Mixed Criticality Systems - A Review*

Alan Burns and Robert I. Davis
Department of Computer Science,
University of York, York, UK.
email: {alan.burns, rob.davis}@york.ac.uk

Abstract

This review covers research on the topic of mixed criticality systems that has been published since Vestal’s 2007 paper. It covers the period up to and including July 2015. The review is organised into the following topics: introduction and motivation, models, single processor analysis (including job-based, hard and soft tasks, fixed priority and EDF scheduling, shared resources and static and synchronous scheduling), multiprocessor analysis, related topics, realistic models, formal treatments, and systems issues. An appendix lists funded projects in the area of mixed criticality.

*Sixth edition, 1/8/2015.
### Contents

1 Introduction .......................... 3

2 Mixed Criticality Models .......... 5

3 Single Processor Analysis ...... 7
   3.1 Job scheduling .................. 7
   3.2 Fixed Priority Scheduling .... 7
      3.2.1 RTA-Based approaches ... 7
      3.2.2 Slack scheduling .......... 11
      3.2.3 Period transformation ... 12
   3.3 EDF Scheduling ................ 13
   3.4 Shared Resources ............... 14
   3.5 Static and Synchronous Scheduling . . 15
   3.6 Varying Speed Processors ... 16

4 Multiprocessor Analysis .......... 16
   4.1 Task Allocation ................ 17
   4.2 Schedulability Analysis ....... 18
   4.3 Communication and other Resources .... 19

5 Links to other Research Topics ... 22
   5.1 Hard and Soft Tasks .......... 22
   5.2 Fault Tolerant Systems ......... 23
   5.3 Hierarchical Scheduling ...... 24
   5.4 Cyber Physical Systems ...... 25
   5.5 Probabilistic real-time systems .... 25

6 More Realistic MCS Models ...... 27

7 More Formal Treatments .......... 29
   7.1 Speedup Factors ............... 29
   7.2 Formal Language Issues ....... 30

8 Systems Issues .................... 30

9 Conclusion .......................... 33

10 Appendix - Projects .............. 35
1 Introduction

An increasingly important trend in the design of real-time and embedded systems is the integration of components with different levels of criticality onto a common hardware platform. At the same time, these platforms are migrating from single cores to multi-cores and, in the future, many-core architectures. Criticality is a designation of the level of assurance against failure needed for a system component. A mixed criticality system (MCS) is one that has two or more distinct levels (for example safety critical, mission critical and low-critical). Perhaps up to five levels may be identified (see, for example, the IEC 61508, DO-178B, DO-254 and ISO 26262 standards). Typical names for the levels are ASILs (Automotive Safety and Integrity Levels), DALs (Design Assurance Levels) and SILs (Safety Integrity Levels). It should be noted that not all papers on MCS assign to ‘criticality’ the same meaning, an issue explored by Graydon and Bate [116].

Most of the complex embedded systems found in, for example, the automotive and avionics industries are evolving into mixed criticality systems in order to meet stringent non-functional requirements relating to cost, space, weight, heat generation and power consumption (the latter being of particular relevance to mobile systems). Indeed the software standards in the European automotive industry (AUTOSAR1) and in the avionics domain (ARINC2) address mixed criticality issues; in the sense that they recognise that MCS must be supported on their platforms.

The fundamental research question underlying these initiatives and standards is: how, in a disciplined way, to reconcile the conflicting requirements of partitioning for (safety) assurance and sharing for efficient resource usage. This question gives rise to theoretical problems in modeling and verification, and systems problems relating to the design and implementation of the necessary hardware and software run-time controls.

A key aspect of MCS is that system parameters, such as tasks’ worst-case execution times (WCETs), become dependent on the criticality level of the tasks. So the same code will have a higher WCET if it is defined to be safety-critical (as a higher level of assurance is required) than it would if it is just considered to be mission critical or indeed non-critical. This property of MCS significantly modifies/undermines many of the standard scheduling results. This report aims to review the research that has been published on MCS.

The first paper on the verification of a Mixed Criticality System used an extension of standard fixed priority (FP) real-time scheduling theory, and was published by Vestal (of Honeywell Aerospace) in 2007 [257]3. It employed a somewhat re-

\[\text{http://www.autosar.org/}\]

\[\text{http://www.arinc.com/}\]

\[\text{The term Mixed Criticality had been used before 2007 to address issues of non-interference in}\]
strictive work-flow model, focused on a single processor and made use of Response Time Analysis [12]. It showed that neither rate monotonic [180] nor deadline monotonic [169] priority assignment was optimal for MCS; however Audsley’s optimal priority assignment algorithm [10] was found to be applicable.

This paper was followed by two publications in 2008 by Baruah and Vestal [42], and Huber et al. [145]. The first of these papers generalises Vestal’s model by using a sporadic task model and by assessing fixed job-priority scheduling and dynamic priority scheduling. It contains the important result that EDF (Earliest Deadline First) does not dominate FP when criticality levels are introduced, and that there are feasible systems that cannot be scheduled by EDF. The latter paper addresses multi-processor issues and virtualisation (though it did not use that term). It focused on AUTOSAR and resource management (encapsulation and monitoring) with time-triggered applications and a trusted network layer.

Further impetus to defining MCS as a distinct research topic came from the white paper produced by Barhorst et al. [15], the Keynote talk that Baruah gave at the 2010 ECRTS conference[^4] and a workshop report from the European Commission [251]. These have been followed up by tutorials on MCS at ESWeek in 2012 and 2013[^5], a workshop at HiPEAC in January 2013[^6], a workshop (WICERT) at DATE 2013[^7], a workshop (ReTiMiCS) at RTCSA 2013[^8], workshops (WMC) at both RTSS 2013[^9] and RTSS 2014[^10], a workshop at the 19th International Conference on Reliable Software Technologies (Ada-Europe) in June 2014, and a full Dagstuhl School on Mixed Criticality and Many Core Platforms in March 2015[^11].

This review [61] is organised as follows. In Section 2 we first consider mixed criticality models. Then in Section 3 single processor systems are covered (including fixed priority and EDF scheduling). Section 4 covers multiprocessor issues and Section 5 links this research to other topics such as hard and soft real-time scheduling and hierarchical scheduling. More realistic models are covered in Section 6, more formal work is covered in Section 7 and systems work is covered in Section 8.

[^5]: Embedded Systems Week: http://www.esweek.org/
[^7]: http://ateproyectos.ugr.es/wicert/index.php/conference-proceedings
[^8]: http://igm.univ-mlv.fr/rtalgo/Events/RETIMICS/
[^9]: http://www.cs.york.ac.uk/robdavis/wmc/
[^10]: http://www.cs.york.ac.uk/robdavis/wmc/
[^11]: http://www.dagstuhl.de/15121
Conclusions are presented in Section 9. A short review of existing projects related to MCS is contained in an appendix.

2 Mixed Criticality Models

Inevitably not all papers on mixed criticality have used the same system or task model. Here we define a model that is generally applicable and is capable of describing the main results considered in this review.

A system is defined as a finite set of components $K$. Each component has a level of criticality (designated by the systems engineer responsible for the entire system), $L$, and contains a finite set of sporadic tasks. Each task, $\tau_i$, is defined by its period (minimum arrival interval), deadline, computation time and criticality level: $(T_i, D_i, C_i, L_i)$. Tasks give rise to a potentially unbounded sequence of jobs.

The primary concern with the implementation of MCS is one of separation. Tasks from different components must not be allowed to interfere with each other. In particular, mechanisms must be in place to prevent a job from executing for more than the computation time $C$ defined for its task, and to ensure that a task does not generate jobs that are closer together than $T^{12}$.

The requirement to protect the operation of one component from the faults of another is present in all systems that host multiple applications. It is however of particular significance if components have different criticality levels. Since without such protection, all components would need to be engineered to the strict standards of the highest criticality level, potentially massively increasing development costs.

After concerns of partitioning comes the need to use resources efficiently. This is facilitated by noting that the task parameters are not independent, in particular the worst-case computation/execution time estimate, $C_i$, will be derived by a process dictated by the criticality level. The higher the criticality level, the more conservative the verification process and hence the greater will be the value of $C_i$. This was the observation at the heart of the paper by Vestal [257].

For systems executing on hardware platforms with deterministic behaviour, any particular task will have a single real WCET (worst-case execution time); however, this value typically cannot be known with complete certainty. This uncertainty is primarily epistemic (uncertainty in what we know, or do not know, about the system) rather than aleatory (uncertainty in the system itself). Although it is reasonable to assume confidence increases (i.e. uncertainty decreases) with larger estimates of worst-case execution time, this may not be universally true [116]. It would certainly be hard to estimate what increase in confidence would result from, say, a 10% increase in all $C$s.

\[ T^{12} \] Or (period minus release jitter) if that is part of the task model.
For systems executing on hardware platforms with time-randomised hardware components [70], then a probabilistic WCET (pWCET) [6, 80, 88, 97] can be obtained. The exceedance function for this probability distribution defines for any specific probability, derived from a required maximum failure rate associated with a criticality level, an execution time budget which has no greater probability of being exceeded on any given run [79]. The pWCET distribution therefore effectively defines different estimates of the WCET budget for the same task, for different criticality levels due to their different requirements on the maximum tolerable failure rate.

