Poster: Model-based Adaptation to Extreme Physical Environments: A Case Study on Mixed-Criticality Industrial Ethernet

Zonghui Li, Hai Wan, Yangdong Deng, Qinghan Yu, Tianchi Li, Kang Wei, Ming Gu
Software School, Tsinghua University, Beijing, China

ABSTRACT

Industry-strength embedded systems have to meet rigorous application-specific requirements for operating environments. Such requirements are becoming increasingly challenging due to the growing system complexity. Existing works typically focus on reliability driven design optimizations to improve the system robustness. Our work addresses the problem from another perspective by adaptively adjusting its service capability according to a model reflecting the interaction between the embedded system and the environments.

This paper proposes a service capability model to capture the criticality of various services. A model-based adaption mechanism is designed to automatically identify the maximum allowed service capability under the current physical environment. A case study was performed on Industrial Ethernet switches to validate its effectiveness on adaptation to high and low temperatures. Experimental results demonstrate the potential of our approach to improve system reliability under extreme physical environments.

1 INTRODUCTION

Industry-strength embedded systems, especially safety-critical systems, have to maintain the reliability of systems in extreme physical environments such as high and low temperatures. Due to the growing system complexity, it is increasingly challenging to provide persistent service under harsh environments. Researchers proposed various solutions to address different aspects of this challenge. One class of works such as [1], depend on system power optimization to reduce heat dissipation. They actually relieve the failure of systems under extreme ambient temperatures. However, the margin of such approaches diminishes with the growing complexity of systems. Another class of works such as [2] build self-adaptive systems from system-level models by considering varying requirements or dynamic contexts. They adapt these changes by replanning or component replacement. To some extent, they actually relieves the failure of systems in extreme physical environments, but do not directly deal with rigorous physical environments.

This paper proposes a service capability model for runtime adaptation to the changes of physical environments. The impacts of a system on environments are regarded as physical contributions and refined into levels of service capability. A system dynamically adapts to variations of physical environments by migrating its service-capability levels. When a system works in extreme physical environments, it degrades its service capability. When the physical environment recovers normal, it updates its service capability. A case study is performed on our Industrial Ethernet switches for extreme high and low temperature tests. The results demonstrate that the switch using the proposed model gracefully goes through high temperature ordeal while the other without using the model breaks down due to exceeded heat.

2 SERVICE CAPABILITY MODEL

2.1 Basic Concepts and Properties

Definition 2.1. *Module* is an indivisible internal functional unit in a system. It has two properties as follows.

Criticality level(cl): It indicates the criticality of the module. The smaller the value, the higher the criticality. It comes from criticality levels of services:

$$\forall m \in M, A = \{s | s \in S \wedge m \in s\}; \qquad m.cl = \min_{s \in A}\{s.cl\}$$

where M is the set of all modules, S is the set of all services in the system, and A is the set of all services containing module m.

Physical gains($pgs[n]$): It indicates the contributions to physical status of the system when the module is working. Its length is n and its values reflect different aspects such as temperature of the contributions to physical status of the system.

$$\forall m \in M, m.pgs[n] = \{\underbrace{w_0, w_1, w_2, ..., w_{n-1}}_{n}\}$$

where w_i is one side gain for physical status.

Definition 2.2. *Service* is an external and indivisible function to satisfy one or multiple requirements of users. It is a set of modules whose cooperations provide the service. It has three properties below.

Modules($ms[l]$): It is the set of all modules providing the service and its number is denoted as l.

$$\forall s \in S, s.ms[l] = \{\underbrace{m_0, m_1, m_2, ..., m_{l-1}}_{l}\}$$

where m_i is the i-th module for the service.

Criticality level(cl): It indicates the criticality of the service. The smaller the value, the higher the criticality.

$$\forall s \in S, s.cl = \max_{m \in s.ms}\{m.cl\}$$

where S is all services in the system.

Physical gains($pgs[n]$): It indicates the service contributions to physical status of the system when the service is active. Its length

ICSE '18 Companion, May 27-June 3, 2018,
Gothenburg, Sweden
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5663-3/18/05.
https://doi.org/10.1145/3183440.3194993

is n and its values reflect the contributions to different aspects such as temperature of physical status.

$$\forall s \in S, s.pgs[i] = \sum_{j=0}^{l-1} s.ms[j].pgs[i]$$

where $0 \leq i \leq n-1$ and $s.pgs[i]$ is one side gain for physical status.

2.2 Service Capability and Physical Gains

To divide service-capability levels and compute physical gains, three steps are presented as below.

