ABSTRACT

Aggressive technology scaling trends are expected to make the hardware of high-performance computation (HPC) systems more susceptible to transient faults. Transient faults are commonly caused by high-energy particles from cosmic radiation or electrical noise and corrupt program computation by causing random bit flips. Transient faults may be masked by program logic without affecting the program output; cause a program to crash, e.g., a transient fault corrupts a pointer variable; or lead to silent data corruption (SDC), where the transient fault introduces an error into the application that is not detected. The HPC community is concerned with the impact of silent data corruption on computation results, on which critical decisions may rely. Due to the insidious nature of SDC, understanding a fault-corrupted program's behavior is crucial for developing and evaluating software resiliency techniques to ensure correct output results from HPC applications. Classical fault injection studies give an overall statistical resiliency profile for an application. However, summarizing critical information and understanding the behavior of the fault-injected program are challenging. In this work, we introduce SpotSDC, a visualization system for analyzing a program's characteristics of resilience to SDC. SpotSDC provides an overview of the SDC impact on an application by indicating the impact of a transient fault over the program's space and time. It highlights the regions of code that are most susceptible to SDC and that will have a high impact on the program's output. SpotSDc also enables users to visualize the propagation of error through an application execution. The results from SpotSDC allow developers to design selective algorithmic error detection and mitigation techniques to protect their applications from SDC.

Introduction

Aggressive technology trends tend to make the hardware of high-performance computation systems more susceptible to transient faults. Transient faults, which commonly caused by cosmic radiation, device noise and other factors, can manifest in applications in three ways. They can cause an application to crash, e.g., the transient fault corrupts a pointer variable and causes a segmentation fault. They can be masked without affecting the application’s output. The most insidious outcome is silent data corruption (SDC), where the transient fault introduces an error in the application that is not detected and will potentially alter the computation results without being noticed. The corrupted computation result will then be used in the subsequent research.

Due to the insidious nature of SDC, understanding how it affects a particular application is critical for developing and evaluating software resiliency techniques. The classical approach for studying how transient faults affect an application is a fault injection campaign, in which a tool injects an artificial fault into an application, observes the behavior of the program, and records the result. Current tools typically use this technique, which randomly injects an error into a program, to repeatedly test the program, collects the diagnosis data of an application, and provides a high-level statistical profile.

However, without a detailed examination of the SDC impact over the space and time of a program execution, the conclusion of the analysis may be incomplete and inaccurate. The space of a program can be huge, and the time scale of program execution can be long. Using the traditional method to provide a detailed understanding of the impact of SDC on these two dimensions is challenging. Examining the fault injection cases is a difficult task for domain experts, since they must repeatedly check the states between the fault injection computation and error-free computation.

At the same time, studying how a transient error propagates through the program and result in SDC or how it is masked by the program logic will help a researcher develops a better understanding of the impact of a transient error on the program.

In this work, we introduce SpotSDC, an interactive visualization system to analyze a program’s characteristics of resilience to SDC. SpotSDC identifies the impact of SDC through space and time. It highlights the regions of code that are most susceptible to SDC and that have a high impact on the program’s output. SpotSDC also provides users with the overall SDC characteristics of the application, and enables them to visualize the propagation of error through an application execution. SpotSDC will enable researchers to design selective algorithmic error detection and mitigation techniques to protect their code from producing erroneous output.

Our key contributions in this paper are as follows:

* An interactive visualization system to study HPC computation kernels’ silent data corruption vulnerability and impact.
* A bit-based visualization to address the error scaling challenges among multiple code regions, a study of the difficulty of visually comparing the sensitivity of various code regions.
* A grand visualization display of the sample space of the fault injection to help domain experts reveal the limits of the data sample.
* A visual fault injection analysis scheme from statistics to annotate source code for reasoning and planning for protection.
* A visual encoding to encompass multiple levels of granularity from program to function, to variable, and finally to individual bits.

