Scheduling and Voltage Scaling for Energy/Reliability Trade-offs in Fault-Tolerant Time-Triggered Embedded Systems

Pop, Paul; Poulsen, Kåre Harbo; Izosimov, Viacheslav; Eles, Petru

Published in:
Proceedings of the 5th International Conference on Hardware/Software Codesign and System Synthesis

Link to article, DOI:
10.1145/1289816.1289873

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
Scheduling and Voltage Scaling for Energy/Reliability Trade-offs in Fault-Tolerant Time-Triggered Embedded Systems

Paul Pop¹, Kåre Harbo Poulsen¹, Viacheslav Izosimov², Petru Eles²
¹Paul.Pop@imm.dtu.dk, s001873@student.dtu.dk
Informatics and Mathematical Modelling Dept.
Technical University of Denmark
DK-2800 Kongens Lyngby, Denmark
²viaiz | petel@ida.liu.se
Computer and Information Science Dept.
Linköping University
SE–581 83 Linköping, Sweden

ABSTRACT
In this paper we present an approach to the scheduling and voltage scaling of low-power fault-tolerant hard real-time applications mapped on distributed heterogeneous embedded systems. Processes and messages are statically scheduled, and we use process re-execution for recovering from multiple transient faults. Addressing simultaneously energy and reliability is especially challenging because lowering the voltage to reduce the energy consumption has been shown to increase the transient fault rates. In addition, time-redundancy based fault-tolerance techniques such as re-execution and dynamic voltage scaling-based low-power techniques are competing for the slack in the schedules. Our approach decides the voltage levels and start times of processes and the transmission times of messages, such that the transient faults are tolerated, the timing constraints of the application are satisfied and the energy is minimized. We present a constraint logic programming-based approach which is able to find reliable and schedulable implementations within limited energy and hardware resources.

Categories and Subject Descriptors
B.8.2 [Performance and Reliability]: Reliability, Testing, and Fault-Tolerance; C.3 [Special-Purpose and Application-Based Systems]: Real-Time and Embedded Systems

General Terms
Algorithms, Design, Performance, Reliability

Keywords
Embedded systems, Energy minimization, Reliability, Scheduling

1. INTRODUCTION
Safety-critical applications have to function correctly, meet their timing constraints and be energy-efficient even in the presence of faults. Such faults can be permanent (i.e., damaged microcontrollers or communication links), transient (e.g., caused by electromagnetic interference), or intermittent (appear and disappear repeatedly). The transient faults are the most common, and their number is increasing due to the raising level of integration in semiconductors.

Researchers have proposed several hardware architecture solutions, such as MARS [16], TTA [15] and XBW [6], that rely on hardware replication to tolerate a single permanent fault in any of the components of a fault-tolerant unit. Such approaches can be used for tolerating transient faults as well, but they incur very large hardware cost if the number of transient faults is larger than one. An alternative to such purely hardware-based solutions are approaches such as re-execution, replication, checkpointing.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ABSTRACT
In this paper we present an approach to the scheduling and voltage scaling of low-power fault-tolerant hard real-time applications mapped on distributed heterogeneous embedded systems. Processes and messages are statically scheduled, and we use process re-execution for recovering from multiple transient faults. Addressing simultaneously energy and reliability is especially challenging because lowering the voltage to reduce the energy consumption has been shown to increase the transient fault rates. In addition, time-redundancy based fault-tolerance techniques such as re-execution and dynamic voltage scaling-based low-power techniques are competing for the slack in the schedules. Our approach decides the voltage levels and start times of processes and the transmission times of messages, such that the transient faults are tolerated, the timing constraints of the application are satisfied and the energy is minimized. We present a constraint logic programming-based approach which is able to find reliable and schedulable implementations within limited energy and hardware resources.

