Modeling Temporal Behavior in Complex Cyber-Physical Systems: Position Paper

Alan Burns
Real-Time System Group
Department of Computer Science
University of York, UK.
email: burns@cs.york.ac.uk   Tel: +44 (0)1904 432779

Background

In the UK a major EPSRC funded project, DIRC, is currently coming to an end. DIRC, Dependability IRC (Interdisciplinary Research Collaboration) is a 6.5 year project funding over 20 postdoc researchers and over 24 PhD students. It involves 5 universities and a number of industrial collaborations. I am one of the Principle Investigators for this project. The focus of the research is the dependability of large complex socio-technical systems with an emphasis on the human and organisational aspects of systems as well as the technical. Although centered on Computer Science, it is a broad interdisciplinary project with Psychologists, Sociologists (particularly Ethnographers), Statisticians and Economists. Whilst not focusing on any particular domain it has undertaken a number of studies in Health Care - both in hospitals and the home. A link to the to DIRC and the significant volume of output from this project can be found at www.dirc.org.uk/.

DIRC is structured as a large number of activities but with 5 key themes running through the whole research programme: **Timeliness** – see discussion below, but also including notions of temporality, affordances and emergent properties. **Risk** - its analysis and perception. **Responsibility** - how to model and predict failures. **Diversity** - to exploit and quantify the gains. **Structure** - of the entire system with an emphasis on fault tolerance.

Within the timeliness theme a framework is being developed to help structure models of the environment, requirements, platforms, equipment and control (software). The rest of this position paper is an overview of the Time Band framework developed under DIRC. It is still subject to research and experimentation. Research reports are available, but it is ongoing work. Nevertheless the motivation for the framework is exactly the challenges identified in the Cyber-Physical Systems call. In particular the need to identify architectural notions and system abstractions that are effective in this domain, and the limitations of more traditional approaches to temporality - in, for example, real-time systems.

DIRC has been successful I feel in bringing together a genuinely interdisciplinary approach to dependability and system development. I would strongly recommend some element of interdisciplinarity in the Cyber-Physical research programme.

A Time Band Framework

One characteristic of Cyber-Physical systems is that they are required to function at many different time scales (from microseconds or less to hours or more). Time is clearly a crucial notion in the specification (or behavioral description) of and com-
plex computer-based systems, but it is usually represented, in modeling schemes for example, as a single flat physical phenomenon. Such an abstraction fails to support the structural properties of the system, forces different temporal notions on to the same flat description, and fails to support the separation of concerns that the different time scales of the system facilitate. Just as the functional properties of a system can be modeled at different levels of abstraction or detail, so too should its temporal properties be representable in different, but provably consistent, time scales.

To make better use of ‘time’, with the aim of producing more dependable computer-based systems, a framework is proposed that explicitly identifies a number of distinct time bands in which the system under study is situated.

A large computer-based system exhibits dynamic behavior on many different levels. As well as the technical components, Human time scales move from the 1ms neuron firing time to simple cognitive actions that range from 100ms to 10 seconds or more. Higher rational actions take minutes and even hours. At the organizational and social level, time scales range from a few minutes, through days, months and even years. Perhaps for some environmentally sensitive systems, consequences of failure may endure for centuries. To move from nanoseconds to centuries requires a framework with considerable descriptive and analytical power.

A number of observers, from a wide range of disciplines, have noted the structural properties time exhibits in natural and engineered systems. The use of hierarchical structures is common in most systems descriptions and again temporal separation is evident in hierarchical control systems and hierarchical scheduling and planning. Although time is such an overarching phenomenon it is surprising how often temporal requirements are poorly specified in an engineering context. Even the vocabulary used to define temporal phenomena (e.g. too early, too late, on time) does not have clear semantics. How late is too late for an air bag controller, GPS decoder, ..., or conference deadline. There are technical, psychological and social issues at play here - but they all impact of the specification and behavior of systems.