The remainder of this paper is structured as follows: Section 2 discusses the related work in this area. Section 3 introduces the domain background. Section 4 talks about the domain tasks. Section 5 discusses the challenge of comparing multiple code regions. Section 6 shows how users can use our tool to improve their sampling. Section 7 introduces the interface of the system, Section 8 demos the usability of the system, and finally, we conclude our research in section 9.

Domain Background And Data Description

In this study, the fault injection tool repeats the fault injection experiment many times and records the result of each experiment and the value of each data variable during program execution.

# The SDC Ratio of Program’s Different Bit

IEEE 745 double-precision binary float-point format has 1 sign bit, 11 exponent bits, and 52 mantissa bits. During the program execution, each dynamic instruction has an equal chance of being corrupted by a transient fault. Each instruction has 64 bits, each with equal chance of being flipped. Figure 1 shows the 64-bit IEEE 754 double-precision binary floating-point representation.

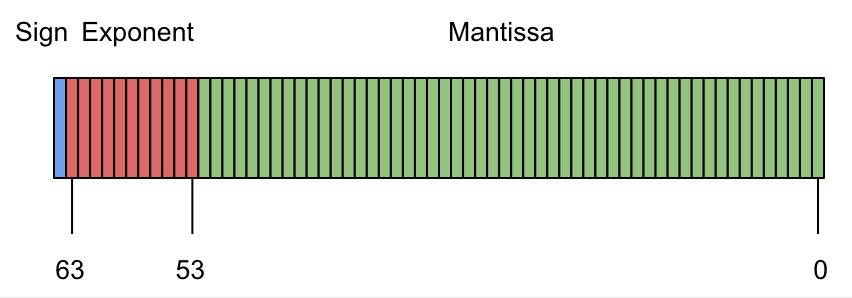


Figure 1 IEEE 754 double-precision binary floating-point format

# Dynamic instruction

A program is constructed of many dynamic instructions. For this study, we focus on the instruction that will change the value of critical variables. Each instruction is a potential fault injection location.

# Fault Injection

A fault injection experiment is the classical method to understand the dependability of a system. In each experiment, an artificial fault (a bit flip) is injected at a data variable once in a random time step during program execution and records the computation result. A collection of fault injection experiments is called a fault injection campaign.

For each fault injection experiment, the following information will also be recorded:

* The name of the function in which each fault is injected.
* The line number in which the fault is injected.
* The variable name in which the fault is injected.
* The injected variable’s initial value.
* The injected variable’s corrupted value after the fault is injected.
* The bit number of a variable is flipped?
* The approximate error of the program output.
* The outcome of a program running, masked, SDC, DUE.
* The dynamic instruction number in which the fault is injected.

In each experiment, we observe the behavior of the program by recording the value of the program’s critical variable. The artificial fault can be injected at any time during the program execution but the observation begins at the start of the program until it exits.

In this research, we study the transient fault caused by a bit flip, in which one bit of a 64-bit float value has been unexpectedly flipped. Here, we use stencil computation as an example to explain what a bit flip is and what kind of result it may cause. As figure 3 shows, one bit of a matrix variable Anext’s one element, which is a float value, is flipped. If the program continues for execution, this error will propagate through to the other elements of the matrix. Once the program finishes executing, it will produce an error outcome.

# Program Outcome

The outcome of a fault injection experiment may be classified in many different ways, e.g., whether the program needs additional execution time to produce a correct solution or the error in a program may propagates to the memory. In this study, we define three categories of a fault injection experiment outcome: Masked, SDC, and DUE based on a threshold value.

In scientific computation, many problems are solved with fault tolerance, in which the program does not give an exact solution but a solution that is close enough to the ground truth. A threshold value, which is defined by a domain expert, is used to define the accuracy of the approximate solution. In a fault injection experiment, we use the threshold value to decide the category of an experiment output.

