Erratum

Leonie Köhler (née Ahrendts), Sophie Quinton, Rolf Ernst

March 7, 2022

1 Introduction

This erratum relates to Ahrendts et al. [2018], a conference paper at ECRTS in 2018 with the title "Verifying Weakly-Hard Real-Time Properties of Traffic Streams in Switched Networks". The central contribution of the paper is the computation of (m,k)-guarantees for traffic streams in switched networks. An (m,k)-guarantee states that no more than m out k consecutive frame transmissions may violate the end-to-end deadline of a traffic stream. The authors discovered that the computed (m,k)-guarantees in their paper are in fact only valid under restrictive assumptions.

This introduction recalls the most important definitions of the paper by Ahrendts et al. [2018] and points out which parts of the computation of (m,k)-guarantees for traffic streams have been identified as faulty in the sense that they only apply under restrictive assumptions. In the subsequent sections of this erratum, the two erroneous theorems from Ahrendts et al. [2018] are discussed in detail. The conclusion of this erratum examines the impact of the discovered faults and points to corrected results in Köhler [2022].

A traffic stream s_i is modeled by an event-triggered task chain $(\tau_{i,1}, \tau_{i,2}, \ldots)$. The first task in the stream s_i, is activated by an external event source, while all successor tasks are activated by the termination events of their respective predecessor task in the chain. The event arrival of each task is described by an *event flow* $e_{i,j}(t)$. All possible event flows for a task are bounded from above by an *event model* $\eta^+_{i,j}(\Delta t)$.

Definition 1 (Event flow)**.** *An event flow $e_{i,j}(t)$ is a function which returns the number of events which activate task $\tau_{i,j}$ within the time interval $[0, t)$ in a given execution run.*

Definition 2 (Event model)**.** *The maximum event model $\eta^+_{i,j}(\Delta t)$ indicates an upper bound on the number of activation events for task $\tau_{i,j}$ in any time interval $[t, t + \Delta t)$. Any event flow $e_{i,j}(t)$ of task $\tau_{i,j}$ is therefore constrained by*

$$\forall t_1, t_2 : \; t_1 \leq t_2 : \; e_{i,j}(t_2) - e_{i,j}(t_1) \leq \eta^+_{i,j}(t_2 - t_1).$$

Ahrendts et al. [2018] deduce an (m,k)-guarantee for a task chain on the basis of the (m,k)-guarantees of each task in the task chain. An (m,k)-guarantee for an individual task is derived by applying principles of Typical Worst-Case Analysis as presented in Xu et al. [2015].

Typical Worst-Case Analysis introduces two event classes: typical events and overload events. If only typical events occur, the system is guaranteed to be schedulable. Overload events are the cause for potential deadline misses. A central element of the paper by Ahrendts et al. [2018] is therefore

1. to find a **valid decomposition of a given event flow** $e_{i,j}(t)$ into a typical event flow $e_{i,j}^{(t)}(t)$ and an overload event flow $e_{i,j}^{(o)}(t)$,
2. to find a typical event model $\eta_{i,j}^{+,(t)}(\Delta t)$ which bounds from above all possible typical event flows $e_{i,j}(t)$, and
3. to **find an overload event model** $\eta_{i,j}^{+,(o)}(\Delta t)$ which bounds from above all possible overload event flows $e_{i,j}^{(o)}(t)$.

The solutions for points 1+3 presented in the paper Ahrendts et al. [2018] are faulty. In fact, the related Theorems 22-23 are only valid under restrictive assumptions as will be discussed in Sections 3 and 4. Generic solutions can be found in Köhler [2022].

2 Notation

For better readability, this erratum will use reduced notations: The task index will suppressed, the superscripts and arguments are simplified. This is leads to the following expressions:

notation of the ECRTS 2018 paper	**notation of this erratum**
$e_{i,j}(t)$	$e(t)$
$e_{i,j}^{(t)}(t)$	$e^t(t)$
$e_{i,j}^{(o)}(t)$	$e^o(t)$
$\eta_{i,j}^{+}(\Delta t)$	$\eta^{+}(\Delta)$
$\eta_{i,j}^{+,(t)}(\Delta t)$	$\eta^{+,t}(\Delta)$
$\eta_{i,j}^{+,(o)}(\Delta t)$	$\eta^{+,o}(\Delta)$

3 Decomposing an Event Flow

The problem is to decompose an event flow $e(t)$ satisfying η^+ into a typical event flow e^t and an overload event flow $e^o(t)$ such that

1. each event in the event flow $e(t)$ satisfying η^+ must be identified as either typical or overload, and
2. the resulting typical event flow e^t, which counts the typical events in each time interval $[0, t)$, satisfies a given $\eta^{+,(t)}$.