The focus on different computation times was extended to task periods in subsequent papers [25, 28, 34, 57]. Here tasks are event handlers. The higher the criticality level the more events must be handled, and hence the task must execute more frequently even if it does not execute for longer.

In MCS a task is now defined by: \((\vec{T}, D, \vec{C}, L)\), where \(\vec{C}\) and \(\vec{T}\) are vectors of values – one per criticality level, with the constraints:

\[
L_1 > L_2 \Rightarrow C(L_1) \geq C(L_2)
\]

\[
L_1 > L_2 \Rightarrow T(L_1) \leq T(L_2)
\]

for any two criticality levels \(L_1\) and \(L_2\).

Note the completion of the model, by making \(D\) criticality dependent [34] has not as yet been addressed in detail. But it would have the constraint:

\[
L_1 > L_2 \Rightarrow D(L_1) \geq D(L_2)
\]

So a task may have a ‘safety critical’ deadline and an early QoS deadline.

All three constraints have the property that a task can progress from satisfying both its \(L_1\) and \(L_2\) parameters to satisfying only its \(L_1\) constraints (for \(L_1 > L_2\)).

Another feature of many of the papers considered in this review is that the system is defined to execute in a number of criticality modes. A system starts in the lowest criticality mode. If all jobs behave according to this mode then the system stays in that mode. But if any job attempts to execute for a longer time, or more frequently, than is acceptable in that mode then a criticality mode change occurs. Ultimately the system may change to the highest criticality mode.

Some papers allow the criticality mode to move down as well as up, but others (indeed the majority) restrict the model to increases in criticality only. We return to this issue in Section 6.

Finally, many papers restrict themselves to just two criticality levels; high (HI) and low (LO) with \(HI > LO\). These are referred to as dual-criticality systems.
Where modes are used, the system is either in a \textit{LO}-criticality mode or a \textit{HI}-
criticality mode. And the set of task parameters is typically: \((T_i, D_i, C_i(\textit{HI}), C_i(\textit{LO}), L_i)\). At the other extreme from just two criticality modes are the models
presented by Ekberg et al. \cite{98,100,102} in which any number of modes are allowed
and the movement between modes is represented by a directed acyclic graph.

3 Single Processor Analysis

Since Vestal’s 2007 paper \cite{257} there has been a series of publications. Most of
these papers address single processor platforms and independent components.

3.1 Job scheduling

Initially a number of papers considered the restricted problem of scheduling, on
a single processor, a finite set of mixed criticality jobs with criticality dependent
execution times \cite{24, 29, 31, 39, 41, 120, 171, 172, 202, 233, 234}. This work has,
however, largely been superseded by work on the more widely applicable task
model.

3.2 Fixed Priority Scheduling

In this section we look at MCS schemes that are based on applying Response-Time
Analysis (RTA), then those that consider slack scheduling and finally approaches
that are derived from period transformations.

3.2.1 RTA-Based approaches

Vestal’s approach was formalised (i.e. proof that the use of Audsley’s priority
assignment algorithm \cite{10} was optimal) by Dorin et al. \cite{93} in 2010. They also
extended the model to include release jitter, and showed how sensitivity analysis
could be applied.

Vestal’s approach allowed the priorities of high and low criticality tasks to be
interleaved, but all tasks had to be evaluated as if they were of the highest criticality.
By introducing monitoring of task execution time, and the prevention of execution
time over-runs, higher resource usage can be delivered \cite{34}. This is a crucial issue
in mixed criticality scheduling; by the introduction of more trusted components a
high utilisation of the available resources is facilitated.

In 2011 this approach was further extended \cite{36,57} to give a scheduling model
and associated analysis framework for a single processor system that dominates
all previous published analysis for MCS (using fixed priority scheduling) in that
it made better use of the processor and could schedule all systems that could be guaranteed by other approaches, plus many that could not. These papers were however restricted to just two criticality levels (or modes). The system’s run-time behaviour is either low-criticality (which relies on all execution times being bound by the low-criticality values and guarantees that all deadlines are met) or high-criticality (where only high criticality work is guaranteed but the rely condition is weakened – the bound on high-criticality execution times is increased). The system’s criticality change (from Low to High, i.e. \( LO \) to \( HI \)) is triggered by the observation, at run-time, that the stronger rely condition has been violated.

This change in criticality level has a number of similarities to systems that move between different operational modes (although there are also some significant differences [56, 116]). In the \( HI \)-criticality mode there are fewer tasks, but they have longer execution times or shorter periods. The literature on mode change protocols [64, 103, 205, 213, 229, 252, 253], however, highlights one important problem: a system can be schedulable in every mode, but not schedulable during a mode change [253]. This is also true for systems that change criticality levels.

An optimal priority ordering is defined in the paper from Baruah et al. [36] in that it maximises the priority of high criticality tasks, subject to the system being schedulable. Both the high and low criticality tasks are ordered via deadline (deadline monotonic) and a simplified version of Audsley’s algorithm is used to assign priorities from the lowest to the highest level. At each priority level the lowest priority task from the low criticality task set is tried first, if it is schedulable then the algorithm moves up to the next priority level; if it is not schedulable then the lowest priority task from the high criticality set is tested. If it is schedulable then again the algorithm moves on to the next level. But if neither of these two tasks are schedulable then the search can be abandoned as the task set is unschedulable. In total a maximum of \( 2N \) tests are needed (where \( N \) is the number of tasks in the system). Note that this result follows from work on robust priority assignment [86]. As each set of \( LO/HI \) criticality tasks can be viewed as additional interference on the other subset, an optimal priority ordering can be obtained with each subset in Deadline Monotonic priority order and a merge operation between them.

The protocol (dropping all \( LO \)-criticality work if any task executes for more than its \( C(LO) \) value\(^{15}\), the derived analysis and the use of optimal priority ordering is shown [36] to out-perform other schemes (in terms of success ratio for randomly generated task sets). The analysis is based on standard RTA (Response-Time Analysis). For any task, \( \tau_i \), first its \( LO \)-criticality response-time (\( R(LO) \))

\(^{13}\)A rely condition formalises the assumptions required for the guarantees to be valid [152].

\(^{14}\)Strictly, only \( 2N-1 \) tests are needed as the highest priority task must be schedulable as its computation time is less than its deadline.

\(^{15}\)First proposed by Baruah [24, 29].
is computed using LO-criticality parameters for all the tasks. A criticality switch must occur before this value if the task is to be impacted by the change, otherwise it will have completed execution. The worst-case response-time in the HI-criticality mode \(R(HI)\) is computed by noting that all LO-criticality tasks must be abandoned by time \(R(LO)\). The paper contains two methods for computing \(R(HI)\), one involves a single upper bound, the other looks at all the possible critically change points before \(R(LO)\) and computes the worst-case. The latter is more accurate, though still not exact; however, the gain is not significant and the simple upper bound test is probably sufficient in most cases.

To illustrate the above approaches one of the graphs from [36] is reproduced in Figure 1. This figure plots the percentage of task sets generated that were deemed schedulable for a system of 20 tasks, with on average 50% of those tasks having high criticality and each task having a high criticality execution time that is twice its low criticality execution time. The compared approaches are (from least effective to most effective): CrMPO which assigned priorities in criticality order, SMC-NO (static mixed criticality with no run-time monitoring) which is Vestal’s original approach, SMC which is an adaptation of Vestal’s approach in which LO-criticality tasks are monitored at run-time and are prevented from executing for more than \(C(LO)\), and AMC-rtb and AMC-max which are the two methods introduced in the previous paragraph (AMC for adaptive mixed criticality). In the graph the UB-H&L line bounds the maximum possible number of schedulable task sets. It serves to illustrate the quality of the AMC-max approach.

The AMC-rtb approach was extended by Zhao et al [269, 270] in 2013 to incorporate preemption thresholds [219] into the model. They demonstrated a reduction in stack usage and improved performance for some parameter ranges. Another approach to combining AMC-rtb and existing scheduling theory is taken by Burns and Davis [60]. They consider the use of deferred preemption [54, 83] and demonstrate a significant improvement over fully preemptive AMC-rtb. The gain in schedulability they demonstrate is obtained by having a final non-preemptive region (FNPR) at the end of each criticality (e.g. at the end of \(C(LO)\) and \(C(HI)\)), and by combining the assignment of priority and the determination of the size of this FNPR.

In keeping with a number of papers on MCS, the work of Baruah et al. [36] (and most of the subsequent modifications) restricted itself to dual criticality systems. Fleming and Burns [105] extended these models to an arbitrary number of criticality levels, focusing particularly on five levels as this is the maximum found in automotive and avionics standards. They observed that AMC-rtb remains a good approximation to AMC-max, and that AMC-max became computational expensive for increased levels. They concluded that AMC-rtb represented an adequate and effective form of analysis. A relatively minor improvement to AMC-max was
Figure 1: Percentage of Schedulable Task Sets

published by Huang et al. [137] (they termed it AMC-IA); however there may be cases where their analysis is optimistic. One characteristic of all the schemes defined above is that tasks do not change their priority after a criticality mode change. If priorities can change then a simple form of sufficient analysis is possible [19]. This work defines a new approach, PMC (priority may change). Evaluations show that PMC performs similarly to AMC-rtb, though neither dominates the other.