The time band abstraction outlined below is an attempt to derive an engineering framework based on natural temporal phenomena. Current architectural description languages, logics, design notations (such as UML) and programming languages are typically extremely limited in their support for time and the many facets it can bring to system structure. Most formulations that attempt to identify time granularity do so by mapping all activities to the finest granularity in the system. This results in cumbersome formulae, and fails to recognize the distinct role time is taking in the structuring of the system. Here we assume that a system is composed of a partially ordered finite set of time bands.

A band is primarily represented by a granularity. System activities are placed in some band B if they engage in significant events at the time scale represented by B. For any system there will be a highest and lowest band that gives a temporal system boundary – although there will always be the potential for larger and smaller bands. By convention the lower bands have the finer granularity. Time has both discrete and continuous characteristics within each band of the framework.

The second defining characteristic of a band is its precision. This allows non-determinacy in specifications. The degree of ‘tolerance’ over any time statement within the band is the precision of the band. Of course the precision of a band can only be measured in a lower band when the units of the precision can be articulated within the granularity of that band.

It is usual within temporal and real-time logics to distinguish between actions that take time and those that are instantaneous. Within a band, the framework defines activities to have duration whilst events are instantaneous — “take no time in the band of interest”. Activities are performed by agents (human or technical). In some bands all agents will be artificial, at others all human, and at
others both will be evident. Some agents will work across bands.

In the specification of a system, an event may cause a response ‘immediately’ – meaning that at this band the response is within the granularity of the band. This helps eliminate the problem of over specifying requirements that is known to lead to implementation difficulties. For example, the requirement ‘when the fridge door opens the light must come on immediately’ apparently give no scope for an implementation to incorporate the necessary delays of switches, circuitry and the light’s own latency. By making the term ‘immediate’ band specific, it enables a finer granularity band to include the necessary delays, latencies and processing time that are needed to support the immediate behavior at the higher band. The obligation on this lower band is to deliver the behavior within the precision of the higher bands – so its ‘instantaneous’ property is maintained. Hence, events that are instantaneous in some band may map to activities that have duration at some lower band with a finer granularity. The key relationship between bands, that allows it to support system decomposition and modeling, is that within any band: activities in lower (faster) bands are assumed to be instantaneous and the state of activities in higher (slower) bands are assumed to be static (unchanging).

Most of the detailed behavior of the system will be specified or described within bands. Issues of concurrency, resource usage, scheduling and planning, response time (duration) prediction, temporal validity of data, control and knowledge validity (agreement) may be relevant at any band. We do note however that with human agents (and potentially with artificial learning agents) time itself within a band will play a central role. Time is not just a parameter of a band but a resource to be used/abused within the band. Users will interpret system behavior from temporal triggers. In particular the duration of an activity will be a source of knowledge and possibly misconceptions; and may be used to give validity (or not) to information, or to infer failure.

In all bands, a common set of temporal phenomena and patterns of behavior are likely to be exhibited by the system itself or its environment. For example, periodic (or regular or cyclic) activities, event handling (responding to an event by a deadline), temporal reasoning (planning and scheduling), interleaving and multi-tasking (and other aspects of concurrency), pausing (or delaying), analysis of response (or completion) time, deadline driven activities, and various aspect of dynamic behavior such as rates of change. Whilst evident in all bands, these phenomena are not identified using the same terminology in the various time bands of interest (i.e., in the technical, psychological and sociological literature). In all complex systems unforeseen emergent properties will also occur. But by analyzing the existence and nature and mapping and the patterns of event firing it may be possible to gain some level of predictability concerning emergence.

In this short paper we have argued that complex systems exhibit behavior at many different time levels and that a useful aid in describing and specifying such behavior is to use time bands. Viewing a system as a collection of activities within a finite set of bands is an effective means of separating concerns and identifying inconsistencies between different ‘layers’ of the system. Time bands are not mapped on to a single notion of physical time. Within a system there will always be a relation between bands but the bands need not be tightly synchronized. There is always some level of imprecision between any two adjacent bands. Indeed the imprecision may be large in social systems and be a source of dependability (robustness).

In developing key abstractions and architectural structures for Cyber-Physical system, we believe that the time bands notion has a number of useful features to offer. The need to develop a layered approach is identified in the Call. Any layering must recognize the different temporality exhibited by these systems.