For the resulting overload event flow $e^o(t)$, a maximum event model can be derived. This follow-up problem will be considered in Section 4.

Proposed Solution in Ahrendts et al. [2018] We will recall here the proposed decomposition in Ahrendts et al. [2018]. It is based on the notion of the sliding window function.

A sliding window function takes as input an event flow $e(t)$ defined up to time T and returns a maximum event model $\eta^+_{e,T}(\Delta t)$ stating how many events are at most contained in any interval of length $0 \leq \Delta t \leq T$ within the trace.

Definition 3 (Sliding window function)**.** *A sliding window function f_{slw} takes a specific event flow $e(t)$ defined on $0 \leq t \leq T$ as an input, and returns a maximum event model for $e(t)$, denoted as $\eta^+_{e,T}(\Delta t)$ for any interval size $0 \leq \Delta t \leq T$. This maximum event model $\eta^+_{e,T}(\Delta t)$ is derived by passing a window of size Δt over the event flow $e(t)$ of length T and noting down the maximum number events contained in any position of the window Δt such that*

$$\eta^+_{e,T}(\Delta t) = \max_{t_1,t_2\,:\,0\leq t_1\leq t_2\leq T\wedge t_2-t_1=\Delta t} \{e(t_2) - e(t_1)\}\,.$$

Theorem 22 from Ahrendts et al. [2018] describes the decomposition of an event flow as follows:

Theorem 22 (Decomposition of an event flow)**.** *Let $e(t)$ be an arbitrary event flow of length T. Known bounds are $\eta^+_{e,t}(\Delta t)$ for all (sub)lengths of the event flow with $0 \leq t \leq T$ and the maximum typical event model $\eta^{+,(t)}(\Delta t)$. A valid decomposition of $e(t)$ in a typical and overload event flow is given by*

$$e^{(o)}(t) = \max_{0\leq\Delta t\leq t} \left\{0,\ \eta^+_{e,\,t}(\Delta t) - \eta^{+,(t)}(\Delta t)\right\}$$
$$e^{(t)}(t) = e(t) - e^{(o)}(t).$$

In other words, Theorem 22 proposes the following algorithm to decompose an event flow $e(t)$ up to time instant t:

- Find the largest number of events in any time interval of size Δt with $0 \leq \Delta t \leq t$, denoted as $\eta^+_{e,\,t}(\Delta t)$.

- Check if in any interval of size Δt with $0 \leq \Delta t \leq t$ the maximum number of events exceeds $\eta^{+,(t)}(\Delta t)$ and select the largest positive deviation:

$$\max_{0 \leq \Delta t \leq t} \left\{ 0,\ \eta^{+}_{e,\,t}(\Delta t) - \eta^{+,(t)}(\Delta t) \right\}$$

- This largest deviation corresponds to the number of overload events in the $e(t)$ up to time instant t.
- All other events are typical events: $e^{(t)}(t) = e(t) - e^{(o)}(t)$.

Error in the proposed decomposition: limited applicability The proposed decomposition algorithm is not universally valid for all possible event flows $e(t)$ as stated in the theorem. Indeed, the decomposition algorithm is only applicable to very specific types of event flows. This restriction is closely related to how overload events are detected in Theorem 22. Multiple occurrences of overload events at different points in time are not properly considered, so that Theorem 22 covers event flows for which an overload event is known to occur only once:

Theorem (Decomposition of event flows with a single disturbance)**.** *Let an event flow $e(t)$ satisfy $\eta^{+,(t)}$, if one of the events in the flow is removed. Otherwise, the event flow $e(t)$ satisfies η^{+} but not $\eta^{+,(t)}$. If this situation applies, we say that the event flow $e(t)$ has a single disturbance and that the decomposition described in Theorem 22 is valid.*

Proof. If the event flow $e(t)$ has a single disturbance, then by definition it must violate $\eta^{+,(t)}$ at least in one time interval of size Δt. To identify a violation of $\eta^{+,(t)}$, we must check whether more than $\eta^{+,(t)}$ events occur in some time interval of length Δt in the event flow. This is done by the decomposition algorithm described in Theorem 22. The maximum deviation between the event flow and the typical event model $\eta^{+,(t)}$

$$\max_{0 \leq \Delta t \leq t} \left\{ 0,\ \eta^{+}_{e,\,t}(\Delta t) - \eta^{+,(t)}(\Delta t) \right\}$$

can by definition of an event flow with a single disturbance not be larger than 1 and thus the decomposition correctly identifies one overload event in an event flow with a single disturbance.