It was noted in the section on Mixed Criticality Models that the period parameter ($T$) can be criticality dependent as well as the worst-case execution time estimate ($C$). An application may consist of event handlers, and have different levels of constraint over the arrival patterns of the events. The higher the criticality, the closer together the events are assumed to arrive; and hence the smaller the $T$ parameter. Baruah and Chattopadhyay [20] have reformulated the SMC and AMC analysis (introduced above) to apply to this model, in which the $T$s rather than the $C$s vary with criticality. Their evaluation results show similar behaviour to that depicted in Figure 1. Criticality specific periods are also address by Burns and

---

16This is the topic of on-going discussions.
Davis [59], and by Zhang et al. [267] (who derived an improved analysis that they termed SAMC – Sufficient AMC).

### 3.2.2 Slack scheduling

An alternative approach to scheduling mixed criticality fixed priority systems is, for two level systems, to use a slack scheduling scheme in which low criticality jobs are run in the slack generated by high criticality jobs only using their low criticality execution budgets. This was first explored by Niz et al. [197]. One difficulty with this approach is to incorporate sporadic tasks. At what point can the ‘slack’ of a non-appearing sporadic task be allocated to low criticality jobs? Even for periodic tasks, ensuring schedulability of high criticality tasks in all circumstances is not straightforward. Niz et al. [197] compute the time at which a high criticality task must be released to ensure that it meets its deadline (a scheme similar to the dual-priority approach outlined in Section 5.1). However, Huang et al. [136] demonstrated that if a low criticality (high priority) task executes beyond its deadline, a high criticality (lower priority) task could miss its deadline. They show that either the low criticality task must be aborted at its deadline or (more practically) its priority must be reduced to a background level. They then derive safe analysis. Niz et al. have subsequently clarified their model (to remove the problem) and improved its performance [198, 199].

While slack is usually generated by tasks not executing for their full budget, it is also produced by the arrival of jobs being less frequent than anticipated in the worst-case. Neukirchner et al. [192, 193] adapt and extend a number of schemes for monitoring activation patterns. Their multi-mode approach is proved to be safe (no false negatives) and efficient (few false positives).

For a dual-criticality system $C(LO)$ values must, of course, be known. Once schedulability has been established however, it is possible to derive [222], using sensitivity analysis [48, 211], a scaling factor $F (F > 1)$ such that the system remains schedulable with all $C(LO)$ values replaced by $F \cdot C(LO)$. Using these scaled values at run-time will increase the robustness of the system, as the $LO$-criticality tasks will be able to execute for a greater time before a criticality change is triggered. Scaling can also be applied to the $C(HI)$ values. Volp et al. [259] look at an alternative means of obtaining $C(LO)$ and $C(HI)$ values; they do not consider them to be estimates of worst-case execution time, but budgets set by some design optimisation process.

As scaling involves changing a task’s computation time, and computation time influences priority assignment, it is possible to extend this approach by also allowing priorities to change as the system is made more robust [58].

Sciandra et al. [225] are extending and applying scaling factors to intelligent
transport systems. Issues of robustness are also addressed by Herman et al. [131].

3.2.3 Period transformation

As Vestal noted [257], an older protocol period transformation [227, 228] (PT), is also applicable to the mixed critically scheduling problem. Period transformation splits a task with period $T$ and computation time $C$ into two (or more) parts so that the task now has the parameters $T/2$ and $C/2$. Assuming all tasks have deadlines equal to their periods, the application of the optimal rate monotonic priority assignment scheme [180] will increase the relative priority of all transformed tasks. If all high criticality tasks are transformed so that their transformed periods are shorter than all low criticality tasks then the rate monotonic algorithm will deliver partitioned (i.e. criticality monotonic) priorities. All high criticality tasks will have priorities greater than all lower criticality tasks. The scheme can easily be extended to task sets with constrained deadlines ($D < T$). However, the scheme does introduce extra overheads from the increased number of context switches, and these could be excessive if there are low criticality tasks with short deadlines. A simple example of a period transformed task would be one with $T = D = 16$, $C(HI) = 8$ and $C(LO) = 4$; this task could be transformed to one with $T = D = 4$ and $C = 2$. Note, this is $C(HI)/4$, not $C(LO)/4$. The computation time is such that if the task executes according to its $HI$-criticality parameter it will take four invocations of the transformed task to complete, but if the $LO$-criticality assumption is valid it will only take two.

If overheads are ignored then Period Transformation performs well. Baruah and Burns postulate [35] (and prove for two tasks) that this is primarily due to the inherent property of PT to deliver tasks sets with harmonic periods (that are then more likely to be schedulable). It does not seem that PT is of specific benefit to MCS.

To split the code of a task, either a static code transformation process must be used or the run-time must employ an execution-time server. With code transformation, the programmer must identify where in the code the split should be made. This does not lead to good code modulisation and is similar to the problems encountered when functions must to be split into short sections so that they can be ‘packed’ into the minor cycles of a cyclic executive [65]. There is also the problem of OS locks being retained between slices of the code; making the protected resource unavailable to other tasks.

With a dual-criticality task such as the one in the example above the point at which the task can be assumed to have executed for two units of time is itself criticality dependent. This to all intents and purposes makes code transformation impractical. Therefore, if the code is not to be changed then a run-time server must be
used to restrict the amount of computation allowed per release of the (transformed) task. In practice this means that:

- Without PT, LO-criticality tasks may have high priorities and hence their execution times must be monitored (and enforced); HI-criticality tasks must also be monitored as they may need to trigger a criticality change if they execute for more than $C(LO)$ thereby triggering the abandonment of LO-criticality tasks.

- With PT, LO-criticality tasks have the lower priorities and hence they do not need to be monitored, HI-criticality tasks must be monitored to enforce the per release budget.

In general, there is less run-time intervention with PT. But recall there is considerably more task switching overhead if the periods of all HI-crit tasks are reduced to less than all LO-criticality task periods.

For multiple criticality levels a number of transformations may be required to generate a criticality monotonic ordering [105]. For example if there are three tasks (H, M, and L) with criticality levels implied by their names, and periods 5, 33 and 9. Then first M must be divided by 11 to get a period of 3 (so less than 9), but then H must be divided by 5 to move it below the new value for M. As a result the transformed periods become 1, 3 and 9. It also seems that the theoretical benefit of PT diminishes with an increased number of criticality levels [105].

3.3 EDF Scheduling

The first paper to consider MCS with EDF scheduling was Baruah and Vestal [42] in 2008. Park and Kim [202] later introduced a slack-based mixed criticality scheme for EDF scheduled jobs which they called CBEDF (Criticality Based EDF). In essence they use a combination of off- and on-line analysis to run HI-criticality jobs as late as possible, and LO-criticality jobs in the generated slack. In effect they are utilising an older protocol developed by Chetto and Chetto [72] for running soft real-time tasks in the ‘gaps’ produced by running hard real-time tasks so as to just meet their deadlines.

A more complete analysis for EDF scheduled systems was presented by Ekberg and Yi [99,125]. They mimicked the FP scheme by assigning two relative deadlines to each high criticality task. One deadline is the defining ‘real’ deadline of the task, the other is an artificial earlier deadline that is used to increase the likelihood of high criticality tasks executing before low criticality ones. At the point that the criticality of the system changes from low to high (due to a task exceeding its low criticality budget), all low criticality tasks are abandoned and the high criticality
tasks revert to their defining deadlines. They demonstrate a clear improvement over previous schemes [126]. Later work [100] generalises the model to include changes to all task parameters and to incorporate more than two criticality levels. Tighter analysis is provided by Easwaran [94], although it is not clear that the method will scale to more than two criticality levels. Further improvements are presented by Yao et al. [261]. They use an improved schedulability test for EDF (a scheme called QPA [266]), and a genetic algorithm (GA) to find better artificial deadlines.

A similar scheme was presented by Baruah et al. [17,33], called EDF-VD (EDF - with virtual deadlines). Again for a dual-criticality system, HI-criticality tasks have their deadlines reduced (if necessary) during LO-criticality mode execution. All deadlines are reduced by the same factor. They demonstrate both theoretically and via evaluations that this is an effective scheme. Note, however, that this scheme is not as general as those reported above [94,99,125]. In these approaches a different reduction factor is used for each task. Nevertheless the use of a single value does allow schedulability bounds to be derived (see Section 7).

EDF scheduling of MCS is also addressed by Lipari and Buttazzo [179] using a reservation-based approach. Here sufficient budget is reserved for the high criticality tasks, but if they only make use of what is assumed by their low criticality requirements then a set of low criticality tasks can be guaranteed. Again only two criticality levels are assumed. In effect low criticality tasks run in capacity reclaimed from high criticality tasks. Deadlines for the high criticality tasks are chosen to maximise the amount of capacity reclaiming.