* **Masked**: A fault is injected into the program, and the program finishes running and gives an output that has the error under the threshold. The fault does not impact the program outcome could mean that the injected error is too small to impact the program’s behavior. The other case, which may be more interesting, is that the injected error is large, but the program logic dismisses the error.
* **Silence Data Corruption (SDC)**: Error is injected into the program, and the program finishes running but the output error is above the threshold. It either gives an incorrect solution to the researchers or pollutes the future computation. However, in neither case, the program will report an error or warn the researchers.
* **Crash**: After the error is injected into the program, the outcome of the program is NAN or infinity. We define this outcome as program crash because this type of output can be easily caught by program’s protection mechanism, e.g., throw exception.

# Feature of The Data

Our data set commonly has hundreds of thousands of fault injection records, and the size of the data is about a few MB. Of each fault injection, the value of each critical variable during the program execution is recorded. For all execution records, the size is hundreds of MB.

# How to Trace Error

In order to measure the error in the fault-injected experiment, we align the golden execution instruction with the fault injection execution instruction. For each alignment instruction, we take the absolute value of difference between two executions. Here, we assume that the golden run and the error run will have a similar computing structure. The computation state of two different run is perfectly matched.

# SDC Ratio and SDC Impact (incomplete section)

The number of times the fault is injected into location A.

# Domain Tasks

We are collaborating with two computer scientists in the fault tolerance research community, including fourteen months of remote meeting and three months of on-site bi-week meetings. The SpotSDC design is constructed based on feedback from the domain experts about what they want to see. On an informal basis, we also ask other researchers interested in fault tolerance analysis how they analyze the bit flip problems in program execution. After our many discussions, we have formalized the domain experts’ interest into four goals.

* **G1: Understand the impact of error in different code regions.**

For each program test, different silent data corruption situation have different error outcome scales. Some cases with large-scale error need more attention compared to the case in which the error is only slight above the error threshold. The large-scale error may severely pollute the next step calculation in the computation pipeline. The study of the error outcome distribution for all tests helps domain experts gain a better understanding of the resilience property of the code region.

* **G2: Understand the silent data corruption vulnerability of different code regions.**

During the diagnostic process, each code section will be tested many times at different time steps. Revealing how many times an error may attack on location will explain how vulnerable the code region is.

* **G3: Reason the interesting feature.**

During our discussion with the domain experts, they frequently mention that they need to go back to the source code to analyze why some code regions are vulnerable and resilient. Visualization presents abstract information to which the domain experts should pay more attention, but they still need to go back to the source code for advanced analysis.

* **G4: Communicate and presentation.**

Domain experts are interested in using the visualization tool to explain to other experts about the fault tolerance analysis and error propagation analysis.

* **T1: Aggregate the code region data based on the program structure.**

The domain experts are interested in understanding the resilience of the program from multiple levels instead of one specific location. They may question how resilient the whole program is to the error or how specific function’s fault tolerance character. An interactive control allowed users to aggregate data from different hierarchical level of a program is essential to answer these questions.

* **T2: Examine the property of a target region.**

How specific code region resilient to the error and why a specific code region is vulnerable to the error are questions do

* **T3: Explore a subset of the data.**

Domain experts are interested to see how do different types of error impact the outcome of the simulation. How does different mantissa and exponent bit change the outcome? How a small error in the program affects the result of a simulation?

* **T4: Connect the source code with the abstract visualization.**

Once the domain experts observe some interesting feature in the data set, they want to check to source code and reason about it. They also add some annotation on their source code to understand the resilience of the program.

Result

# Impact of Different Bits

Figure 2 and 3 demonstrate that most of the fault injection caused by the bit flips occur in the exponent bit, and the majority of the mantissa bit does not result in silent data corruption.

