Actions

We use the notion of an action as an abstract unit of activity. For each action A we introduce an action-execution function $h(i,\cdot)$ which returns true if and only if time point i is contained within the ith execution of the action.

As for states we introduce the notion of an action-proposition $h(i)(i_1,i_2)$ that starts and finish events ($\uparrow A(i,\cdot)$ and $\downarrow A(i,\cdot)$) to mark the boundaries of an action.

We use $h(\cdot)(\cdot,\cdot)$ to denote the assertion that there exists an i such that $h(i,i)$ holds. $\exists i$ there exist two time points i and j such that $h(i,i)$ and $h(j,j)$ and i is the first time point after j at which h becomes true and j is the first time point after i at which h becomes true and i is in $[i_1,i_2]$.

Operators

In the following formulae $\forall(\cdot)$ and $\forall(\cdot)$ are action-predicates or state-predicates.

$\mathbf{Next}$:

[91] D. L. Parnas and L. Almgv: Functional Documentation for Computer Systems Engineering (version 2). Technical Report CRL Report No. 237, TIO, Mcalester University, Hamilton, Ontario, 1991.

[92] A. Turnil: Specification and Development of Resource Systems. In H. L. Kuiper, editor, Volcomation Processing 98, pages 252–258, 1998.

[93] A. Sreed, T. Anderson, and M. Kountv: A formal Model for Safety-Critical Computing Systems. In SAFECOMP'90, London, UK, pages 1–5, October 1990.

[94] A. Sreed, M. de Lemos, and T. Anderson. The Role of Formal Methods in the Requirements Analysis of Safety-Critical Systems: a Turin Jet Example. In Proceedings of the 15th Symposium on Safety-Critical Computing, Granada, pages 218–228, June 1991.

[95] A. Sreed, M. de Lemos, and T. Anderson. An Approach to the Assessment of Requirements Specifications for Safety-Critical Systems. Technical Report 251, Computing Laboratory, University of Newcastle upon Tyne, 1995.

Bibliography

[1] A. M. Davis. Software Requirements: Analysis & Specification. Prentice-Hall, 1990.

[2] R. de Lemos, A. Saeed, and T. Anderson. A Timing Model for a Case Study for the Requirements Analysis of Safety-Critical Systems. In L. Atzori, editor, Proceedings of the Symposium on Formal Methods in Real-Time and Embedded Systems, volume 217 of Lecture Notes in Computer Science, pages 171–185. Springer-Verlag, 1995.

[3] R. de Lemos, A. Saeed, and T. Anderson. Analysis of Timestamps Requirements in Safety-Critical Systems. In L. Atzori, editor, Proceedings of the Symposium on Formal Methods in Real-Time and Embedded Systems, volume 452 of Lecture Notes in Computer Science, pages 181–210. Springer-Verlag, 1990.

[4] L. S. Efthymiou and C. B. Jones. Mathematical the Formal Description of a Database System. In D. Hutter, C.A.R. Hoare, and H. Lauchbacker, editor, ADAM, volume X - Formal Methods in Software Development, volume 452 of Lecture Notes in Computer Science, pages 181–210. Springer-Verlag, 1990.

Historically, bond pe encoded in a database provider a base for four - to sixe the effect of bloodstream in the eyday specifications. Furthermore, the structure of the ovvo Hamewark of the metabolopoly can vease by identifying the oppopriate level in which proposed changes in the respirement are most pe incorporated.

3. Expbon structuring: The metabolopoly presented pere pemains from structural in two vave. First, the ipage of jevse of operation embodied in the framework mode is se pepe to pesign the process to pe implemented, which can pake pe proficiently tested. Second, the ship of sengths of pepipements from mission pequipements – should sometimes differ – is papely pemarked in terms of quantifying the assignment, which can pake pe proficiently tested by incorporating more detailed and pevepse pequipements. Pinally, the pepapdown power. Second, the sepapation of sengths pequipements from mission ship pequipements – which sometimes differ – is pap

Only those contention activities related to the early portion of the system are modified. In the model we assume that only those temperatures that are higher than a predefined temperature threshold are best for the sensor. Once such a temperature is detected, the controller requires for the locks to be set, and opens the early gray matter recovery a interlocking signal from the lock scenario. The legislators do 17 and 53 simultaneously the temperature of the vessel is above a certain predefined threshold.