A different approach to using spare capacity was derived by Su et al. [241,242] by exploiting elastic task model [67] in which the period of a task can change. They propose a minimum level of service for each LO-criticality task $\tau_i$ that is defined by a maximum period, $T_{max}^i$. The complete system must be schedulable when all HI-criticality tasks use their $C(HI)$ values and all LO-criticality tasks use their $C(LO)$ and $T_{max}^i$ values. At run-time if HI-criticality tasks use less than their full HI-criticality entitlement then the LO-criticality tasks can run more frequently. They demonstrate that for certain parameter sets their approach performs better than EDF-VD.

### 3.4 Shared Resources

With mixed criticality systems it is not clear to what extent data should flow between criticality levels. There are strong objections to data flowing from low to high criticality applications unless the high criticality component is able to deal with potentially unreliable data [226] – this happens with some security protocols [47]. Even with data flowing in the other direction there remains the schedul-
ing problem of not allowing a high criticality task to be delayed by a low criticality task that has either locked a shared resource for longer than expected or is executing at a raised priority ceiling level for too long.

Sharing resources within a criticality level is however a necessary part of any usable tasking model. In single criticality systems a number of priority ceiling protocols have been developed [14, 230]. These are beginning to be assessed in terms of their effectiveness for mixed criticality systems. Burns [55] extends the analysis for fixed priority systems by adding criticality specific blocking terms into the response-time analysis. He notes that the original form of the priority ceiling protocol (OPCP) [230] has some useful properties when applied to MCS. Resources can be easily partitioned between criticality levels and starvation of $LO$-criticality tasks while holding a lock on a resource can be prevented. With AMC-OPCP, a task can only suffer direct blocking if a resource is locked by a lower priority task of the same criticality.

For EDF-based scheduling Zhao et al. [269] attempt to integrate the Stack Resource Protocol (SRP) [14] and Preemption Threshold Scheduling with approaches to EDF scheduling that involve tasks having more than one deadline. This is not straightforward as these schemes assume that relative deadlines are fixed.

Alternative approaches are proposed by Lakshmanan et al. [162] by extending their single processor zero slack scheduling approach [197] to accommodate task synchronisation across criticality levels for fixed priority systems. They define two protocols: PCIP (Priority and Criticality Inheritance Protocol) and PCCP (Priority and Criticality Ceiling Protocol). Both of these contain the notion of criticality inheritance. This notion is also used by Zhao et al. [271] in their HLC-PCP (Highest-Locker Criticality Priority Ceiling Protocol) which they apply to the AMC scheduling scheme (see Section 3.2.1). For a dual criticality system they define three modes of execution, the usual two plus an intermediate mode which covers the time during which $LO$-criticality tasks are allowed to continue to execute if they are holding a lock on a resource that is shared with a $HI$-criticality task.

A more systematic scheme is proposed by Brandenburg [52]. Here all shared resources are placed in resource servers and all access to these servers is via a MC-IPC protocol. As a result only these servers and the support for the MC-IPC protocol have to be developed to the highest criticality level. Resource users can be of any criticality level, including non-critical.

### 3.5 Static and Synchronous Scheduling

The move between criticality levels can be captured in a static schedule by switching between previously computed schedules; one per criticality level. This is
explored by Baruah and Fohler [38]. Socci et al. [236] show how these Time-
Triggered (TT) tables can be produced via first simulating the behaviour one would
obtain from the equivalent fixed priority task execution. Construction of the tables
via tree search is addressed by Theis et al [248], and via the use of linear program-
mapping (LP) by Jan et al. [149]. For legacy systems Theis and Fohler [247] show
how an existing single table may be used to support MCS. A particularly simple
table driven approach is to use a cyclic executive, this is investigated by Burns et
al. [18, 62].

This use of tables is extended to synchronous reactive programs by Baruah [16,
26]. Here a DAG (Directed Acyclic Graph), of basic blocks that execute according
to the synchrony assumption, is produced that implements a dual-criticality pro-
gram. The synchronous approach is also considered by Yip et al. [262] and by
Cohen et al. [75]. The latter proving an application of mixed criticality from the
railway industry, and an example of why data needs to flow between criticality
levels.

3.6 Varying Speed Processors

Most analysis for MCS assumes a constant speed processor, but there are situa-
tions in which the speed of the processor is not known precisely (for example with
asynchronous circuitry). Baruah and Guo [21] consider power issues that could
lead to a processor having variable speed. As a processor slows down the execu-
tion time of the tasks increase. They simplify the model by assuming two basic
speeds, normal and degraded. At the normal speed a scheduling table is used; at
the degraded speed only HI-criticality jobs are executed and they use EDF. They
have extended this work [22, 127] to include a more expressive model and issues
of processor self-monitoring (or not).

Voltage scheduling, and thereby variable speed computation, is used by Huang
et al. [140, 141] to respond to a temporal overload – if a $C(HI)$ value is exceeded
and could lead to a LO-criticality task missing its deadline then energy is utilised
to enable the processor to reduce computation times. Overall, their approach aims
to reduce the system’s expected energy consumption.

4 Multiprocessor Analysis

The first paper to discuss mixed criticality within the context of multiprocessor
or multi-core platforms was by Anderson et al. [8] in 2009 and then extended in
2010 [189]. Five levels of criticality were identified; going from level-A (the high-
est) to level-E (the lowest). They envisaged an implementation scheme, which
they call $MC^2$, that used a cyclic executive (static schedule) for level-A, partitioned preemptive EDF for level-B, global preemptive EDF for levels C and D and finally global best-effort for level-E. They considered only harmonic workloads but allowed slack to move between containers (servers). Each processor had a container for each criticality level, and a two-level hierarchical scheduler (see Section 5.3). Later work from this group [73, 131] evaluates the OS-induced overheads associated with multiprocessor platforms. This framework is also used by Bommer [51] to support segmented mixed criticality parallel tasks. Parallel jobs are also considered by Liu et al. [181].

In the remainder of this section we first look at task allocation (with global or partitioned scheduling), then consider analysis and finally communications and other systems resources. We note that there has also been work on implementing mixed-criticality synchronous systems on multiprocessor platforms [27].

4.1 Task Allocation

The issue of allocation was addressed by Lakshmanan et al. [163] by extending their single processor slack scheduling approach [197] to partitioned multiprocessor systems employing a Compress-on-Overload packing scheme. Allocation in a distributed architecture was addressed by Tamas-Selicean and Pop [243–246] in the context of static schedules (cyclic executives) and temporal partitioning. They observed that scheduling can sometimes be improved by increasing the criticality of some tasks so that single-criticality partitions become better balanced. This increase comes at a cost and so they employ search/optimisation routines (Simulated Annealing [107, 244] and Tabu [243, 245]) to obtain schedulability with minimum resource usage. Search routines, this time GAs (Genetic Algorithms), are also used by Zhang et al. [268] to undertake task placement in security-sensitive MCS. Their objective is to minimise energy consumption “while satisfying strict security and timing constraints”. A toolset to aid partitioning is provided by Alonso et al. [5].

A more straightforward investigation of task allocation was undertaken by Kelly et al. [154]. They considered partitioned homogeneous multiprocessors and compared first-fit and best-fit approaches with pre-ordering of the tasks based on either decreasing utilization or decreasing criticality. They used the original analysis of Vestal to test for schedulability on each processor, and concluded that in general first-fit decreasing criticality was best.

A comprehensive evaluation of many possible schemes is reported by Rodriguez et al. [216]. They consider EDF scheduling and used the analysis framework of EDF-VD (see Section 3.3). One of their conclusions is the effectiveness of a combined criticality-aware scheme in which HI-criticality tasks are allocated Worst-Fit and LO-criticality tasks are allocated using First-Fit; both with Decreas-
ing Density. The same result is reported by Gu et al. [119]. They additionally note that if there are some very ‘heavy’ LO-criticality tasks (i.e. high utilisation or density) then space must be reserved for them before the HI-criticality tasks are allocated.

A global allocation scheme for MCS is proposed by Gratia et al. [115]. They adapt the RUN scheduler [214], which uses a hierarchy of servers, to accommodate HI and LO criticality tasks.

Between fully partitioned and fully global scheduling is the class of schemes termed semi-partitioned. This is being addressed by Bletsas and Petters [49, 50] and Al-Bayati et al. [2]. The latter work uses two allocations for their two criticality modes. HI-criticality tasks do not migrate. During a mode change, carry-over LO-criticality jobs are dropped and new LO-criticality jobs executing on a different processor are given extended deadlines/periods (i.e. they utilise the elastic task model).

With dual-criticality fault tolerant systems, a scheme in which high criticality tasks are replicated (duplicated) while low criticality tasks are not is investigated by Axer et al. [13] for independent periodic tasks running on a MPSoC (multi-processor system-on-chip). They provide reliability analysis that is used to inform task allocation.

A more theoretical approach (i.e. it is not directly implementable) is proposed by Lee et al. [164] with their MC-Fluid model. A fluid task model [135] executes each task at a rate proportional to its utilisation. If one ignores the cost of slicing up tasks in this way then the scheme delivers an optimal means of scheduling multiprocessor platforms. To produce a mixed criticality version of the fluid task model the fact that tasks do not have a single utilisation needs to be addressed. Lee et al. [164] do this and they also produce an implementable version of the model that performs well in simulation studies (when compared with other approaches).