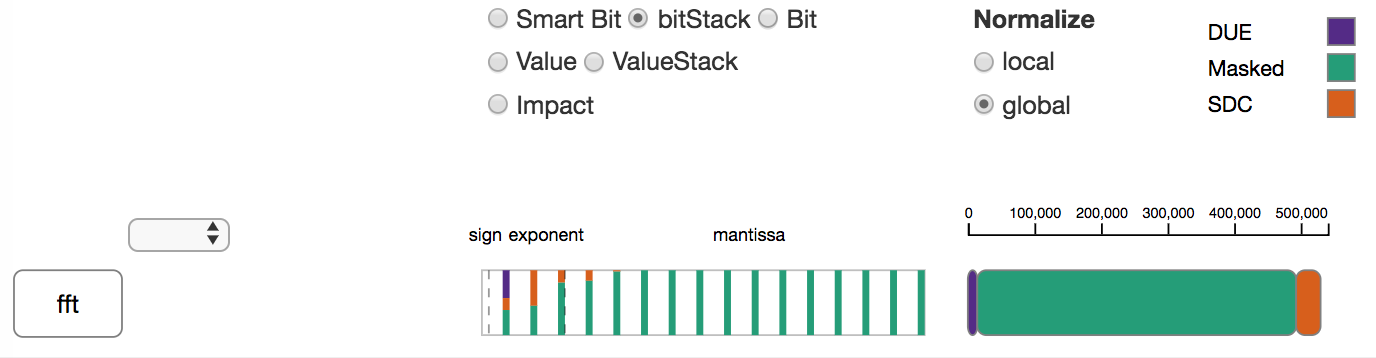


Figure 2. SDC ratio of CG in each bit

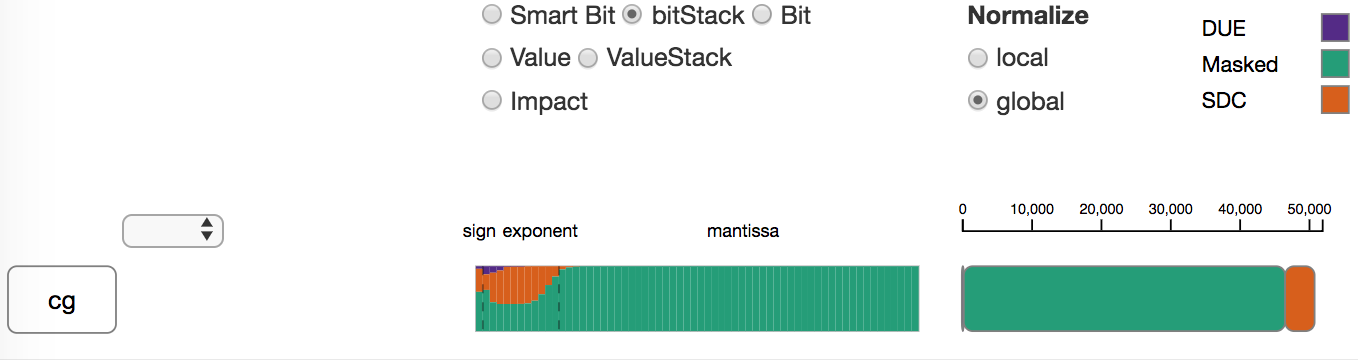


Figure 3. SDC ratio of FFT in every four bits

Figures2 and 3 show the summary results of data collected by the fault injection campaign in FFT and CG, two different applications. Both visualization show that the highest bit has a lower SDC ratio than a lower bit in the two applications. In CG, the highest exponent bit has smaller SDC ratio compare to the second highest exponent bit. In FFT (Figure 2), for the data we have, the highest exponent bit. The DUE (program crash) ratio is high, but DUE can be detected easily.

# Sample of Data set

The data is collected by a random fault injection campaign. Therefore, understand the sample distribution of bit flip in a program is necessary to make an accurate conclusion about the SDC ratio or SDC impact of a specific code region.

