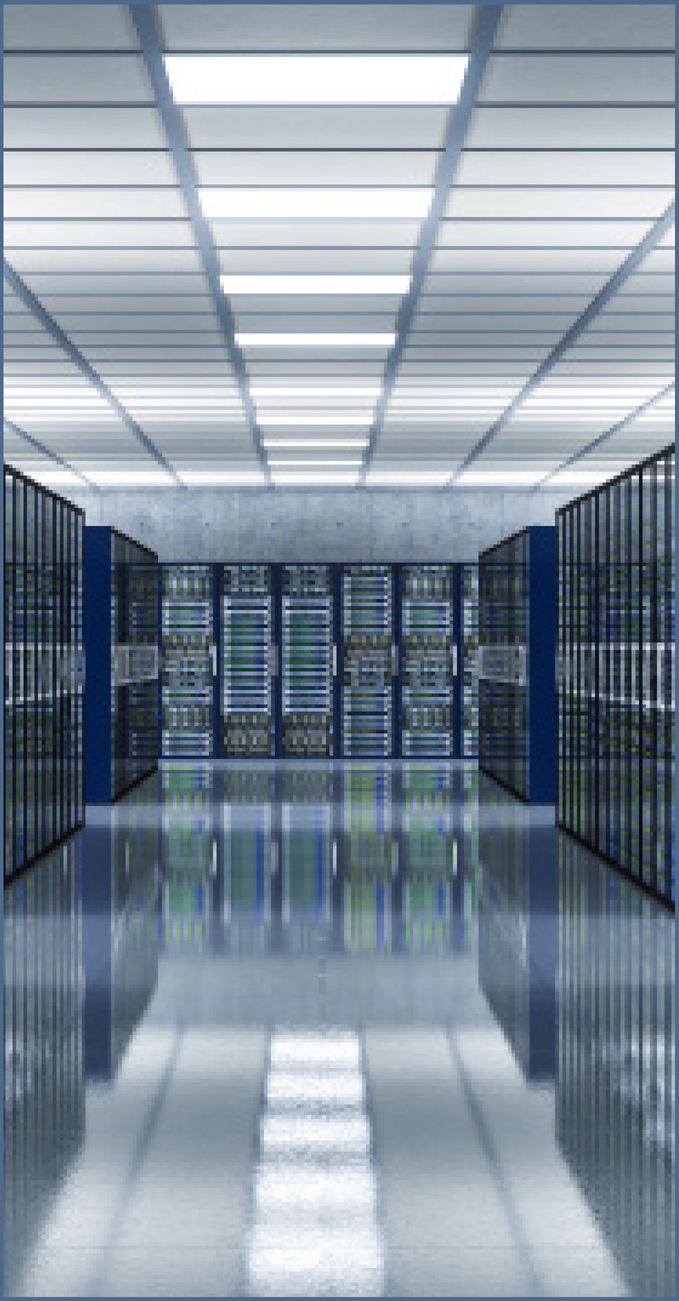

JS|HELD

PERSPECTIVES

What's Cooking? Thermal and Overtemperature Events of Datacenters

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

You may have read storage and operational temperature specifications on a box of newly purchased electronics or somewhere buried in the back of a user manual. Computers, servers, networking equipment, and other electronics all have manufacturer specifications indicating what temperature/conditions the equipment was designed to withstand. Datacenters are full of this type of equipment. So, what happens if that equipment is subjected to an overheating event? What is an overheating event? How do we evaluate this type of event and its effect on equipment? This paper will discuss overheating events, the typical scenarios that can occur, how they can occur, how these events are validated, and how to effectively respond to the event with the right technical team.

DATACENTERS AND HEAT

Datacenters can be large facilities or small segmented rooms containing racks and rows of equipment. Typically, a datacenter will house many servers, networking devices, and other electronics. The infrastructure of the datacenter will supply power and provide cooling to run the equipment and keep it at optimum temperatures (typically, a large datacenter will have large HVAC units handling the cooling for the entire room). Since the equipment creates heat as it runs, it is critical for all server rooms or locations, both large and small, to manage the heat. This is to maintain operation within manufacturer specifications for both reliability and performance.

Manufacturers typically have different specifications including maximum and minimum heat thresholds. The manufacturers determine these through quality assurance testing and stress testing, which varies depending on the device and manufacturer.

Storage and Operating Temperatures

When manufacturers provide the temperature specifications of equipment, there are multiple temperatures to consider and understand. First, there are operating temperatures and storage temperatures. Storage temperatures are the temperatures that the equipment is designed to withstand while the equipment is powered off whereas operating temperatures are the suggested ranges that the equipment should run within for performance and reliability. Storage temperature specifications tend to be more broad than operating temperature.

With regard to operating temperatures, there are ambient temperatures, board-level temperatures, and processor temperatures. Ambient temperatures indicate what is perceived to be the room temperature taken from a sensor on the equipment, typically on a fan intake or outside of the chassis. The board-level and processor temperatures are taken from components within the equipment. Processors tend to run much hotter than the rest of the system and have their own cooling unit (fan and heat sink). These sensors are all designed to log the temperature condition of the equipment and tell the system how to react if temperature increases such as increasing fan speed, indicating error messages or, in some cases, shutting down the equipment to prevent damage.