### 4.2 Schedulability Analysis

For globally scheduled systems Li and Baruah [173] take a ‘standard’ multiprocessor scheme, fpEDF [23] and combine it with their EDF-VD approach (see Section 3.3). Evaluations indicate that this is an effective combination. Extensions of this work [37] compare the use of partitioning or global scheduling for MCS. Their interim conclusion is that partitioning is by far the most effective approach to adopt.

Notwithstanding this result, Pathan derives [203] analysis for globally scheduled fixed priority systems. They adopt the single processor approach [36] (see Section 3.2) and integrate this with a form of analysis for multiprocessor scheduling that is amenable to optimal priority ordering (via Audsley’s algorithm [10]).
They demonstrate the effectiveness of their approach (by comparing success ratios).

A different and novel approach to multi-core scheduling of MCS is provided by Kritikakou et al. [158, 160]. They identify that a HI-criticality task will suffer interference from a LO-criticality task running on a different core due to the hardware platform’s use of shared buses and memory controllers etc.. They monitor the execution time of the HI-criticality task and can identify when no further interference can be tolerated. At this point they abort the LO-criticality task even though it is not directly interfering. An implementation on a multi-core platform demonstrated effective performance of their scheme [160].

Extensions to deal with precedence constraints were given by Socci et al. [237] but only for jobs (not tasks).

4.3 Communication and other Resources

With a more complete platform such as a multiprocessor or System on Chip (SoC), perhaps with a NoC (Network-on-Chip), more resources have to be shared between criticality levels. The first design issue is therefore one of partitioning (as addressed above), how to ensure the behaviour of low criticality components does not adversely impact on the behaviour of higher criticality components. Pellizzoni et al. [206] in 2009 was the first to consider the deployment of mixed criticality systems (MCS) on multi-core and many-core platforms. They defined an Architectural Analysis and Design Language (AADL), a form of ADL (Architectural Description Language), for mixed criticality applications that facilitates system monitoring and budget enforcement of all computation and communication. Later Obermaisser et al. [201] introduce a system model with gateways and end-to-end channels over hierarchical, heterogeneous and mixed criticality networks.

For a bus-based architecture it is necessary to control access to the bus so that applications on one core do not impact unreasonably on applications on other cores (whether of different or indeed the same criticality level). Pellizzoni et al. [207] show that a task can suffer a 300% increase in its worst-case execution time due to memory access interference even when it only spends 10% of its time on fetching from external memory on a 8-core system. To counter this, Yun et al. [263] propose a memory throttling scheme for MCS. Kotaba et al [157] also propose a monitoring and control protocol to prevent processes flooding any shared communication media be it a bus or network. Kritikakou et al. [159] consider a scenario in which there are a few critical tasks that can suffer indirect interference from many lower critical tasks. They attempt to allow as much parallelism as possible - commensurate with the critical tasks retaining their temporal validity. Bounding the interference that a safety-critical task can suffer from lower criticality tasks using the same shared
communication resources on a multi-core platform is also addressed by Nowotsch et al. [200].

Within the time-triggered model of distributed computation and communication a mixed criticality system is often viewed as one that has both time-triggered and event-triggered activities (also referred to as synchronous and asynchronous) [210, 239]. The time-triggered traffic is deemed to have the highest criticality, the event-triggered traffic can be either just best-effort or can have some level of assurance if its impact on the system is bounded; what Steiner [239] calls rate-constrained. Protocols that support this distinction can be supported on networks such as TTEthernet. Another TDMA-based approach, though this time built into the Real-Time Ethernet protocol, is proposed by Carvajal and Fischmeister in their open-source framework, Atacama [69].

A reconfigurable SDRAM controller is proposed by Goossen et al. [113] to schedule concurrent memory requests to the same physical memory. They also use a TDMA approach to share the controller’s bandwidth. A key aspect of this controller is that it can adapt to changes in the run-time characteristics of the application(s). For example, a criticality mode change which should result in more bandwidth being assigned to the higher criticality tasks can be accommodated by what the authors call a use-case switch. Criticality aware DRAMs are also addressed by Jalle et al [148] in the context of a Space case study in which there are two criticality levels ‘control’ and ‘payload’.

Virtual DRAMS are adapted by Ecco et al. [96] to isolate critical tasks (which are guaranteed) from non-critical tasks that, although not guaranteed, do perform adequately. Each virtual device supports one critical task and any number of non-critical tasks. All critical tasks run on dedicated cores, and hence the only potential source of inter-criticality interference is from the interconnection fabric (bus). By use of virtual devices, the critical tasks benefit from interference-free memory access.

Kim at al. [155] propose a priority-based DRAM controller for MCS that separates critical and non-critical memory accesses. They demonstrate improved performance for the non-critical traffic. Note this work is focussed on supporting critical and non-critical traffic on the same memory banks (rather than mixed-criticality). A similar approach and result is provided by Goossens et al. [112] with their open-page policy.

Giannopoulou et al. [107, 108] use a different time-triggered approach. They partition access to the multiprocessor bus so that at any time, t, only memory accesses from tasks of the same criticality can occur. This may introduce some inefficiencies, but it reduces the temporal modelling of a mixed criticality shared bus to that of a single criticality shared bus. The latter problem is not, however, straightforward (but is beyond the scope of this review).
The problems involved in using a shared bus have lead Giannopoulou et al. to also include a Network-on-Chip (NoC) in their later work \[109\]. Baruah et al. \[18, 62\] apply a one criticality at a time approach to MCS scheduled by the use of a Cyclic Executive; they considered both partitioned and global allocation of jobs to frames.

Tobuschat et al. \[254\] have developed a NoC explicitly to support MCS. Their IDAMC protocol uses a *back suction* technique \[92\] to maximise the bandwidth given to low (or non) critical messages while ensuring that high-criticality messages arrive by their deadlines. The more familiar wormhole routing scheme \[196\] for a NoC has been expanded by Burns, Harbin and Indrusiak \[63, 146\] to provide support for mixed criticality traffic. Response-time analysis, already available for such protocols \[231\], is augmented to allow the size and frequency of traffic to be criticality aware.

An alternative to having a NoC be used for all traffic (task to task and task to off chip memory) is proposed by Audsley \[11\]. He advocates the use of a separate memory hierarchy to link each core to off chip memory. A criticality aware protocol is used to pass requests and data through a number of efficient multiplexers. If the volume of requests and data is criticality dependent then analysis similar to that used for processor scheduling can be used on this memory traffic.

Controller Area Network (CAN) \[110\] is a widely used network for real-time applications, particularly in the automotive domain. It has been the subject of considerable attention with Response-Time Analysis derived \[87\] for what is, in essence, a fixed priority non-preemptive protocol. The use of CAN in mixed criticality applications has been addressed by Burns and Davis \[59\]. In this work it is the period of the traffic flows and the fault model that changes between criticality levels. A MixedCAN protocol was developed that makes use of a Trusted Network Component that polices the traffic that nodes are allowed to send over the network. Evaluations are used to show the advantages of using MixedCAN rather than a criticality agnostic approach. However the paper, in keeping with many other publications, only considered dual-criticality systems.

Herber at al. \[130\] also addressed the CAN protocol. They replaced the physical network controller with a set of virtual controllers that facilitate spacial separation. A weighted round robin scheduler in then used to give temporal isolation. Their motivation is to support virtualisation in an automotive platform. They do not however use criticality specific parameters for the different applications hosted on the same device.

Other protocols that have been considered in terms of their support for mixed criticality systems include FlexRay \[114\] and switched Ethernet \[78\]. In the latter case, a change in criticality mode is broadcast to the entire system by adding a new field to the IEEE 1588 PTP (Precision Time Protocol).
A further communication protocol is addressed by Addisu et al. [1]. They consider JPEG2000 Video streaming over a wireless sensor network. With such a network the available bandwidth varies in an unpredictable way. They propose a bandwidth allocation scheme that is criticality aware. A wireless protocol (WirelessHART) is also used by Jin at al. [151] to support delay analysis with fixed priority scheduling.

5 Links to other Research Topics

5.1 Hard and Soft Tasks

Although the label ‘Mixed Criticality Systems’ is relatively new, many older results and approaches can be reused and reinterpreted under this umbrella term. In particular dual-criticality systems in which there are hard and soft tasks combined has been studied since at least 1987 [167]. Hard tasks must be guaranteed. Soft tasks are then given the best possible service. But soft tasks are usually unbounded in some sense (either in terms of their execution time or their arrival frequency) and hence they must be constrained to execute only from within servers (execution-time servers). Servers have bounded impact on the hard tasks. Since 1987 a number of servers have been proposed. The major ones for fixed priority systems being the Periodic Server, the Deferrable Server, the Priority Exchange Server (all described by Lehoczky et al. [167]), and the Sporadic Server [238]. The ability to run soft tasks in the slack provided by the hard tasks is also supported by the Slack Stealing schemes [82, 89, 166, 212] which have similar properties to servers. These all have equivalent protocols for dynamic priority (EDF) systems; and some EDF specific ones exist such as the Constant Bandwith server [177].