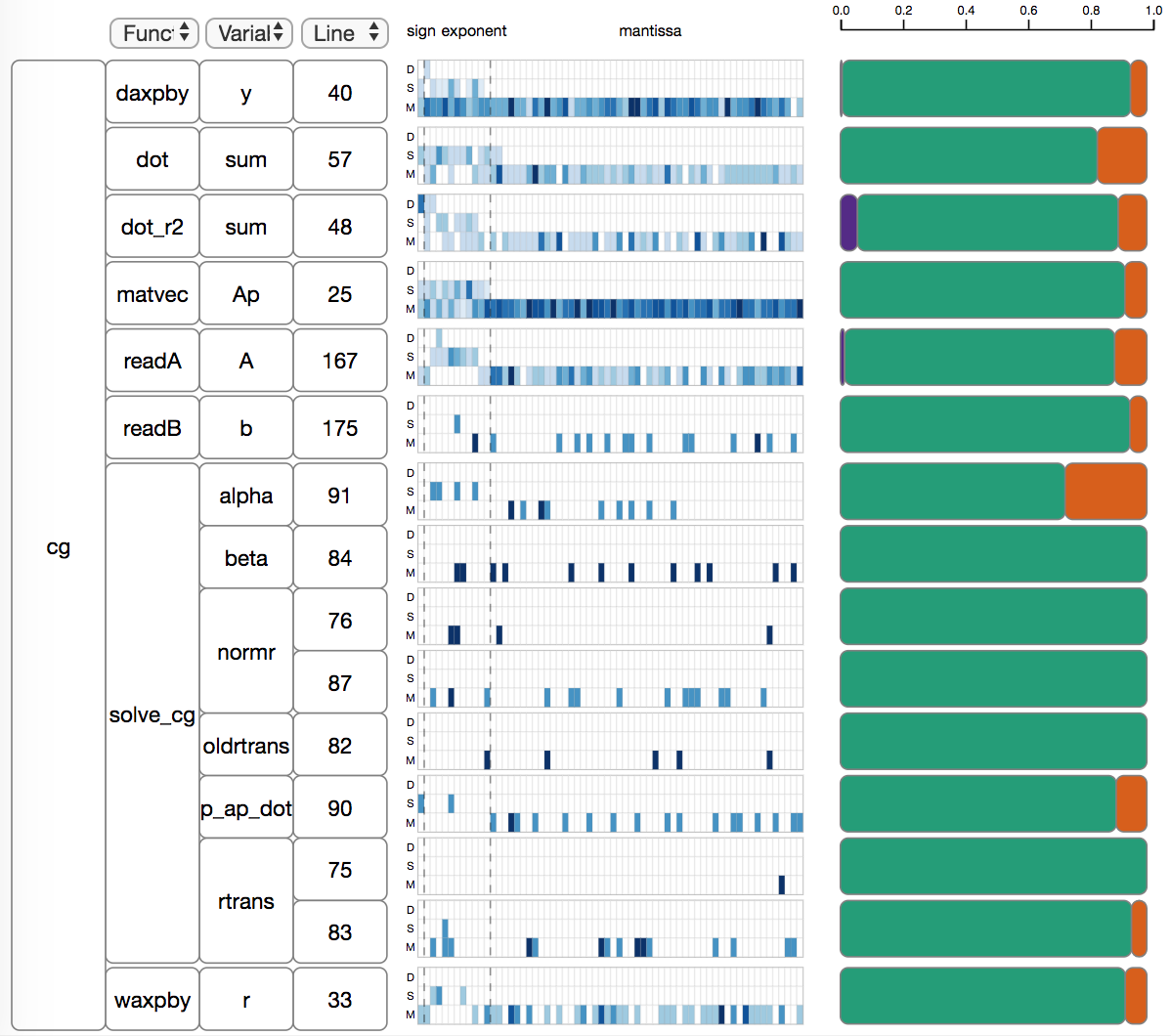


Figure 4. Displaying the bit flip distribution in a different line of code.