Categories and Subject Descriptors
B.8.2 [Performance and Reliability]: Reliability, Testing, and Fault-Tolerance; C.3 [Special-Purpose and Application-Based Systems]: Real-Time and Embedded Systems

General Terms
Algorithms, Design, Performance, Reliability

Keywords
Embedded systems, Energy minimization, Reliability, Scheduling

1. INTRODUCTION
Safety-critical applications have to function correctly, meet their timing constraints and be energy-efficient even in the presence of faults. Such faults can be permanent (i.e., damaged microcontrollers or communication links), transient (e.g., caused by electromagnetic interference), or intermittent (appear and disappear repeatedly). The transient faults are the most common, and their number is increasing due to the raising level of integration in semiconductors.

Researchers have proposed several hardware architecture solutions, such as MARS [16], TTA [15] and XBW [6], that rely on hardware replication to tolerate a single permanent fault in any of the components of a fault-tolerant unit. Such approaches can be used for tolerating transient faults as well, but they incur very large hardware cost if the number of transient faults is larger than one. An alternative to such purely hardware-based solutions are approaches such as re-execution, replication, checkpointing.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CODES+ISSS '07, September 30–October 3, 2007, Salzburg, Austria.
Copyright 2007 ACM 978-1-59593-824-4/07/0009...$5.00.

233
slack with DVS, to tolerate transient faults. In [22] fault tolerance and
dynamic power management is studied, and rollback recovery with
checkpointing is used in order to tolerate multiple transient faults in
the context of distributed systems.

Addressing simultaneously energy and reliability is especially
challenging because lowering the voltage to reduce energy consump-
tion has been shown to exponentially increase the number of tran-
sient faults [23]. The main reason for such an increase is that, for
lower voltages, even very low energy particles are likely to create a
critical charge that leads to a transient fault. However, this aspect has
received very limited attention. Zhu [24] has proposed a reliability-
aware DVS greedy heuristic for single processors, while in [23] a sin-
gle-task checkpointing scheme is evaluated.

In [11] we have shown how re-execution and active replication can
be combined in an optimized implementation that leads to a schedula-
ble fault-tolerant application without increasing the amount of em-
ployed resources. In [12] we have addressed transparency/performance
trade-offs during the synthesis of fault-tolerant schedules. In this paper,
we consider a very different trade-off, namely, energy versus reliability.
To the best of our knowledge, we are the first to address such a trade-
off in the context of multiprocessor embedded systems.

We consider heterogeneous distributed time-triggered systems,
where both processes and messages are statically scheduled. The the
transient faults are tolerated through process re-execution by switch-
ing to pre-determined contingency schedules. In this context, we pro-
pose an approach to the scheduling and voltage scaling that decides
the voltage levels and start times of processes and the transmission
times of messages, such that the transient faults are tolerated, the tim-
ing constraints of the application are satisfied and the energy con-
sumption in the no-fault scenario is minimized. We propose a novel
constraint logic programming-based algorithm for the synthesis of
fault tolerant schedules that takes into account the influence of volt-
age scaling on reliability.

The next two sections present the system architecture and the appli-
cation model, respectively. The energy and reliability models are pre-
ented in Section 4. Section 5 presents our problem formulation, the
scheduling strategies considered, and a motivational example. Section 6
outlines the proposed scheduling and voltage scaling approach. The evalua-
tion of the proposed strategies is presented in Section 7.

2. SYSTEM MODEL

We consider architectures composed of a set $\mathcal{N}$ of DVS-capable
nodes which share a broadcast communication channel. The commu-
nication channel is statically scheduled such that one node at a time
has access to the bus, according to the schedule determined off-line.

We have designed a software architecture which runs on the CPU
in each node, and which has a real-time kernel as its main compo-
nent. The processes activation and message transmission is done
based on the local schedule tables.

In this paper we are interested in fault-tolerance techniques for tol-
erating transient faults, which are the most common faults in today’s
embedded systems. We have generalized the fault-model from [14]
that assumes that one single transient fault may occur on any of the
nodes in the system during the application execution. In our model, we
consider that at most $k$ transient faults may occur anywhere in the sys-
tem during one operation cycle of the application. Thus, not only sev-
eral transient faults may occur simultaneously on several processors,
but also several faults may occur on the same processor. The number of
$k$ transient faults correspond to a reliability goal $R_k$. We consider that
if the system reliability $R_k$ drops below the required reliability $R_{k'}$, then
the assumption of only $k$ transient faults occurring is no longer valid,
and $k' > k$ faults are likely to occur instead.