Since their initial specification, analysis has improved and means of allocating and sharing capacity between servers have been investigated (see for example [44, 45, 264]). However, these results on servers (and examples of how they can be implemented in Operating Systems and programming languages) are generally known (see standard textbooks [65, 68, 182]). And hence they are not reviewed in more detail here. Note however, that standard servers only deal with the isolation/partitioning aspect of MCS. To support sharing (of resources) there must be some means of moving capacity from the under utilised servers of high criticality tasks to the under provisioned servers of lower criticality tasks. The Extended Priority Exchange server [238] as well as work on making use of gain time, show how this can be achieved.

Another way of maximising the slack available for soft tasks is the dual-priority scheme [66, 90]. Here there are three bands of priority. The soft tasks run in the middle band while the hard tasks start in the lower band but are promoted to the
higher band at the latest possible time commensurate with meeting their deadlines. So hard task execute when they have to, or when there are no soft tasks, soft tasks run otherwise.

5.2 Fault Tolerant Systems

Fault tolerant systems (FTS) typically have means of identifying a fault and then recovering before there is a system failure. Various recovery techniques have been proposed including exception handling, recovery blocks, check-points, task re-execution and task replication. If, following a fault, extra work has to be undertaken then it follows that some existing work will need to be abandoned, or at least postponed. And this work must be less important than the tasks that are being re-executed. It follows that many fault tolerant systems are, in effect, mixed criticality.

To identify a fault, timeouts are often used. A job not completing before a deadline is evidence of some internal problem. Earlier warning can come from noting that a job is executing for more than its assumed worst-case execution time. Execution-time monitoring is therefore common in safety critical systems that are required to have at least some level of fault tolerance. Again this points to common techniques being required in FTS and MCS.

In was noted earlier, in the discussion on CAN (Section 4.3), that a fault model can be criticality dependent [59] – a task may, for example, be required to survive one fault if it is mission critical, but two faults if it is safety critical. The difference between assumed computation times at different criticality levels, may be a result of the inclusion or not of recovery techniques in the assumed worst-case execution time of tasks.

Although there is this clear link between FTS and MCS there has not yet been much work published that directly addresses fault-tolerant mixed criticality system. Exceptions being work by Huang et al. [143, 144] and a paper by Pathan [204] that both focus on service adaptation and the scheduling of fault-tolerant MCS. Work by Thekkilakattil et al. uses Zonal Hazard Analysis and Fault Hazard Analysis [250] and Error-Burst models [249] to deliver both flexibility and real-time guarantees (for the most critical tasks). Lin et al. [175] attempt to integrate mixed criticality with the use of primary and backup executions (in both of the two criticality modes they consider).

As highlighted already in this review, many models and protocols for mixed criticality behaviour allow the system to move through a sequence of mode (criticality modes). With a two mode system ($HI$ and $LO$) the system starts in the $LO$ mode in which all deadlines of all tasks are guaranteed, but can then transition to the $HI$ mode in which only the $HI$-criticality tasks are guaranteed (and the $LO$-
criticality tasks may actually be abandoned). It may, or may not, later return to the 
LO mode when it is safe to do so. Burns [56] attempts to compare these criticality 
mode changes with the more familiar system mode change. He concludes that the 
LO mode behaviour should be considered to be the ‘normal’ expected behaviour. 
A move away from this mode is best classified as a fault; with all other modes been 
considered forms of graceful degradation. A move back to the fully functional LO 
mode is closest in nature to an operational (sometime known as exceptional) mode 
change. Such a mode change is planned but may never occur.

5.3 Hierarchical Scheduling

One means of implementing a MCS where strong partitioning is needed between 
applications is to use a hierarchical (typically two-level) scheduler. A trusted base 
scheduler assigns budgets to each application. Within each application a secondary 
scheduler manages the threads of the application. There are a number of relevant 
results for such resource containment schemes (e.g. [71,84,85,178,218,265]). Both 
single processor and multiprocessor platforms can support hierarchical scheduling.

Unfortunately when hierarchical scheduling is applied to MCS there is a loss 
of performance [161]. A simple interface providing a single budget and replenish-
ment period (which is often associated with virtualisation or the use of a hypervi-
isor [4]) is too inflexible to cater for a system that needs to switch between criticality 
levels. To provide a more efficient scheme, Lackorznshi et al. [161] propose ‘flattening’ the hierarchy by exposing some of the interval structure of the scheduled 
applications. They develop the notion of a scheduling context which they apply 
to MCS [258]. In effect they assign more than one budget to each ‘guest’ OS. 
As a result, applications that would otherwise not be schedulable are shown to 
utilise criticality to meet all deadlines. An alternative, but still flexible approach, 
is provided by Groesbrink et al. [117,118]. They allow budgets to move between 
virtual machines executing on a hypervisor that is itself executing on a multi-core 
platform. The hypervisor controls access to the processor, the memory and shared 
I/O devices. Yet another scheme is described by Marinescu et al [185]; they are 
more concerned with partitioning as opposed to resource usage, but they do ad-
dress distributed heterogeneous architectures. Hypervisors are also used by Cilku 
and Puschner [74], to give temporal and spacial separation on a multiprocessor 
platform, and Perez et al. [208] use a hierarchical scheduler to statically partition 
a wind power mixed criticality embedded system requiring certification under the 
IEC-61508 standard. A hypervisor for a mixed criticality satellite software systems 
is discussed by Salazar et al. [220] and one for general control systems is addressed 
by Crespo et al [77].
5.4 Cyber Physical Systems

In parallel with the development of a distinct branch of research covering mixed criticality systems has been the identification of Cyber Physical Systems (CPSs) as a useful focus for system development. Not surprisingly it has been noted that many CPSs are also mixed criticality. For example Schneider et al. [224] note that many CPSs are a combination of deadline-critical and QoS-critical tasks. They propose a layered scheme in which QoS is maximised while hard deadline tasks are guaranteed. Izosimov and Levholt [147] use a safety-critical CPS to explore how metrics can be used to map potential hazards and risk from top level design down to mixed criticality components on a multi-core architecture.

Maurer and Kirner [186] consider the specification of cross-criticality interfaces (CCI) in CPSs that define the level of communication allowed between ‘open’ subsystems/components.

5.5 Probabilistic real-time systems

In mixed criticality systems, the worst-case execution time of a task is expressed as a function of the criticality level (e.g. $C(LO)$ and $C(HI)$) with larger values for the WCET obtained for higher criticality levels. Research into probabilistic hard real-time systems can be viewed as extending this model to a continuum (or at least a large number of discrete values). Instead of a number of single values for the WCET with different levels of confidence, the worst-case execution time is expressed as a probability distribution, referred to as a pWCET [46].

The exceedance function (or $1 - CDF$ \textsuperscript{17}) for the pWCET gives the probability that the task will exceed the specified execution time budget on any given run. Conversely, the exceedance function may be used to determine the execution time budget required such that the probability of overrunning that budget does not exceed a specified probability. This is illustrated in Figure 2. Here, an execution time budget of 55 has a probability of being exceeded on any single run of $10^{-5}$, whereas the execution time budget required to ensure that the probability of exceedance on any single run is at most $10^{-9}$ is 70. We note that exceedance probabilities and failure rates (e.g. $10^{-9}$ failure per hour) are not the same, but that such probabilities can be transformed into failure rates by accounting for the number of jobs in a given time period, or via probabilistic schedulability analysis techniques.

Probabilistic analysis provides an alternative treatment for mixed criticality systems, where high criticality tasks are specified as having an extremely low acceptable failure rate (e.g. $10^{-9}$ per hour), whereas a higher failure rate (e.g. $10^{-6}$ or $10^{-7}$ per hour) is permitted for lower criticality tasks. Probabilistic worst-case

\textsuperscript{17}Cumulative Distribution Function.
execution times [6, 70] and the probabilistic worst-case response times [91, 183] derived from them provide a match to requirements specified in this way. These techniques can potentially be used to show that pathological cases with very high execution times / high response times have a provably vanishingly low probability of occurring, thus avoiding the need to over-provision compute resources to handle these cases.

Just as MCS has expanded from a focus on worst-case execution times to one that includes arrival rates (for sporadic work), probabilistic analysis has been developed [3] for the case where the arrival rate of tasks is described by a probability distribution. This work could form a further link between MCS and probabilistic analysis.

Guo et al. [128] demonstrate the usefulness of a probabilistic framework in their analysis of an EDF scheduled system in which there is a permitted (but low) probability of timing faults. The chances of a HI-criticality task executing for more than its LO-criticality value is also expressed as a probability. Their current work assumes that task execution times are independent; this is an unrealistic assumption, but one that could be weakened in future work.
6 More Realistic MCS Models

The abstract behavioural model described in Section 2 has been very useful in allowing key properties of mixed criticality systems to be derived, but it is open to criticism from systems engineers that it does not match their expectations. In particular:

- In the HI-criticality mode, LO-criticality tasks should not be abandoned. Some level of service should be maintained if at all possible, as LO-criticality tasks are still critical.
- For systems which operate for long periods of time it should be possible for the system to return to the LO-criticality mode when the conditions are appropriate. In this mode all functionality should be provided.

It can be argued that these criticisms are, at least partly, misplaced as any high integrity system should remain in the LO-criticality mode for its entire execution: the transition to HI-criticality mode is only a theoretical possibility that the scheduling analysis can exploit [36]. Nevertheless, in less critical applications (such as those envisaged in the automotive industry) actual criticality mode changes may be experienced during operation and the above criticisms should be addressed.