In Figure 4, line 75 does not have an SDC outcome for the fault injected in this location, and the SDC ratio in this line is 0. However, the user can check the heat-map on the right to see the distribution of the bit flip that occurs in those locations. For line 75, all the bit flips happen in the low mantissa bit. As we mentioned before, bit flip in the mantissa has much less impact. In order to reach a more concrete conclusion about the impact of this line, the user needs to apply more fault injection experiments in this location with balance bit flip distribution.

# Vulnerability and Resiliency

As the visualization in Figure 5 shows **matvec-Ap-25** has been executed most of the time, and the number of SDC outcome caused by error injected is largest. The line of code has been executed most frequently does not imply high SDC frequency. The user can choose to do local normalization (Figure 6), which will show the SDC ratio in this line of code. **Daxpby-y-40** is executed more frequently than **dot-sum-57** when we try to compare these two lines in the global domain. Once we analyze the SDC ratio in local domain, we can see that **dot-sum-57** has a higher SDC ratio than **daxpby-y-40**. At the same time, the user can check the heat map in the middle, which displays the output error distribution in the different line of code. In Figure 5, **line 25** has the highest chance of being attacked by the transient fault. However, for all the SDC output caused by fault injected in this region, most of the output error is relatively small.

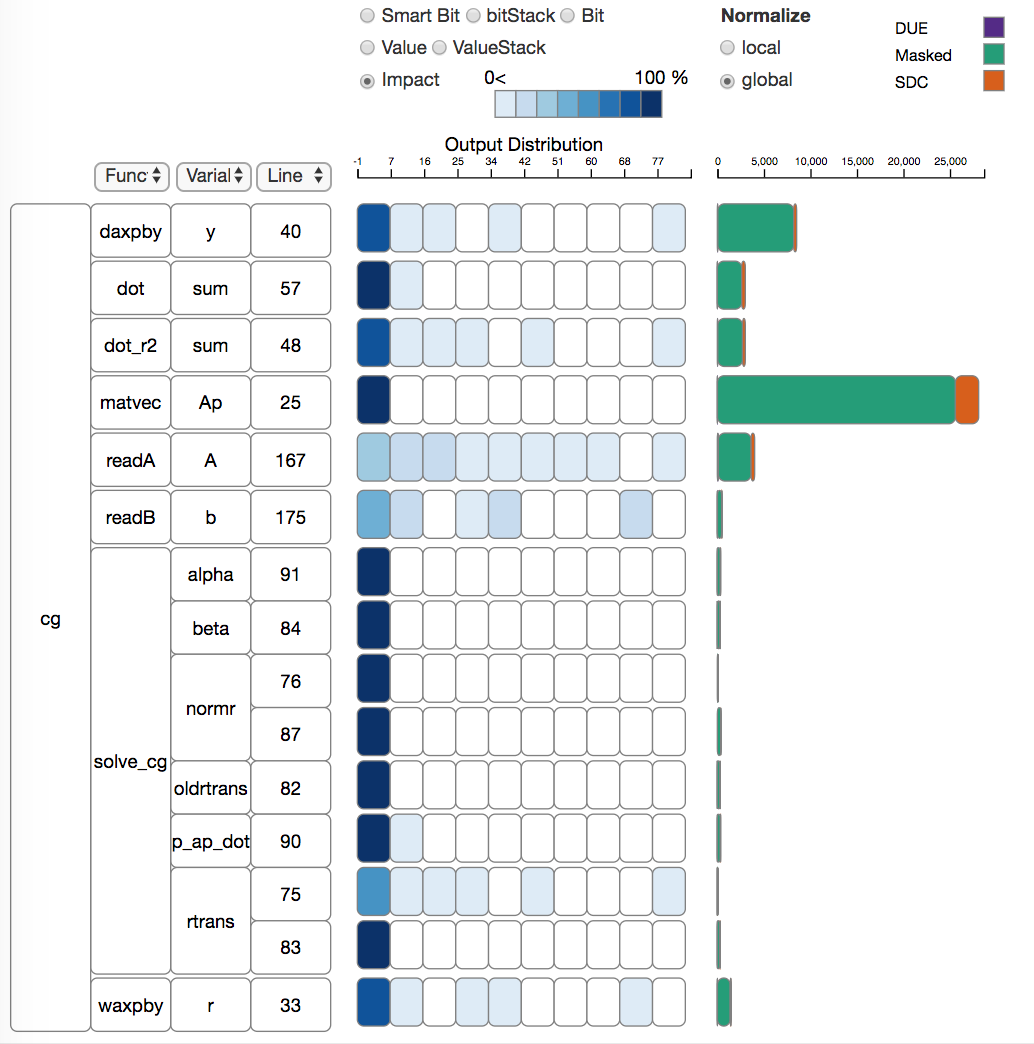


Figure 5 Which code region is more vulnerable to the fault injection.

