

İKİNCİLİK ÖDÜLÜ

FPGA'LAR ÜZERİNDE AYGIT DNA'SI KULLANIMI İLE DONANIM TASARIMLARINA YÖNELİK SAHTECİLİK FAALİYETLERİNİN ÖNLENMESİ

Orhun Süzer/ İTÜ Elektronik Mühendisliği

Proje Yöneticisi: Doç. Dr. Müştak Erhan Yalçın

Gelişen yaşam koşullarının paralelinde uzayan insan ömrü ve artan insan sayısı tüketim taleplerini de artırmış bu artış üretim miktarlarının artmasına sebep olurken üretim giderlerini ise azaltma eğilimini oluşturmuştur. Başta yüksek oranda fikri mülkiyet ve katma değer içeren ürünler olmak üzere giderlerinin düşürülmesi fikri giderek küreselleşen kapitalist dünya içerisinde kendine büyük bir yer bulmuş ve dış kaynak kullanımı adı verilen bir üretim tarzını ticari hayat içerisine sokmuştur.

Dış kaynak kullanımı ile büyük ölçekli üretim tesislerinin yüksek refah seviyesine sahip; iş gücünün pahalı olduğu ülkelerden gelişmemiş ya da gelişmekte olan; emeğin ve iş gücünün daha ucuz olduğu ülkelere kurulması söz konusu olmuştur. Bu ekseninde araştırma, geliştirme ve tasarım merkezleri gelişmiş ülkelerde kalırken, üretim faaliyetleri uzak doğu ülkelerine doğru kaymıştır.

Ne var ki dış kaynak kullanımı ile başka ülkelere taşınan üretim tesisleri gerek buldukları ülkelerin yasal boşlukları, gerekse ülke içi güvenlik ve gelir seviyeleri doğrultusunda bir çok riski de beraberinde getirmiştir. Bu risklerden en önemlileri kopyalama ya da istek fazlası üretimdir. Kopyalama, söz konusu üretilecek ürünlerin tasarımlarının kopyalanarak başka kişi/ kurumlara satılması olarak tanımlanabilir.

İstek fazlası üretim ise, üretilecek tasarımın ,tasarım sahibi firmanın istediğinden daha fazla sayıda üretilerek pazara başka markalar ya da tasarım sahibi markanın sahteleri halinde sürülmesi olarak tanımlanabilir.

Daha önce de belirtildiği üzere, yüksek oranda fikri mülkiyet ve katma değer içeren ürünlerde tasarımın istenmeyen kişilerin eline geçmesi söz konusu yaratılan değer de ortadan kalkmasına sebep olacak ve bu ürünleri birer metadan farksız kılacaktır.

Bu sebeple yüksek teknoloji ve ileri mühendislik teknikleri içeren ürünler başta olmak üzere katma değeri yüksek olan her ürün için dış kaynak kullanımında yaşanabilecek bir kopyalama veya istek fazlası üretim büyük bir tehdittir.

Bu bitirme çalışması çerçevesinde, uzun süren mühendislik faaliyetleri

sonucunda ortaya çıkan yüksek katma değerli ürün tasarımlarının korunması amacıyla gerçekleştirilmiştir. Bitirme çalışmasında korunmak istenen değer sahada programlanabilir kapı dizileri olarak da bilinen FPGA ürünleri üzerinde gerçekleştirilen donanım tasarımları olmakla birlikte belirli bir tasarım segmentine yönelik değil tüm FPGA tasarımlarına yönelik bir koruma yöntemi önerilmiştir. Bu yöntem Xilinx FPGA ailelerinin birçoğunda bulunan Ayyıt DNA'sı isimli bit dizisinden yararlanmaktadır. Ayyıt DNA'sı değeri her FPGA için farklı olmakla birlikte, değiştirilemez olup FPGA'lerin üretimi sırasında donanımsal olarak programlanmıştır (hardwired). Söz konusu çalışma içerisinde her bir FPGA'ye yüklenecek olan konfigürasyon dosyasının o FPGA ile Ayyıt DNA'sı değeri üzerinden bağlanması önerilmiş olup herhangi bir kopyalama ve istek fazlası üretim durumunda fazladan üretilmiş donanım üzerinde kopyalanmış herhangi bir tasarım dosyasının çalışması engellenecektir. Başka bir deyişle, üretilen ve pazara çıkan her bir ürün üzerinde bir donanım ve bir de tasarımı bulunmakta olup her bir donanım tek bir tasarım ile eşleştirilecek ve sadece onunla uyumlu hale getirilecektir. Dolayısıyla kopyalanan bir tasarımın istek dışı üretilen bir donanım üzerinde çalışması engellenecektir. Söz konusu yöntemde Ayyıt DNA'sının şifrelenerek referans ve kontrol değeri adı altında bir bellek üzerinde tutulması öngörülmektedir. Donanımın söz konusu tasarım ile çalışması sırasında, tasarımlar ilk önce bu değeri kontrol edecek doğruluğunu onayladıktan sonra çalışmaya başlayacaktır. Her FPGA için DNA değeri farklı olduğu için, şifrelenmiş değerlerden her biri sadece bir tasarım için doğru değer olarak görülecektir. Söz konusu şifreleme algoritması olarak TEA (Tiny Encryption Algorithm), FPGA olarak Xilinx firmasının Spartan 3A modeli ile birlikte Atmel 45DBI6DB bellek kullanılmıştır. Bitirme çalışmasının son kısmında belirtildiği üzere; saklanmak istenen her bir tasarımın tek bir donanım ile eşleştirilmesi işlemi ile başarılı sonuçlar elde edilmiş olup bu sonuçlar basit bir led yakma tasarımının sadece belirli bir FPGA üzerinde çalışması ile de ispat edilmiştir. Önerilen yöntem, seri üretim süreçlerinde herhangi bir değişiklik yaratmaması sebebiyle kolayca uygulanabilecek bir yöntem olup, tasarım yapılacak hedef ürünlerden ve üretim platformundan bağımsız olması ve hali hazırda bir tasarım olarak bulunması da uygulanmasını kolaylaştıran diğer etmenlerdendir.