To prevent the abandonment of all LO-criticality tasks following a criticality mode change a number of reconfigurations are possible:

1. Let any LO-criticality job that has started, run to completion (this is in effect what is assumed in many forms of analysis [36]).
2. Reduce priorities of the LO-criticality tasks [34], or similar with EDF scheduling [138, 139].
3. Increase the periods and deadlines of LO-criticality jobs [150, 240–242], called task stretching or the elastic task model.
4. Decrease the computation times of some or all of the LO-criticality tasks [58].
5. Abandon LO-criticality work in a disciplined sequence [106, 124, 142, 215].

The fourth approach leads to a modification to the system model; whereas for HI-criticality tasks we have $C(HI) \geq C(LO)$, for LO-criticality tasks we now have $C(HI) \leq C(LO)$. For some tasks $C(HI) = 0$, that is they are abandoned. For others a lower level of service can be guaranteed. For some they may be able to continue with their full computation time budgets.
The fifth approach is addressed by Fleming and Burns [106]; they introduce a further notion into the standard model; tasks are allocated to applications and each application is assigned (by the system designers) an importance level. LO-criticality tasks are abandoned in inverse order of importance. Huang et al. [142] also introduce an extension to the standard model by the use of an ICG (Interference Constraint Graph) to capture more specifically which tasks need to be dropped when particular higher criticality tasks exceed their allocated criticality-aware execution times.

Obviously all five schemes can be used together: complete all started jobs, allow some new jobs to have an extended deadline or reduced computation time, reduce the priorities of some others jobs and abandon those of lowest importance.

A flexible scheme utilising hierarchical scheduling is proposed by Gu et al. [95, 122, 123]. They differentiate between minor violations of LO-criticality execution time which can be dealt with within a component (an internal mode change) and more extensive violations that requires a system-wide external mode change. In doing so they introduce a new mixed-criticality resource interface model for component-based systems which supports isolation, virtualisation and conditionality.

In keeping with other mode change situations ([64,103,205,213,229,252,253]) a simple protocol for controlling the time of the change of mode back to LO-criticality is to wait until the system is idle (has no application tasks to run) and then the change can safely be made [252]. Santy et al. [223] extend this approach and produce a somewhat more efficient scheme that can be applied to globally scheduling multiprocessor systems (in which the system may never get to an idle tick). With a dual criticality system that has just transitioned into the HI-criticality mode (and hence no low-criticality jobs are executing); their protocol first waits until the highest priority HI-criticality job completes, then it waits until the next highest priority job is similarly inactive. This continues until the lowest priority job is inactive; it is then safe to reintroduce all LO-criticality tasks. Obviously if there is a further violation of the $C(LO)$ bound then the protocol is abandoned and subsequently restarted. The authors call this a SCR (Safe Criticality Reduction); their paper also has a second protocol, but this is less intuitive and considerably more expensive at run-time.

A more aggressive scheme for returning a system back to its LO-criticality mode is proposed by Bate et al. [43]. In this approach a bailout protocol is proposed. HI-criticality tasks take out a loan if they execute for more than their $C(LO)$ estimate. Other tasks repay the loan by either not executing at all or by executing for less than expected. When the loan is repaid (and a further condition is met) the system returns to its normal mode. They demonstrate, using a scenario-based assessment, that the bailout protocol returned the system to the normal mode.
much quicker than the ‘wait for idle tick’ scheme.

As well as experiencing a criticality mode change a system can, of course, be structured to behave in a number of operational or behavioural modes. As indicated earlier, Burns [56] compares and contrasts these two forms of mode change. De Niz and Phan [198] note that the criticality of a task can depend on the behavioural mode of the system. They develop scheduling analysis for this dependency and consider the static allocation of such tasks to multiprocessor platforms.

7 More Formal Treatments

In this section we consider speedup factors and (formal) language issues.

7.1 Speedup Factors

It has been shown [24, 26, 29, 31] that the mixed criticality schedulability problem is strongly NP-hard even if there are only two criticality levels. Hence only sufficient rather than exact analysis is possible. A list of open problems with regard to the schedulability of MCS is provided by Ekberg and Yi [101].

For approaches and tests that are only sufficient, an assessment of their quality is possible if a speedup factor can be computed. A speedup factor [153] of \( X (X > 1) \) for schedulability test \( S \) implies that a task set that is schedulable on a processor of speed 1 will be deemed schedulable by \( S \) if the processor’s speed is increased to \( X \). Of course, in general, it is not possible to know if the task set is schedulable on the original speed 1 processor (this would require an exact and possibly even a clairvoyant test), but a real scheduling scheme and test with a speedup factor of say 2 is clearly better than one with a speed up factor of 10.

For job-based fixed priority scheduling, a priority assignment scheme and test has been found [30, 31, 40, 172] with a speed up factor of \( S_L \) (for \( L \) criticality levels), where \( S_L \) is the root of the equation \( x^L = (1 + x)^L - 1 \). For \( L = 2 \) the result is \( S_2 = (1 + \sqrt{5})/2 \) which is equal to the golden ratio, \( \phi = 1.618 \). This can be compared with a partitioned approach (all HI-criticality jobs have priorities higher than all LO-criticality jobs) which has an unbounded speedup factor. This latter result is easily illustrated by considering a two job system. The LO-criticality job has a small computation time, 1, and deadline of 2. The HI-criticality job has a huge computation time of \( V \) and a deadline of \( V + 1 \). These two jobs will both meet their deadlines if the LO-criticality task is given the highest priority. But the reverse priority assignment (which executes the HI-criticality job first) will only be schedulable if \( V + 1 \) will fit into the deadline 2. To obtain this a speedup of \( (V + 1)/2 \) is required. As \( V \) can be arbitrary large the speedup factor is effectively...
unbounded.

For EDF scheduled systems Baruah et al. [33, 40] prove that a variant of EDF (EDF-VD, described in Section 3.3) in which HI-criticality sporadic tasks (in a dual-criticality system) have their deadlines reduced (in the LO-criticality mode) is also schedulable on a single processor that is speeded up by a factor $\phi$. They also show that a finite set of independent jobs scheduled on $m$ identical multiprocessors is schedulable with a speed-up factor of $\phi + 1 + 1/m$. And on a partitioned system a speed-up factor of $\phi + \epsilon$ is derivable for any value of $\epsilon > 0$. In later work [32] they improve this bound to $4/3$ (1.333) rather than $\phi$ (1.618). Further formal analysis of EDF-VD is provided by Li [170], Muller and Masrur [191] and Gu and Easwaran [121].

7.2 Formal Language Issues

The application of formal design languages, such as real-time BIT (Behavior Interactions Priorities), are being used to model MCS. And verification approaches such as model checking or simulation are being applied to both application software and multi-core platforms. See, for example, the work of Socci et al. [235]. State-space explosion is of course always an issue with these approaches.

A 2005 paper by Amey at al. [7], which predates Vestal’s work, looked at the (smart) certification of mixed criticality systems. They report real industrial application of formal code analysis to prove isolation between tasks of difference criticality levels. In one application, concerning safety-critical landing guidance for ship-borne helicopters, SIL 4 code (the highest in UK Defence Standard 00-55 [188]) was executing in the same processor and memory space as SIL3 and SIL2 code. Another application (a civil jet engine monitoring unit) have Level-C and Level-E code co-located (DO-178B standard [217] has levels A down to E). In both of these examples formal analysis of information flow at the program level was able to demonstrate code segregation.

Compile time checking is also advocated by Lindgren at al. [176] with their experimental RTFM-language. Language constructs allow static assessment of the interfaces between critical and non-critical code. At run-time however separation is achieved by assigning higher priorities to the critical tasks. As indicated earlier this is not a very effective strategy in terms of efficient resource usage.

8 Systems Issues

A fundamental issue with MCS is separation. Many of the more theoretical papers reviewed here assume various levels of run-time monitoring and control. However,
few papers consider or demonstrate how the required mechanisms can be implemented, Neukirchner et al. [194] presented one such paper. They consider memory protection, timing fault containment, admission control and (re-)configuration middleware for MCS. Their framework [104] is aimed at supporting AUTOSAR conforming applications within the automotive domain. An early paper looking at non-interference at the memory level for IMA platforms within the avionics industry is that of Hill and Lake [134].

Another detailed study of the overheads for two common implementations schemes for MCS is presented by Sigrist et al. [232]. They conclude that overheads of up to 97% can be encountered and they recommend that all scheduling models be extended to include parameters to capture the impact of run-time overheads.

The issue of monitoring is also addressed by Motruk et al. [190] in the context of their IDAMC (Integrated Dependable Architecture for Many Cores). This work builds on the more general (i.e. not MCS specific) work on separation, isolation and monitoring for SoC/NoC architectures. The MultiPARTES project (see Section 10) is addressing virtualisation in terms of Model Driven Engineering for MCS [4, 76, 255, 256]. Goossens et al. [111] are also looking at virtualisation “to allow independent design, verification and execution” with their CompSOC architecture. Paravirtualisation of legacy RTOSs to provide the necessary memory isolation is considered by Armbrust et al. [9].

