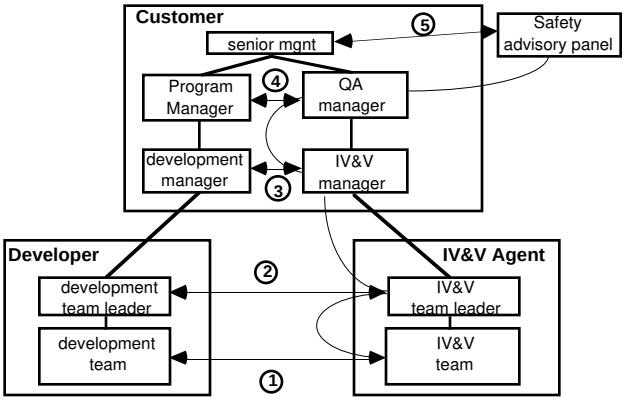
- **o o on** A co p ete eta e ana ys s o t e ent re syste s n eas b e_ E ort as to be a ocate so as to ax e ect veness_For exa p e a cr t ca ty an r s k ana ys s t be per or e to eter ne w c co ponents nee t e ost scrut ny_ n s a so a actor e ort nee s to be a ocate at t e r t po nts n t e eve op ent o a pro uct e_ a ocu ent so t at t e pro uct s ature enou to be ana y e but not so ature t at t cannot be c an e _
- **o** o be ost e ect ve I reports are nee e as qu c k y as poss b e_ ere s a ways a e ay between t e e very o an nter pro uct to t e I tea an t e co p et on o ana ys s o t at pro uct_ Dur n t s t e t e eve op ent process cont nues_ Hence I ana ys s ta k es too on t e resu ts t be ava ab e too ate to be use u _In enera t e ear er an error s repo te t e c eaper t s to correct an t e ess ret cent t e eve oper s to x t_
- **o** Contact between t e eve op ent tea an t e I tea s cu t to ana e_ e I tea nee s to a nta n n epen ence w st ensur n t ey obta n enou n or at on ro t e eve opers to o t e r ob_Fro t e eve opers po nt o v ew nteract on w t t e I tea represents a cost over ea w c can nter ere w t pro ect ea nes_ Inev tab y t e I contractor as ess access to t e eve op ent tea t an s ea_
- **o n p o** Docu entat on ro t e eve op ent tea s usua y a e ava ab e to t e I contractor n ra t or to ac tate ear y ana ys s_ e rawbac k s t at ocu ents ay be rev se w e t e I tea s ana y n t e a k n t e resu ts o t e ana ys s rre evaht be ore t s n s e _
- **po n p o** e I contractor as by necess ty cons erab e scret on over t e k n s o ana ys s to per or on erent pro ucts an w c prob e s to report_It s v ta to t e e ect ve use o I t at t e I contractor pr or t es t e prob e s t ent es_I too any tr v a prob e s are repo te t s ay swa p t e co un cat on c anne s w t t e eve oper an t e custo er an co pro se t e cre b ty o t e I a ent_
- **o o** e I contractor ay ave cu ty n ett n ts essa e across espec a y t e eve op ent contractor sputes I s asses ent_ ten prob e s oun by I ave cost an sc e u e p cat ons an n suc c rcu stances t e custo er ay be unw n to sten_ e e ect veness o I t en epen s on av n a cre b e a vocate w t n t e custo er or an at on_

e scuss so e o t ese prob e s n ore eta be ow_

Coo n on p o

In or er to nvest ate t ese prob e s urt er we eve ope a set o scenar os escr b n part cu ar I act v t es an use t ese to exp ore w ere coor nat on prob e s occur_Easterbroo k 2] escr bes t ese scenar os


Spec library
Carl
Analysis tool
DR tracker
Diane
makes mistakes
spos t on
xes errors
cant trace errors
section has been re-written
ew
ra t
L st o c ose ssues
makes mistakes
no time available
up ates o e
runs too
no errors
error still there
new drafts
c oses D


Customer
senior mgnt
5
Safety advisory panel
Program Manager
4
QA manager
development manager
IV&V manager
3
Developer
IV&V Agent
2
development team leader
IV&V team leader
development team
IV&V team
1

C C

s paper as exa ne t e ro e o I n t e so tware eve op ent process concentrat n espec a y on ts ro e n requ re ents an es n processes_ I prov es an n epen ent assess ent o bot eve op enta an operat ona r s It e ps to ent y sa ety re ab ty an per or ance concerns ear y n t e so tware ecyc e an as enera y been e onstrate to save one y t ou ear y ent cat on o errors_

e ro e o I s co p e entary to t at o A_ ere A ocuses on c ec n t at appropr ate stan ar s an process o e s are app e I ocuses on t e tec n ca nte r ty o t e so tware t rou ana ys s o spec ca ons es ns co e an ot er ocu entat on_ Hence I w ensure t at t e requ re ents are co p ete t at a propose syste arc tecture w eet t e requ re ents an t at traceab ty s e onstrate a on requ re ents es ns an test cases_

An nterest n e er ent property o t e I process s t at t e I a ent can p ay a ro e as a process prove ent a ent or a nu ber o reasons_ F rst t e reco en at ons a e by I n response to errors o ten a ress ways to prevent s ar errors occurr n n t e uture_ econ t e I tea ave so e ex b ty to app y new tec n ques an too s espec a y w ere t ese p u perce ve aps n t e ana ys s per or e by t e eve oper_ t ese new tec n ques an too s e onstrate t e r va ue n ent y n errors t e eve op ent tea ay c bose to a opt t e t e se ves_ F na y t e presence o an I contractor prov es an ncent ve or t e eve opers to prove t e r own nterna