WHAT IS OVERHEATING?

A datacenter overheating event occurs when equipment is subjected to high temperatures for a period of time which could range from a brief event to one spanning many hours. If the cooling system (such as HVAC) of a datacenter fails, the heat from the equipment has nowhere to go. The hot air from the exhaust keeps cycling through the intake and can rapidly and exponentially increase. In some of the worst cases, the heat from this kind of event has been known to cause dangerously hot environments, in excess of 150 degrees Fahrenheit, in a short period of time.

As temperatures rise, most datacenter equipment is designed to try to compensate. For instance, the fans within the system will spin faster, trying to cool the electronic components. If equipped with sensors, the systems will begin to log the overtemperature event, send warning messages, and, in some cases, start to shut down to try to protect the components. Critical systems may continue to run if automatic shutdown is disabled.

DAMAGE EVALUATION

A common problem after an overheating event is validation of damage. A visual inspection is typically the first step in evaluating damage. If temperatures rise to extreme levels and for a long period of time, sometimes there will be visible damage, such as melted plastic. If temperatures are great enough during an overheating event, they can cause fires within the equipment or even trigger fire sprinklers, causing secondary water damage. However, not all equipment is necessarily going to show obvious damage, and it becomes a challenge to validate damage when there is no visual confirmation.

If no visible damage is present, in many cases it becomes necessary to engage a technical representative to obtain additional data to validate the incident and damages. The data collected from the equipment and surrounding systems is used to determine:

- What happened to cause the overheating event.
- The duration of the overheating event.
- What temperatures were reached on each device.
- How systems reacted to the event.
- Whether verifiable hardware failures are due to the overheating event.

Using Log Data

Log data can include error logs, warnings, and critical failures from computers, networking devices, and other equipment within the datacenter. Some more sophisticated systems log the temperatures on a component level and save that information. Building management systems, alarm systems, and HVAC equipment may also have useful log information that could show the overall temperatures of the room and the timeline of any event.

The log data and failure analysis allow for a quantifiable method of confirming the event, noting the number of failures, and for logging what transpired after the event. For instance, the log data may show that the equipment entered a thermal shutdown mode to protect the equipment from damage. Other logs may show an increase in component failures during and after the event. Logs may also show issues with the system predating the incident.

Failures and Post Overheating Event Concerns

Common concerns after an overheating event include:

- Failures of critical devices.
- Effect(s) on future reliability.
- Voidance of manufacturer warranty / service contracts.

Failures can occur immediately after the event and are typically quantifiable. However, it is common for there to be a concern with future reliability or unknown failures. Depending on the situation, further evaluations can be performed to try to quantify any additional impacts. This can include further testing of the equipment or individual components, additional monitoring of equipment after the event, or even performing some stress and load tests of the equipment to attempt to quantify the likelihood of additional failures. It is important to work with the equipment owners, equipment manufacturers, and technical representatives to develop a protocol for each specific situation.

In addition to hardware failures, a common issue is the voidance of warranty due to exposure to conditions outside of the manufacturer's specifications. How a manufacturer responds to such an event is typically a case-by-case matter. It is important to work with the manufacturers and provide the actual temperature and timeline information in these situations. Additionally, it is important to analyze what equipment was under warranty at the time of the incident and whether the warranty has been confirmed as voided. The adjuster will need to review their specific policy on how they respond to loss of warranty or service contract.

CONCLUSION

Analyzing overheating events in datacenters can be complex, with many factors to evaluate and consider. A quick response and thorough evaluation are imperative. Having a technical evaluation completed early in the process can ensure the right questions are asked and that documentation and evidence of the event are retained. Doing so will ensure that the correct damage assessment is performed, proper corrective actions are taken, and that all issues and concerns can be addressed.

ACKNOWLEDGMENTS

We would like to thank Anthony Danza, CCFE, and Troy Bates for providing insight and expertise that greatly assisted this research.

Anthony Danza is a Senior Vice President and Regional Lead in J.S. Held's Equipment practice. Anthony has over 17 years of insurance consulting experience and has worked on thousands of projects from large catastrophes to small losses involving technical issues and equipment. Anthony has worked as a team leader to successfully perform damage assessments, feasibility of repair versus replacement, comparable replacement analysis/estimates, actual cash value estimates, production impact resolution, and claim evaluation.

Anthony can be reached at adanza@jsheld.com or +1 714 742 3531.

Troy Bates is an Executive Vice President in J.S. Held's Equipment Practice. He specializes in equipment damage assessment, feasibility of repair versus replacement, comparable replacement analysis / estimates, actual cash value estimates, production impact resolution, and claim evaluation. Troy has evaluated a wide variety of equipment and systems including, but not limited to, information technologies, electronics, medical equipment, telecommunications, and other specialized equipment. He focuses on high-end computer hardware, personal computers, application software, operating systems, programming languages, data recovery, printers and printing routing technology, telephone switch equipment, switches, routers, networking topologies, data cabling, and telecommunication cabling.

Troy can be reached at tbates@jsheld.com or +1 714 660 9171.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.