The error detection and fault-tolerance mechanisms are part of the
software architecture. We assume a combination of hardware-based
(e.g., watchdogs, signature checking) and software-based error detec-
tion methods, systematically applicable without any knowledge of the
application (i.e., no reasonableness and range checks) [13]. The soft-
ware architecture, including the real-time kernel, error detection and
fault-tolerance mechanisms are themselves fault-tolerant. In addition,
we assume that message fault-tolerance is achieved at the communi-
cation level, for example through hardware replication of the bus.

We use re-execution for tolerating faults. Let us consider a process
$P_i$ and a fault-scenario consisting of $k = 2$ transient faults that can
happen during one cycle of operation. The first execution runs at a
voltage level $V$. In the worst-case fault scenario, the first fault happens
during the process $P_i$’s first execution, and is detected by the error de-
tection mechanism, after a worst-case error detection overhead $\alpha_i$.
Once the error has been detected, the task has to be recovered. After a
worst-case recovery overhead of $\mu_i$, $P_i$ will be executed again. Since
we concentrate on minimizing the energy consumption in the no-fault
scenario, we consider that all the re-executions are performed at full
speed, i.e., at the maximum voltage $V_{\text{max}}$ and frequency $f_{\text{max}}$. Its sec-
ond execution in the worst-case could also experience a fault. Finally,
the third execution of $P_i$ will take place without fault. Note that the
overheads $\alpha_i$ and $\mu_i$ for a process $P_i$ are considered as part of its worst-
case execution time $C_i$.

3. APPLICATION MODEL

We model an application $\mathcal{A}(\mathcal{V}, \mathcal{E})$ as a set of directed, acyclic, polar
graphs $G_j(\mathcal{V}_j, \mathcal{E}_j) \in \mathcal{A}$. Each node $P_j \in \mathcal{V}$ represents one process. An
edge $e_{ij} \in \mathcal{E}$ from $P_j$ to $P_i$ indicates that the output of $P_j$ is the input
of $P_i$. A process can be activated after all its inputs have arrived and
it issues its outputs when it terminates. Processes are non-preemptable
and thus cannot be interrupted during their execution. Fig. 1 depicts an
application $\mathcal{A}$ consisting of a graph $G_1$ with five processes, $P_1$ to $P_5$.

The communication time between processes mapped on the same
processor is considered to be part of the process worst-case execution
time and is not modeled explicitly. Communication between processes
mapped to different processors is performed by message passing
over the bus. Such message passing is modeled as a communication
process inserted on the arc connecting the sender and the receiver
process, and is depicted with black dots in the graph in Fig. 1.

The mapping of a process in the application is determined by a
function $\mathcal{M}: \mathcal{V} \rightarrow \mathcal{N}$, where $\mathcal{N}$ is the set of nodes in the architecture. For
a process $P_j \in \mathcal{V}$, $\mathcal{M}(P_j)$ is the node to which $P_j$ is assigned for execu-
tion. We consider that the mapping is given, and we know the worst-
case execution time $C_i$ of process $P_i$, when executed on $\mathcal{M}(P_i)$. In
Fig. 1, the mapping is given in the table besides the application
graph. We also consider that the size of the messages is given.

All processes and messages belonging to a process graph $G_j$ have the
same period $T_j = T_{\text{rep}}$ which is the period of the process graph. If com-
municating processes are of different periods, they are combined into
a merged graph capturing all activations for the hyper-period (LCM
of all periods). A deadline $D_{\text{rep}} \leq T_{\text{rep}}$ is imposed on each process graph $G_j$.