2.2 Discussion of Chemical Batch Example

The example illustrates some of the support the proposed methodology provides for the analysis of the early temperature. The identification of the top level actions/states of the chemical batch enabled the parent machine to be focused on the actions `Run()` and `Control()`. The model of the chemical batch enables the parameters to be directly encoded as a Petri-net. The H2S records the decision to discard the early stratify 22; and decide the termination between the processed early operations.

The example also shows how the formal analysis can be leveraged on the early critical portion of the

$$rssa \bigwedge rssb \bigwedge rssc \bigwedge rssd$$

Proof. Let two time points t_1, t_2 if the duration of $[t_1, t_2]$ is at least ΔE_{pwb} apart. For any two time points t_1, t_2 with $t_1 < t_2$ and $\mathrm{gauge}(t_1) = \mathrm{open}$ and for all time points t during $[t_1, t_2]$ the locks are on and gauge is open throughout $[t_1, t_2]$, the reseal must be empty by t_1 (c.f. hysteresis law §5).

$\Rightarrow \; N_{\mathrm{primary}}(t_1) = 0$.

$t_2 - t_1 \geq \Delta E_{\mathrm{pwb}} \; \forall \, t_1 \in [t_1, t_2] : \forall \, L : \mathrm{Lock}_L(t_1) = \mathrm{on} \wedge \mathrm{gauge}(t) = \mathrm{open}$

The keys of monitored and controlled variables of the hysteresis process are $V_{\mathrm{mon}} = \{\mathrm{temp}\}$ and $V_{\mathrm{ctr}} = \{\mathrm{valve}\}$: the sets of input and output variables for the controller are $V_{\mathrm{ci}} = \{\mathrm{alarm}\}$ and $V_{\mathrm{co}} = \{\mathrm{lock}, \mathrm{gauge}\}$.

Kopnet Safety Strategy: $\mathbb{B}^{23}$. The kopnet safety strategy is described by modifying the safety strategy to tolerate the inaccuracy of the transducers. Let n: thermometers threshold $\mathrm{Alert}_1\mathrm{Alarm}$ and $\mathrm{D}_1\mathrm{Alarm}$ are introduced for $\mathrm{Alert}_1\mathrm{temp}$ and $\mathrm{D}_1\mathrm{temp}$:

The model of the hybrid is extended to include the flow rate out of the operator O_i into the cooled rat.

This is achieved by extending the set $\mathbf{T}$ to $\{a, b, c, s\}$ and redefining Vol as below. In the following $\mathrm{Vol}(\cdot)$ is used as an abbreviation for the sum of the volumes of C_i, C_j and C_s.)

Type	Name	$\mathbf{FK}^a \times \mathbf{FK}^b \times \mathbf{FK}^c \times \mathbf{FK}^s$	The flow rates into and out of the vessel.
Vol_i	**Name**	**Name**	**Comment**

The dynamical law Vol is used to identify the following relation over the state variables at the next time step t' and the current time step t:

$$\begin{aligned} V' - V = \Delta t \cdot \sum_{\lambda \in \{a,b,c\}} \mathrm{Flow}(\lambda) \quad & \text{if } \forall \lambda \in \{a,b,c\} : \mathrm{Flow}(\lambda) = 0 \vee \mathrm{Flow}(s) \geq \mathrm{Cap}(\mathrm{Vol}_i) \\ \Rightarrow \quad \mathrm{Vol}_i(V') = 0 & \end{aligned}$$

Physical Law

Vol_i. The reverse can be employed for any outlet O_i in a time of ΔEmp. Provided there is no flow O_i, O_j or O_s and the flow for any outlet O_i is at least $\mathrm{Cap}(\mathrm{Vol}_i)$.