Figure 1 shows an exemplary event flow with a single disturbance, where the typical event model $\eta^{+,(t)} = \lceil \Delta / P \rceil$ is fully periodic and the worst-case event model $\eta^{+} = \lceil (\Delta t + J)/P \rceil$ is periodic with jitter. The event flow satisfies $\eta^{+,(t)}$ if the 4th event is removed. The decomposition algorithm recognizes that an overload event occurs in the event flow for $t \geq 3P$ because for different values of Δt the typical event model $\eta^{+,(t)}(\Delta t)$ is exceeded by 1, e.g., for $\Delta t = P$. □

Note that in Köhler [2022], a generic and efficient decomposition of event flows is proposed.

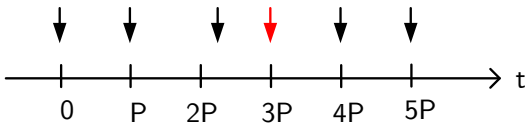

Figure 1: Event flow with a single disturbance

4 Finding an Overload Event Model

The follow-up problem is to find a maximum event model for the occurrence of overload events in a decomposed event flow.

Proposed Solution in Ahrendts et al. [2018] We will recall here the proposed solution in Ahrendts et al. [2018] which was formulated in Theorem 23:

Theorem 23 (Obtaining an overload event model)**.** *A maximum overload event model is*

$$\overline{\eta}^{o}(\Delta t) = f_{slw}\left(\max_{0\leq\Delta t^{*}\leq\Delta t}\left\{\eta^{+}(\Delta t^{*}) - \eta^{+,(t)}(\Delta t^{*})\right\}\right)$$

where f_{slw} is a sliding window function.

Error in the proposed overload event model: limited applicability Similar to the case of event flow decomposition, Theorem 23 delivers only a correct bound for event flows with a single disturbance. Again multiple occurrences of overload events at different points in time are not properly considered in Theorem 23.

Theorem (Overload event models for event flows with a single disturbance)**.** *The overload event model*

$$\eta^{+,(o)}(\Delta t) = f_{slw}\left(\max_{0\leq\Delta t^{*}\leq\Delta t}\left\{\eta^{+}(\Delta t^{*}) - \eta^{+,(t)}(\Delta t^{*})\right\}\right)$$

is safe for event flows with a single disturbance.

Proof. Event flows with a single disturbance have one overload event and thus a safe overload event model is simply $\eta^{+,(o)}(\Delta t) = 1$. The formulation

$$\eta^{+,(o)}(\Delta t) = f_{slw}\left(\max_{0\leq\Delta t^{*}\leq\Delta t}\left\{\eta^{+}(\Delta t^{*}) - \eta^{+,(t)}(\Delta t^{*})\right\}\right)$$

is complicated but safe and tight since there is (by definition of an event flow with a single disturbance) at least one time interval Δt^{*} for which $\eta^{+}(\Delta t^{*}) -$

$\eta^{+,(t)}(\Delta t^*) = 1$ and none with $\eta^+(\Delta t^*) - \eta^{+,(t)}(\Delta t^*) > 1$. By applying the sliding window function, it is assured that $\eta^{+,(o)}$ is a monotonically increasing function. □

Note that Köhler [2022] describes an efficient way to find maximum overload event models in case of sporadic overload event arrival. A less efficient but generic way to find overload event models is also proposed which relies on mixed-integer linear programming.

5 Conclusion

We proposed in Ahrendts et al. [2018] (1) a decomposition of event flows into typical events and overload events, and (2) an overload event model which bounds the occurrence of overload events in event flows. These result were erroneously supposed to be applicable to any event flow $e(t)$, but they are in fact not and apply only to specific cases – in particular to event flows with a single disturbance. This limits considerably the relevance of the results for practical problems and also invalidates the experiments in Ahrendts et al. [2018]. Note that the results of Ahrendts et al. [2018] have been reused in Köhler and Ernst [2019].

The reader may refer to Köhler [2022] which provides generic solutions for the issues raised in this erratum and discusses a new set of experiments.

References

Leonie Ahrendts, Sophie Quinton, Thomas Boroske, and Rolf Ernst. Verifying weakly-hard real-time properties of traffic streams in switched networks. In *ECRTS 2018-30th Euromicro Conference on Real-Time Systems*, pages 1–22, 2018.

Leonie Köhler. *A Compositional Performance Analysis for Embedded Computing Systems with Weakly-Hard Real-Time Constraints*. PhD thesis, TU Braunschweig, 2022.

Wenbo Xu, Zain AH Hammadeh, Alexander Kröller, Rolf Ernst, and Sophie Quinton. Improved deadline miss models for real-time systems using typical worst-case analysis. In *2015 27th Euromicro Conference on Real-Time Systems*, pages 247–256. IEEE, 2015.

Leonie Köhler and Rolf Ernst. Improving a compositional timing analysis framework for weakly-hard real-time systems. In *2019 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pages 228–240. IEEE, 2019.