4. ENERGY AND RELIABILITY MODELS

We use the power model from [5] which shows that by varying the
circuit supply voltage $V_{\text{bus}}$, it is possible to trade-off between power
consumption and performance. The reliability $R_j$ of a process $P_j$ is
defined as the probability of its successful execution, and it is cap-
tured by the exponential failure law [13]:

$$R_j = e^{-\lambda C_i}$$

where the term $\lambda$ is the failure rate, which describes the amount of er-
rors that will occur per second. For a system with the ability to handle
5. PROBLEM FORMULATION

The problem we are addressing in this paper can be formulated as follows. Given an application \( \mathcal{A} \) with a reliability goal \( R_g \) corresponding to \( k \) transient faults, mapped on an architecture consisting of a set of hardware nodes \( \mathcal{N} \) interconnected via a broadcast bus \( B \), we are interested to determine the schedule tables \( S \) such that the application is fault-tolerant, schedulable, and the energy of the no-fault execution scenario is minimized. Note that deciding on the schedule tables \( S \) simplifies deciding on both the start times and the voltage levels for each process.

5.1 Scheduling Strategies

The scaled execution of processes and the recovery slack needed for re-executions introduce delays that can violate the timing constraints of the application. In addition, reducing the voltage to decrease the energy consumption, has a negative impact on the application reliability.

Let us consider the example in Fig. 1, where we have an application consisting of five processes, \( P_1 \) to \( P_5 \), and two messages, \( m_1 \) and \( m_2 \), mapped on an architecture with two processors, \( N_1 \) and \( N_2 \). Processes \( P_1, P_2, P_3 \) and \( P_5 \) are mapped on \( N_1 \), and \( P_4 \) is mapped on \( N_2 \). Message \( m_1 \) is sent from \( P_1 \) to processes \( P_3 \) and \( m_2 \) from \( P_3 \) to \( P_4 \). The worst-case execution times of each process on its corresponding processor are depicted in the table, and the deadline of the application, depicted with a thick vertical line, is 215 ms. The voltage levels for each processor and reliability numbers \((d, \lambda_0)\) are also given in the figure. We consider a reliability goal \( R_g = 0.999999990 \) and \( k = 1 \).

In Fig. 1 we illustrate three scheduling strategies: (a) full transparency, (b) transparent recovery and (c) no transparency. For each alternative, on the left side \((a_1-c_1)\) we show the shortest possible schedule when no faults occur and no voltage scaling is performed. In case no voltage scaling is performed, the energy consumption \( E^0_{\mathcal{A}} \) and reliability \( R^0_{\mathcal{A}} \) of application \( \mathcal{A} \) do not depend the scheduling strategy. We would like to determine in \( a_2-c_2 \) schedules that minimize the energy consumption, and meet the deadline, even in the presence of faults. The right side \((a_3-c_3)\) depicts the worst-case fault scenario (resulting in the longest schedule) corresponding to the minimal energy schedules in \( a_2-c_2 \).

\[ R_t' = 1 - (1 - R_t) ^ {1+k} \tag{2} \]

where the last term is the probability of all processes failing in the same run. For independent faults, the reliability of \( \mathcal{A} \) is \([13]\):

\[ R_{\mathcal{A}} = \prod_{i=1}^{n} R_{t_i}' . \tag{3} \]

4.1 Energy/Reliability Trade-off Model

The equations presented so far do not account for the influence of voltage on reliability. However, lowering the voltage has been shown to dramatically lower the reliability \([23]\). Thus, the failure rate \( \lambda \) of a system is dependent on the voltage the system is run at. The relation between the two can be described by the expression proposed in \([23]\):

\[ \lambda(f) = \lambda_0 f \tag{4} \]

in which \( \lambda_0 \) is the failure rate of the processor when run at maximum voltage \( V_{\text{max}} \) and frequency \( f_{\text{max}} \), and \( f \) is an architecture specific constant. The variable \( f \) denotes the scaling factor, capturing both the voltage and the corresponding change in frequency. Equation 4 considers normalized voltages, i.e., \( V_{\text{max}} \) is assumed to be 1. Thus, for a scaling factor \( f \), the corresponding supply voltage is \( V_{\text{dd}} = f \times V_{\text{max}} \). Regarding frequency, for a small threshold voltage \( V_r \), the circuit delay becomes \( 1/V_{\text{dd}} = 1/f \).