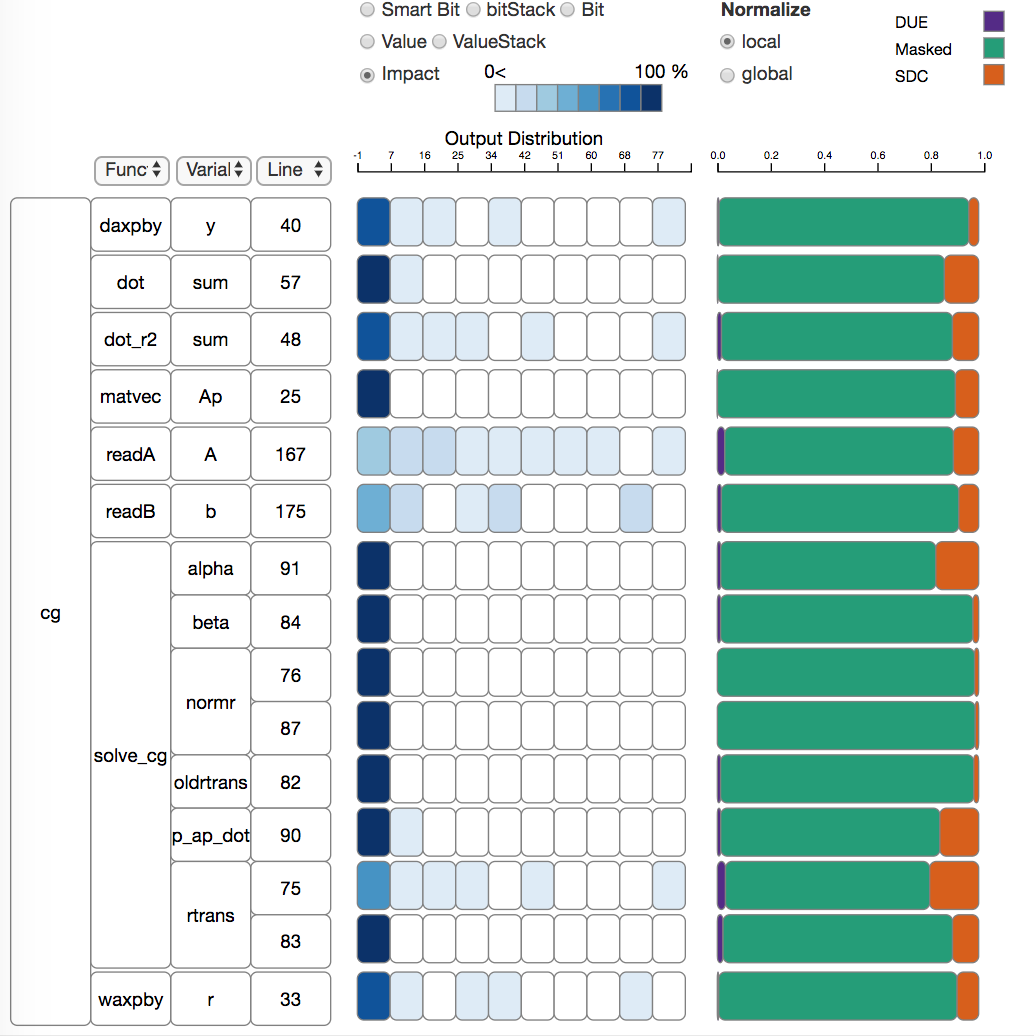


Figure 6. How different iterations will affect the error injection result.

# Error Injection In Different Iteration

During the program execution, when the error is injected into the program may impact the outcome of the simulation differently. A user can choose iteration information as the first level of the location indication tree and check how error that happens earlier or later may affect the outcome of the simulation. As we can see from Figure 7, the number of times error is injected into the earlier iterations 1 to 6 is the same. In zero iteration, the program initializes the value of the variables. However, as we can observe from Figure 8, once we filter out the masker sample, error that happens earlier has a greater impact than that which happens later. Error injected into the first iteration causes the greatest amount of SDC, and as the iteration number increases, the number of SDC caused by error in this iteration decreases.