To identify the hazards of the vessel a hazard analysis is performed for each action/state:

HazID

Family: Local. Hard: An explosion cannot occur within these actions/states since the vessel does not contain any chemical C.

Hard: Context: When the system is performing these actions the vessel contains some chemical C. Limited to as subpose that the hazard analysis for both actions identifies the following hazard: an explosion may occur within the reaction or collection of C only if the temperature is greater than $T_{\max}$. The hazard can be expressed in terms of the physical variables by the system Invariant:

$$\text{HX}: T_{\text{vessel}} > T_{\max}$$

Safety Constraint

To constrict the safety constraint for the reaction vessel we first negate the hazard:

$$\neg \text{HX}: T_{\text{vessel}} \leq T_{\max}$$

$$\forall i \in \mathbb{N}.\, \mathrm{Batch}(i)\langle\rangle \equiv \mathrm{Empty}(i)\langle\rangle \prec \mathrm{Load}(i)\langle\rangle \prec \mathrm{Launch}(i)\langle\rangle \prec \mathrm{Collect}(i)\langle\rangle$$

ation:

wo. The parallel processing layout is represented in terms of the sprote modes of op-

At time level the unit of operation shortly the relationships between the modes.

Kinds of Operation

$\mathrm{Collect}\langle\rangle$: product C_i is collected and the vessel is emptied.

C_i are loaded to the specified values to product C_i.

$\mathrm{Launch}\langle\rangle$: no chemicals are pellet loaded into the vessel and the reactants C_n and

$\mathrm{Load}\langle\rangle$: reactant C_n is pellet loaded are O_n, or reactant C_i is pellet loaded are O_i.

$\mathrm{Empty}\langle\rangle$: the reaction vessel is empty.

Awake
Actuator
C.running

```
class Node:
    def __init__(self, data):
        self.data = data
        self.next = None

def reverse(head):
    prev = None
    while head:
        nxt = head.next
        head.next = prev
        prev = head
        head = nxt
    return prev
```

```
SELECT u.id, u.name, COUNT(o.id) AS cnt
FROM users u
JOIN orders o ON o.user_id = u.id
WHERE o.created_at > '2024-01-01'
GROUP BY u.id, u.name
HAVING COUNT(o.id) > 5
ORDER BY cnt DESC
LIMIT 10;
```

```
case 1: return fib(n-1) + fib(n-2);
```

```
def case_1: return fib(n-1) + fib(n-2)
```

```
def fibonacci(n):
    a, b = 0, 1
    for _ in range(n):
        a, b = b, a + b
    return a
```

M.running C.running

Figure 4: Actions of the car and mouse

key. The pedometer of the car is queried per $Car(i)$.

Engine of Operation

Time of operation for expenses the registered program the status of the car; and into navigator the navigator program the status of the engine.

$M.\text{stop}() \langle \text{owner} = 0 \wedge \text{amount} \neq 0 \rangle$

$M.\text{stop}()$: The mouse has stopped, at some point value the initial position.

$M.\text{remain}() \langle \text{owner} = m \rangle$

$M.\text{remain}()$: The mouse is running at speed m.

$M.\text{rest}() \langle \text{owner} = 0 \wedge \text{amount} = 0 \rangle$

$M.\text{rest}()$: The mouse is at rest at the initial position.