Let us now return to the application reliability derived previously. Thus, the reliability of a single process, scaled with a factor \( f \) is:

\[ R_{t_i}'(f) = e^{-\lambda_0 f} \tag{5} \]

We can now update Equation 2 that captures the reliability of a process \( P_i \). Considering that all \( k \) recoveries are running at full speed (at \( f_{\text{max}} \), with a corresponding reliability \( R_{t_i}'(f) \)), the reliability of \( P_i \) is:

\[ R_{t_i}(f) = 1 - (1 - R_{t_i}') ^ {1+k} = 1 - (1 - e^{-\lambda_0 f}) ^ {1+k} \tag{6} \]

\[ \begin{aligned}
\text{Shortest schedule, no-fault scenario} & \quad \text{Deadline = 215} & \quad \text{Minimum energy schedule, no-fault scenario} & \quad \text{Worst-case scenario} \\
\text{Deadline = 215} & \quad \text{Energy = } E^0_{\mathcal{A}} & \quad \text{Energy = } E^0_{\mathcal{A}} & \quad \text{Energy = } E^0_{\mathcal{A}} \\
\text{Minimized} & \quad \text{Voltage levels } & \quad \text{Minimized} & \quad \text{Minimized}
\end{aligned} \]
Whenever a fault occurs, the faulty process has to be re-executed. Thus, the scheduler in a processor that experiences a fault has to switch to another schedule, containing a different start time for that process. For example, according to the schedule in Fig. 1a1, processes are scheduled at the times indicated by the light blue rectangles in the Gantt chart. Once a fault occurs in \( P_5 \), the scheduler on node \( N_1 \) will have to switch to another schedule, illustrated in Fig. 1a3, where \( P_3 \) is delayed with \( C_3 \) to account for the fault.

All the alternative schedules needed to run the application in case of faults are produced off-line by a scheduling algorithm. The end-to-end worst-case delay of an application is given by the maximum finishing time of any schedule, since this is a situation that can happen in the worst-case scenario. For the application in Fig. 1a1, the largest delay is produced by the schedule depicted in Fig. 1a3, which has to be activated when a fault happens in \( P_5 \).

Depending on how the schedule table is constructed, the re-execution of a process has a certain impact on the execution of other processes. In Fig. 1a1, we have constructed the schedule such that each execution of a process \( P_i \) is followed by a recovery slack, which is idle time on the processor, needed to recover (re-execute) the failed process. For example, for \( P_1 \) on node \( N_2 \), we introduce a recovery slack of \( k \times C_3 = 15 \text{ ms} \) to make sure we can recover \( P_3 \) even in the case it experiences the maximum number of \( k \) faults. Thus, a fault occurrence that leads to the re-execution of any process \( P_i \) will only impact \( P_i \), and not the other processes, since the re-execution time for \( P_i \) is already accounted in the schedule table. We call such an approach fully transparent, because fault occurrence in a process is transparent to all other processes, on the same, or on other processors.

The minimum energy in this case, corresponding to the schedule in Fig. 1a2 is 92.13% of \( E_0^A \). Note that this minimum energy schedule has to meet the deadline even in the worst-case fault scenario. Due to this, we are able to scale only \( P_1 \), at 66%, without missing the deadline. For such a limited voltage reduction, the reliability, calculated according to Equations (3) and (6), meets the reliability goal. Although transparency has the advantages of fault containment, improved debugability and less memory needed to store the fault-tolerant schedules [12], it will, however, introduce large delays that can violate the timing constraints of the application, and reduce the slack available for voltage scaling.

We would like a scheduling approach where the delay is reduced, thus increasing the slack available for voltage scaling. The straightforward way to reduce the end-to-end delay is to share the recovery slacks among several processes. For example, in Fig. 1b1, processes \( P_4 \) and \( P_5 \) share the same recovery slack on processor \( N_1 \). This shared slack has to be large enough to accommodate the recovery of the largest process (in our case \( P_3 \)) in the case of \( k \) faults. This slack can then handle \( k \) faults also in \( P_5 \), which takes less to execute than \( P_4 \).