Step One: Order services by their criticality levels and collect services having the same criticality level into a single group. G_i denotes the set of services that have the criticality level equal to i. So we have the following.

$$G_i.cl = i; \qquad G_i.ms = \bigcup_{s \in G_i} s.ms; \qquad G_i.pgs = \sum_{m \in G_i.ms} m.pgs$$

Step Two: H_i denotes the service capability with level i, and it is the prefix sum of G: $H_i = \sum_{j=0}^{i} G_j$. That is,

$$H_i.cl = i; \qquad H_i.ms = \bigcup_{j=0}^{i}(\bigcup_{s \in G_j} s.ms); \qquad H_i.pgs = \sum_{m \in H_i.ms} m.pgs$$

Step Three: Δpgs_{ij} denotes the altered physical gains of the transition from the *i-th* to *j-th* service-capability level.

$$\Delta pgs_{ij} = H_j.pgs - H_i.pgs$$

The high-level service capability includes all services of lower service-capability levels.

3 CASE STUDY ON INDUSTRIAL ETHERNET SWITCHES

Our Industrial Ethernet switches are designed for train networks and integrate the functionality of both standard Ethernet and industrial control network by providing mixed-criticality services. The services of time synchronization and time-triggered communication provide real-time and deterministic transmission for industrial control and thus have the highest criticality level 0. Their failures will lead to out of control and even accident. The lower criticality level 1 and the lowest 2 are data monitoring and Internet services, respectively. Their failures do not affect the train control. According to the industry practice of China, the range for high and low temperature tests is from -25°C to 75°C. Based on our service capability model, the state machine of the service-capability transitions is illustrated in Fig. 1. Fig. 2 presents the runtime service-capability level of two switches with ambient temperatures.

In the initial four hours (-25°C for two hours), the two switches are both working at the highest service-capability level H_2. At the forth hour, the temperature quickly increases to 75°C. After undergoing 75°C for about two hours, one switch, denoted as A, monitors the device package temperature up to 101°C and its capability degrades from H_2 to H_0 and as a result that data monitoring and Internet services are lost. On the other hand, the other switch, denoted as B, is still working at H_2 and everything is well. After tolerating 75°C for about 5 hours, at the ninth hours all communication functionalities of switch B stall. The nearest read device package temperature is 136°C. The FPGA of switch B is erased due to excessive heat protection. Switch A is still working at H_0 and provides the real-time transmission service. At the tenth hour, the temperature decreases to 25°C. After about 1.5 hours, switch A senses the device package temperature dropping to 68°C and the capability resumes from H_0 to H_1 . When the device package temperature recovers to 63°C, switch A returns to the highest service-capability level H_2 and all communication functionalities recover. At the fourteenth hour, the temperature of switch A is stable at 50°C. As a comparision, switch B has been down since the ninth hour. The experiment demonstrates the advantages of our service capability model for the self-adaptation to extreme environments.

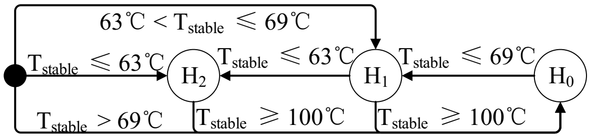

Figure 1: The state machine of service-capability transitions. The T_{stable} is the current stable temperature.

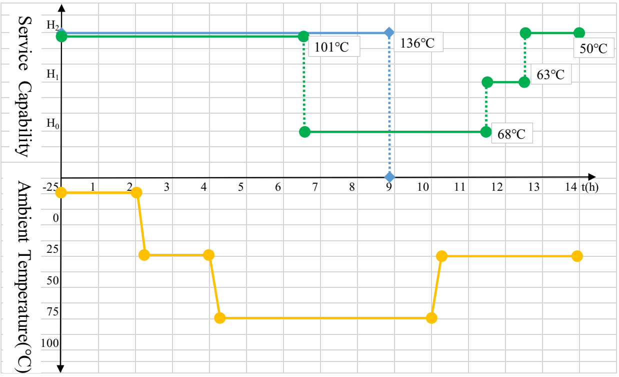

Figure 2: Runtime service capability with temperature.

4 CONCLUSIONS

In this paper, we propose a service capability model to enable the system adaptability to extreme environments by the transitions of service-capability levels. A case study is performed in our Industrial Ethernet switches for high and low temperature tests. It demonstrates the advantages of our model for adapting to extreme environments.

REFERENCES

[1] Yong Fu, Nicholas Kottenstette, Chenyang Lu, and Xenofon D Koutsoukos. 2012. Feedback thermal control of real-time systems on multicore processors. In *Proceedings of the tenth ACM international conference on Embedded software*. ACM, 113–122.

[2] Thomas Vogel and Holger Giese. 2014. Model-driven engineering of self-adaptive software with eurema. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 8, 4 (2014), 18.