The development of purpose built hardware (FPGA based) to support reliable MCS is being undertaken as part of the RECOMP project (see Section 10). They aim to reduce the cost of certification for MCS on multiprocessor architectures by use of open source hardware and software [187, 195, 209]. Santos et al. [221] are also looking at systems built on FPGA platforms. They have developed a criticality-aware scrubbing mechanism that improves system reliability by up to 79%. Scrubbing is a technique for recovering from SEU (single event upsets) that effect FPGA platforms in harsh environments such as space.

Many MCS papers have, either explicitly or implicitly, focused on issues of safety and reliability. Criticality can however also refer to security. Within this domain it is usual to have different security levels. And hence much of the extensive literature on security is relevant, but is out of scope of this review. Some work is nevertheless applicable to safety and security; for example the definition of a separation kernel for a system-on-chip built using a time-triggered architecture [260].

Such a separation kernel has been developed by Li et al. [174]. They can host guest operating systems, such as Linux but have their own real-time operating system (RTOS), QUEST-V. They partition the available cores into Sandboxes that have different criticality levels. Their architecture is aimed at achieving efficient resource partitioning and performance isolation.

Another high-assurance (micro) kernel is sel_4. Lyons and Heiser [184] show
how the sel_4 model can be extended to cater for mixed criticality.

To implement the criticality mode change the run-time support system must support execution time monitoring, the modes and mode changes. Baruah and Burns [34] show how this can be achieved within the facilities provided by the Ada programming language. Kim and Jin do the same for a standard RTOS [156]. They make use of bitmaps to provide a very efficient implementation.

A further operating system designed to support mixed criticality is Kron-OS [81]. This controls the execution of RSFs (Repetitive Sequence of Frames) that is partitioned between two criticality levels.

As an alternative to using an RTOS to give the right level of protection and (safe) resources sharing, Zimmer et al. [272] have designed a processor (Flex-PRET) to directly support MCS. They use fine-grained multithreading and scratch-pad memory to give protection to hard real-time tasks whilst increasing the resource utilisation of soft tasks. In effect soft tasks (threads) can safely exploit the spare capacity generated from the hard tasks at the cycle level. They have a soft-core FPGA implementation that caters for up to 8 hardware threads (each of which can support a number of software threads). A more focused scheme aimed at partitioning the cache is described by Lesage et al. [168].

Although research on MCS has generated many different approaches, there have been few empirical benchmarks or comparative studies. One useful study however was published in 2012 by Huang et al. [136]. They compared Vestal’s scheme with its optimal priority assignment, their improved slack scheduling scheme and Period Transformation (PT) (see Section 5.1). They conclude that Vestal’s approach and period transformation usually (though not always) outperform slack scheduling; and that there are additional overheads with period transformation and slack scheduling. Nevertheless the overheads were not excessive (typically an extra 0.3%). Later Fleming and Burns [105] compared Vestal’s approach, AMC (see Section 3.2) and PT for multiple criticality levels. As the number of criticality levels increased the relative advantage of PT, even when overheads are ignored, was observed to decrease. This observation was also supported, in 2014, by Huang et al. [137] who updated their study and concluded that AMC-based scheduling gave the best performance for fixed priority sporadic task systems. This study also looked at the overheads involved in user-space implementation of AMC on top of Linux, but without kernel modifications. The need for useful benchmarks is noted in a number of papers. One example, industrially inspired, case study is provided by Harbin et al. [129].

Another systems issue of crucial important in many mobile embedded systems is power consumption. The work of Broekaert et al. [53] allocates and monitors power budgets to different criticality levels. If a crucial VM (Virtual Machine) “overpassed its power budget during its time partition, the extra power consumed
will be removed from the initial power budget of the next low critical VM scheduled”. Energy consumption is also addressed by Legout et al. [165]. They trade energy usage with deadline misses (of low-criticality tasks), and claim a 17% reduction in energy with deadline misses kept below 4%. The objective of minimizing energy usage is used by Zhang et al. [268] to drive task allocation (in a multiprocessor system). As discussed earlier, a slightly different approach is taken by Huang et al. [140]. They advocate the use of DVFS (Dynamic Voltage and Frequency Scaling) to increase the speed of the processor if HI-criticality tasks need more than their \( C(LO) \) requirement. Hence LO-criticality work is not abandoned, but more energy is used. They integrate their approach with the EDF-VD scheduling scheme (see Section 3.3).

Complex mixed criticality systems also present a number of significant challenges at the specification and design stage. Herrera et al. [132, 133] propose a modelling and design framework for MCS hosted on Systems-on-Chip and/or Systems-of-Systems. They present a core ontology but freely admit that there is considerable work to do before a sound engineering process is available for system builders/architects.

9 Conclusion

As identified in the introduction, the fundamental issue with MCS is how to reconcile the differing needs of separation (for safety) and sharing (for efficient resource usage). These concerns have lead to somewhat of a bifurcation in the resulting research. Much of the implementation and systems work, in for example the funded projects (see the appendix), has concentrated on how to safely partition a system so that high integrity components can, in some way, share computational and communication resources. By comparison, the more theoretical and scheduling research has largely focused on how criticality-specific worst-case execution times can be utilised to deliver systems that are schedulable at each criticality level but have high processor utilisation.

Unfortunately these two areas of research are not easily integrated. Flexible scheduling requires, at least, dynamic partitioning. Certified systems require complete separation or at least static partitioning. Future work must address this mismatch.

A second topic for future work is a move away from a processor-centric view of MCS to one that incorporates other shared resources. For example communication – particularly on a multi-core or many-core platform. Can a shared bus provide the required separation, or is a Network-on-Chip protocol required? Work is only beginning to address these issues.
What becomes clear from reading the extensive literature that has been produced since Vestal’s paper, is that MCS presents a collection of interesting issues that are both theoretically intriguing and implementationally challenging. It is to be expected that MCS will continue to be a focus for practical and theoretical work for some time to come.

Acknowledgements

The authors would like to thank Sanjoy Baruah for a number of very useful discussions on the topic of this paper. The research that went into writing this paper is funded in part by the ESPRC grant, MCC (EP/K011626/1).
10 Appendix - Projects

This appendix outlines some of the publicly funded projects that have to some degree focused on MCS.

1. **MultiPARTES** is a research project aimed at developing tools and solutions for building trusted embedded systems with mixed criticality components on multicore platforms\(^{18}\). It is a collaborative EU FP7 ICT research project with 9 partners. A major outcome of the project is the *XtratuM*, an open source hypervisor designed as a generic virtualization layer for heterogeneous multicores. Project completed in 2013.

2. The **RECOMP** (Reduced certification cost for trusted multi-core platforms) research project aims to establish methods, tools and platforms for enabling cost-efficient certification and re-certification of safety-critical systems and mixed-criticality systems, i.e. systems containing safety-critical and non-safety-critical components\(^{19}\). It was a European funded project from the ARTEMIS Joint Undertaking. Project completed in 2013.

3. **ACROSS** is a research project that aims to develop and implement an ART-EMIS cross-domain reference architecture exploiting, for example, PikeOS, partitioning and time-triggered bus access protocols, for embedded systems based on the architecture blueprint developed in the EU FP7 project GENESIS\(^{20}\). Project completed in 2013.

4. **CERTAINTY** (Certification of Real Time Applications designed for mixed criticality) is an EU FP7 research project\(^{21}\). It aims to be a key enabler of the certification process for mixed-critical embedded systems featuring functions dependent on information of varying confidence levels. Such a certification process is particularly needed in the avionic, automotive and automation domains, where concurrent functions with real-time and safety-critical requirements are a reality.

5. **MCC** (Mixed Criticality Embedded Systems on Many-Core Platforms) is a UK funded (EPSRC) project looking at the design, verification and implementation of Mixed Criticality Systems\(^{22}\). It has a specific focus on developing NoC criticality-aware protocols.

\(^{18}\)http://www.multipartes.eu/
\(^{19}\)http://atc.ugr.es/recomp/
\(^{20}\)http://www.across-project.eu/
\(^{21}\)http://www.certainty-project.eu/
\(^{22}\)http://www.cs.york.ac.uk/research/research-groups/rts/mcc/
6. **PROXIMA** is an EU FP7 IP Project\(^{23}\). The PROXIMA thesis is that the temporal behaviour of mixed-criticality complex real-time embedded systems executing on multi-core and many-core platforms can be analysed effectively via innovative probabilistic techniques. PROXIMA defines new hardware and software architectural paradigms based on the concept of randomisation.

7. **CONTREX** (Design of embedded mixed-criticality CONTRol systems under consideration of EXtra-functional properties) focusses on platforms and addresses properties such as real-time, power, temperature and reliability\(^{24}\). It aims to develop meta-models for design and analysis.

8. **DREAMS** (Distributed REal-time Architecture for Mixed Criticality Systems) aims to produce a European reference architecture for mixed-criticality systems\(^{25}\).

9. **EMC\(^2\)** (Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments) is an ARTEMIS project with 100 (approx) partners is looking at open and adaptive systems.

\(^{23}\)http://www.proxima-project.eu/
\(^{24}\)https://contrex.offis.de/home/
\(^{25}\)http://www.dreams-project.eu/
References