In Fig. 1b we consider an approach called transparent recovery, where the fault occurring on one processor is masked to the other processors in the system, but not, as in the case with full transparency, within a processor. Thus, on a processor \( N_i \) where a fault occurs, the scheduler has to switch to an alternative schedule that delays the descendants of the faulty process running on \( N_i \). However, a fault happening on another processor, is not visible on \( N_i \), even if the descendants of the faulty process are mapped on \( N_i \). For example, in Fig. 1b1, where we assume that no faults occur, in order to isolate node \( N_i \) from the occurrence of a fault on node \( N_j \), message \( m_j \) from \( P_j \) to \( P_3 \), cannot be transmitted at the end of \( P_1 \)’s execution. \( m_j \) has to arrive at the destination at a fixed time, regardless of what happens on node \( N_i \), i.e., transparently. Consequently, the message can only be transmitted after a time \( k \times C_3 \), at the end of the recovery of \( P_1 \) in the worst-case scenario. However, a fault in \( P_1 \) will delay process \( P_2 \) which is on the same processor.

This approach will lead to a reduced delay, as depicted in Fig. 1b1. With this additionally available slack, we are able to perform voltage scaling on more processes, thus the minimum energy schedule is 49.68% of \( E_0^A \). However, for such a voltage scaling the reliability is reduced to 0.999 999 800 < \( R_g \), and the reliability goal is missed.

Another approach, depicted in Fig. 1c, is not to mask fault occurrences at all. In this case, even the processes on different processors will be affected by the fault occurrence on the current processor. For example, an error in \( P_1 \) on \( N_2 \) will have to be communicated to processor \( N_3 \) in order to switch to an alternative schedule that delays the scheduling of \( P_1 \) which receives message \( m_1 \) from \( P_1 \). This would create even more slack, leading to the schedule depicted in Fig. 1c2, that consumes only 33.96% \( E_0^A \), which is the largest obtainable energy reduction that does not violate the deadline. However, in this case the reliability of the system is further reduced to 0.999 999 787 < \( R_g \).

As the previous examples have shown, voltage scaling reduces reliability. The aim of this paper is to propose a schedule synthesis approach that is able to minimize the energy while at the same meeting the reliability and timing requirements. We will base our solution on the transparent recovery approach (Fig. 1b), which has been shown to quickly produce good quality schedules [11]. Thus, the scheduling algorithm is responsible for deriving offline the root schedules, i.e., the schedules in the no-fault scenario. The scheduler in each node, starting from the root schedule, based on the occurrence of faults, is able to derive online, in linear time, the necessary contingency schedule [11].

### 5.2 Motivational Example

Let us consider the example in Fig. 2 where we have an application of six processes mapped on an architecture of two nodes. All the relevant information is presented in the figure, similar to the previous example. Using transparent recovery, the shortest schedule without voltage scaling, is shown in Fig. 2a. The energy is \( E_0^A \), and the deadline of 260 ms and the reliability goal of 0.999 999 900 are met.

Optimizing the application for minimum energy consumption, with the deadline as a hard constraint, results in the schedule shown in Fig. 2b, where the energy consumed is 67.68% of \( E_0^A \). Process \( P_1 \) is running at voltage level of 33% of \( V_{max} \), \( P_3 \), and \( P_4 \) at 66%, while \( P_2 \) and \( P_5 \) are not scaled. In this case, the reliability is lowered to 0.999 999 878 which does not meet the reliability goal.

However, by carefully deciding on which processes are scaled and...
by how much, it is possible to reduce the negative impact on reliability without a significant loss of energy savings. Thus, in Fig. 2e, by choosing not to scale \( P_1 \) and starting \( P_3 \) before \( P_2 \) on \( N_2 \), we are able to reach a reliability of 0.999 999 920, which meets the reliability goal at an only 5.75% reduction in energy savings compared to the minimum energy schedule in Fig. 2b.

This example shows that reliability has to be considered at the same time with scheduling and voltage scaling. Our CLP-based schedule synthesis strategy is able to produce schedules with constrained reliability, which yield, as the experiments will show, energy savings comparable to schedules with unconstrained reliability.

