Embedded Systems, because of their simplicity and specific functionalities, can be vulnerable to side channel attacks. These side channel attacks are aimed not at the mathematics of an encryption algorithm but rather the way the algorithm is implemented in hardware by using the electrical characteristics of the device to extract system information. One example of a side channel attack, and the specific focus of this paper, is a power analysis attack which uses the total power consumed by the device to extract bit values being processed. My research is aimed at evaluating the security of an Advanced Standard Encryption (AES) core which uses Wave Dynamic Differential Logic (WDDL) to defend against a Correlation Power Analysis (CPA) attack. To do this I used the ChipWhisperer Side Channel Attack platform to implement several of my AES designs onto an Field Programmable Gate Array (FPGA) and attack them using a CPA attack. Since there are multiple stages of AES, I examined the security variations by converting only individual stages to WDDL and then tried various combinations of stages converted to WDDL. The results of my research were a 4538% increase in security of a fully implemented WDDL design on the AES core, but also an 805% increase in area of the design. These results show the effectiveness of implementing WDDL in an encryption core to defend against a power analysis attack but also show the challenges of using this type of design in an embedded system that has limited space.