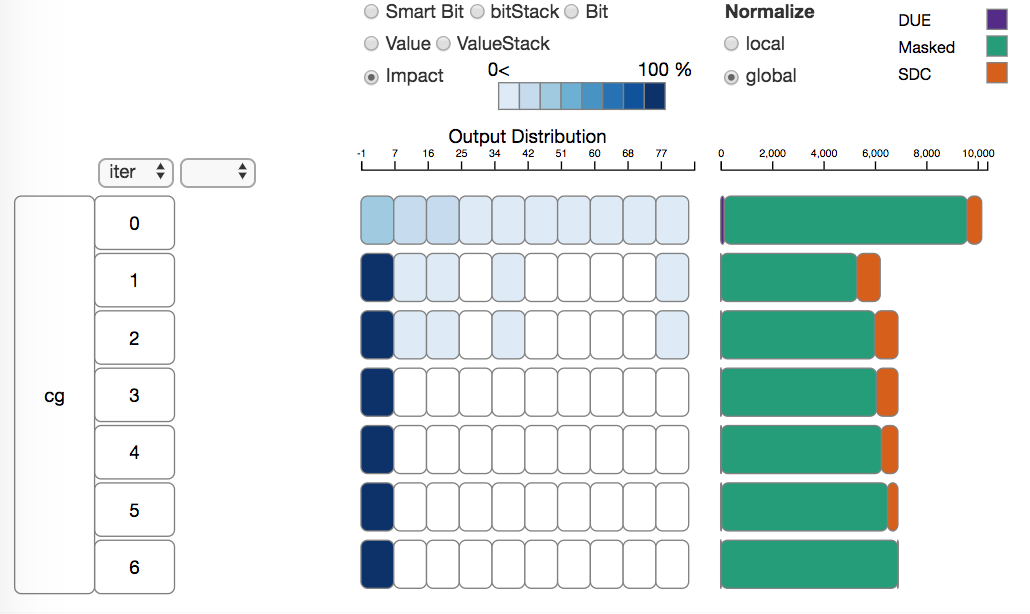


Figure 7.How different iterations will affect the error injection result.

Conclusion

In this research, we design a visualization tool, SpotSDC, to help domain experts understand the impact of silent data corruption on an HPC computation kernel. We demo our tool's usability on two different computation kernels, Conjugate Gradient and Fast Fourier transform. Spot SDC helps domain experts understand the impact of a bit flip on the different levels of the program and reveals more insight into how different bits of a variable flip may impact the outcome of the program. At the same time, Spot SDC also enables users to study the sample size of the random fault injection and determine the sample space.