6. CLP-BASED SYNTHESIS STRATEGY

The problem presented in the previous section is NP-complete (scheduling in even simpler contexts is NP-complete [21]). In this section we present a constraint logic programming (CLP) approach for solving the problem. Thus, a system is described by a set of logic constraints which define valid conditions for the system variables. A solution to the modelled problem is an enumeration of all system variables, such that there are no conflicting constraints.

The logic constraints used to model our problem fall under the following categories: (i) precedence constraints, (ii) resource constraints, (iii) timing, (iv) reliability and energy constraints, and (v) constraints for fault tolerance. Constraints (i)–(iii) have been extensively discussed in the literature [17]. The reliability and energy constraints (v) are captured by the equations introduced in the previous sections. Here we will concentrate on the constraints for fault tolerance.

6.1 Constraints for Fault Tolerance

When scheduling with fault tolerance using the transparent recovery technique, the precedence constraints have to take into account the recovery slack. There are two cases, treated separately.

1. Processes on the same node. Processes executed on the same processor share recovery slack. This slack is scheduled immediately after the processes, and thus will not impact the precedence constraints. Such a situation is depicted in Fig. 1b1, where \( P_1 \) and \( P_2 \) are mapped on the same processor, and share recovery slack. Thus, the constraint for processes on the same processing element is simply \( M(P_i) = M(P) \).

2. Processes on different nodes. Things are more complex if the two processes are mapped on different processors. In such a situation, a process cannot be started until the recovery of its predecessors on all other processors is guaranteed. The situation where two processes on different processors have to communicate, can be split into two special cases. These are illustrated in Fig. 3a and b, respectively.

Let us consider the dependency between processes \( P_2 \) and \( P_3 \). In Fig. 3a, \( P_3 \) is scheduled after \( P_1 \). The figure shows the critical recovery path. This is the path which determines when data is available to be transmitted. In this example the longest recovery path is \( k \) re-executions of \( P_2 \), and hence \( P_3 \) can start at time: \( \text{Start}(P_3) \geq \text{Start}(P_2) + \frac{C_2/f_2}{k} \times C_2 \). In Fig. 3b, \( P_2 \) is now scheduled after \( P_1 \) (\( P_1 \) has a larger execution time in this example). In this case, the longest recovery path to \( P_3 \) is \( k \) re-executions of \( P_1 \) plus a single execution of \( P_2 \).

That is, the availability of data is not only determined by the sending process, but also on all the processes with which the sending process shares slack. To generalize the shown constraints, in a way that can be used in the CLP model, detailed information of the recovery schedule is needed. This is achieved by creating a separate schedule for the recovery processes. For the examples shown in Fig. 3, the created recovery schedule is depicted in the Gantt chart entitled “re-execution schedule”.

The recovery schedule is set up in the following way. For each process \( P \), a recovery process \( S \) is inserted into the recovery schedule with an edge \( e_{P,S} \). In the recovery schedule the precedence and resource constraints are imposed. The finishing times of the processes in the recovery schedule are described by:

\[
\text{Finish}(S_i) \geq \text{Start}(P_j) + \frac{C_i/f_i^T}{k} \times C_i + C_j
\]

(7)

\[
\text{Finish}(S_i) \geq \text{Start}(S_j) + C_i
\]

Note that the first part of the expression, up to the “and” operator, captures the situation depicted in Fig. 3a. The rest relates to Fig. 3b.

Using the recovery schedule, the general logic constraint for processes on different processors can now be written: \( \text{Start}(P_j) \geq \text{Finish}(S_i) \). With the previous definitions of the recovery schedules and constraints for processes on the same, and on different processors, a general constraint for slack sharing can be derived:

\[
M(P_i) = M(P) \wedge \text{Start}(P_j) \geq \text{Start}(P_i) + \frac{C_i/f_i^T}{k} \vee \text{Finish}(S_i) \geq \text{Finish}(P_i)
\]

(8)

In the last part of the expression it is not stated that \( M(P_i) \neq M(P) \), as this is an implicit consequence of the first part of the clause.