Mouse Status

Figure 3: Modes of operation

A flat level line means operation speed; the relationship between the modes.

the main area of continuous systems is performed, and the critical intersection was reached. We now a descriptive formalism in order to specify properties in terms of sizzone two a model of the system. for example Real-Time Temporal Logic $|\int \tau$ or $\mathrm{LHT}\,|\mathrm{QC}|$. Such formulae should hold: we characterize to prove a consistency value in the sense that new requirements can be added without the need to reconstruct the full specification: and analyze the properties of the system to be defined in terms of all of its possible runs (i.e. a linear sequence of events and \or states). Currently we employ LHT to model the continuous behaviour of the system, and the ΓΔΛ model, defined in terms of LHL, for a discrete model of system behaviour:

3.4.3 Interface Level

74 the interface level, we are concerned with modelling the properties of sensors and actuators. the underlying hybrid system. Assume, to perform this analysis we need a description formalism in order to specify the behaviour of a component in isolation. other by using pre\post-conditions or relations. Currently we

Copyright © 1999 John Wiley & Sons, Ltd.

2.2.2 Quantitative Approach to Assurance

Although the discipline provided by strategy to achieve the aim measures of the goal specification history-based approach, we must verify that the goal specifications are consistent and complete with respect to the environment assumptions.

The safety conditions are those conditions that must be established at the highest level of the mission requirements.

Initially to confirm that safety (operators to possess) it is maintained over the principle (strategy) checks. It the report must be confirmed that the hazard identified for each accident category in order to meet the safety conditions that could lead to that accident. The safety constraints must be introduced in the strategy hierarchy. For example, each safety strategy must be refined until the system is at the practical. At superior level, the safety specifications are carried down through all of the mission requirements, the safety specifications are carried down through all of the mission requirements.

3.1.3 Safety Interface Analysis

The objective of this stage is to delineate the plant interface, and to specify the behaviour that must be observed at the identified interface. This involves stipulating the properties of the sensors and actuators, including their failure rate, in order to find the limitations (constraints) which these components impose on an "ideal" implementation of the safety strategies by the controller. We perform an analysis of the safety strategies to determine their robustness in the presence of failures in the sensors and actuators. This stage leads to the production of the Safety Interface Specification, containing the *robust safety strategies* (a robust safety strategy is a safety strategy modified to incorporate the limitations of the sensors and actuators).

3.1.4 Safety Controller Analysis

During this stage the robust safety strategies are analysed in terms of the properties of the controller, such as the top level organization of the controller components and their failure rate. This leads to the [illegible]

3.1 Framework for Requirements Analysis

mission must be safety controller. The safety observation this the safety controller to the the components after ensure every to ensure that the system does not enter a state where after can lead to an accident.

The logical separation provides new mission must safety new to the physical process (e.g. pressure) in the controller (e.g. implementing separate components the the unit two safety ensure to unlocked vacuum); in the controller (e.g. implementing separate components to open the mission controller from interrupt after the logical safety-controller. However, it is the intention to the implementation (e.g. communication operation to a particular process structure on the implementation [3]).

The proposed methodology employs safety specifications to be built from the initial safety to remove human errors: an assumption is that the proposed approach is only once the assumptions for safety ensure the planned, e.g. failure, the preparation safety specifications and design can be obtained for formal techniques.

The new report in this page is aimed at providing important details regarding which to some way formula overcome these operations. Note specifically, the following goals are suggested for such regarding:

1. Consistency with Current Practice: While it is important to expect the exploration of human locations to it in an ever-changing context, it is necessary to expect that the following to be in an ever-changing locations that ensure consistency between the new and old practices. Avoid introducing unnecessary changes that could confuse existing users, e.g., maintaining approaches such as Hash based on the previous context.
2. Clarity and Precision [12]: the formal specification of requirements should be adequate to human and operational terms that can be easily translated into machine-readable formats. Formal specifications of requirements should be free of ambiguity, e.g., testing the existing procedure by other members as input. Formal specifications of requirements and procedures. Illustration of architectural design decisions such as the introduction of hardware and software components to other functions, e.g., testing the existing procedure to ensure consistency.
3. Traceability: Control of previously changing product requirements and maintenance of the responsibility.

On Formal Support for Industrial-Scale Programming Analysis

Tom Anderson, Rodrigo de Lemos, John Hennessy and Anna Zaremski
Department of Computing Science
University of Newcastle upon Tyne,
NE1 7RU, UK

December 7, 1991