7. EXPERIMENTAL RESULTS

For the evaluation of our techniques we used applications of 10, 15, 20, 25 and 30 processes mapped on architectures consisting of 3 nodes. Ten examples were randomly generated for each application dimension, thus a total of 40 applications were used for experimental evaluation. Execution times were assigned randomly within the 10 to 100 ms. We have ignored communications for the experiments. The failure rate constant has been set to \( d = 2 \) and the initial failure rate \( \alpha_0 = 10^{-6} \) faults per second. Half of the processes in the graphs have been randomly chosen to be made redundant using re-execution. The remainder of the processes are considered non-critical, and are not made redundant. We have used the ECL/PS' CLP system [1], version 5.10_44 on 3.5 GHz AMD 64-bit computers with two gigabytes of RAM. We have set a progressive time-out for each run, based on the application size, to 10, 15, 20, 25 and 30 minutes, respectively. The best result determined during each run has been used in the evaluations.

In the experiments, the fully transparent schedule without voltage scaling has been used as reference. This is a schedule that a designer would determine in a straightforward manner, by introducing an amount of \( k \times C_i \) recovery slack after each process \( P_i \). Let us call this approach Straightforward Solution, or SS. The deadline for the graphs in the experiments has been set to the length of the optimal SS schedule. The reliability goal has been set to: \( R_s = 1 - 10(1 - R_s^0)^k \), which means that the probability of faults happening may be no more than ten times greater than in the schedule without voltage scaling.

We have considered two situations, with \( k = 1 \) and \( k = 2 \).

We were first interested to determine the impact of voltage scaling on reliability. For this, we have applied our scheduling and voltage scaling optimization with the objective of minimizing the energy

![Figure 3. Fault-tolerance Constraints Example](image-url)
consumption, but without imposing any reliability constraints. Let us denote this approach with Energy Optimization, EO. The results, averaged over the 10 applications for each application size, are presented in Fig. 4 for $k = 1$ and 2. In the energy plots, Fig. 4a and c, we present the energy consumption obtained with EO relative to that of SS as the application size increases. The reliability plots in Fig. 4b and d present the absolute reliability of the approaches evaluated. As we can see from the figures, EO is able to obtain close to 40% energy savings compared to SS. These savings increase as $k$ increases. However, this is at the expense of a significant reduction in reliability, which drops rapidly as the application size and $k$ increase. For example, for an application of 30 processes and $k = 2$, the average reliability is below 0.87. Therefore, the reliability has to be addressed during scheduling and voltage scaling.

This was the focus of our second round of experiments. We have performed scheduling and voltage scaling with the goal of minimizing the energy as in EO, but we have additionally imposed the reliability constraint that the resulted system reliability has to be within the reliability goal $R_g$ (as set by Equation ). We have called this approach Reliable Energy Optimization (REO). As we can see in Fig. 4b and d, the reliability with REO no longer drops below $R_g$. Moreover, as Fig. 4a and c show, the energy savings of REO relative to SS are comparable to those of EO, which does not care about reliability. This means that our CLP-based scheduling and voltage scaling approach is able to produce reliable implementations without sacrificing the reduction in energy consumption.

We have also considered an MP3 encoder application [20]. The deadline for the application is 25 ms. The MP3 is executed on an architecture with two processing elements that can be run at three voltages: 1.5V, 0.7V, and 0.5V. We have shown that it is possible to eliminate the negative impact of voltage scaling on reliability without a significant loss of energy savings.

8. CONCLUSIONS

In this paper we have addressed the scheduling and voltage scaling for fault-tolerant hard real-time applications mapped on distributed embedded systems where processes and messages are statically scheduled.

We have captured the effect of voltage scaling on system reliability and we have shown that if the voltage is lowered to reduce energy consumption, the reliability is significantly reduced. Hence, we have proposed a CLP-based approach that takes reliability into account when performing scheduling and voltage scaling.

As the experimental results have shown, our CLP-based strategy is able to produce energy-efficient implementations which are schedulable and fault tolerant. By carefully deciding on the start times and voltages of processes we have shown that it is possible to eliminate the negative impact of voltage scaling on reliability without a significant loss of energy savings.

REFERENCES


Figure 4. Experimental Results