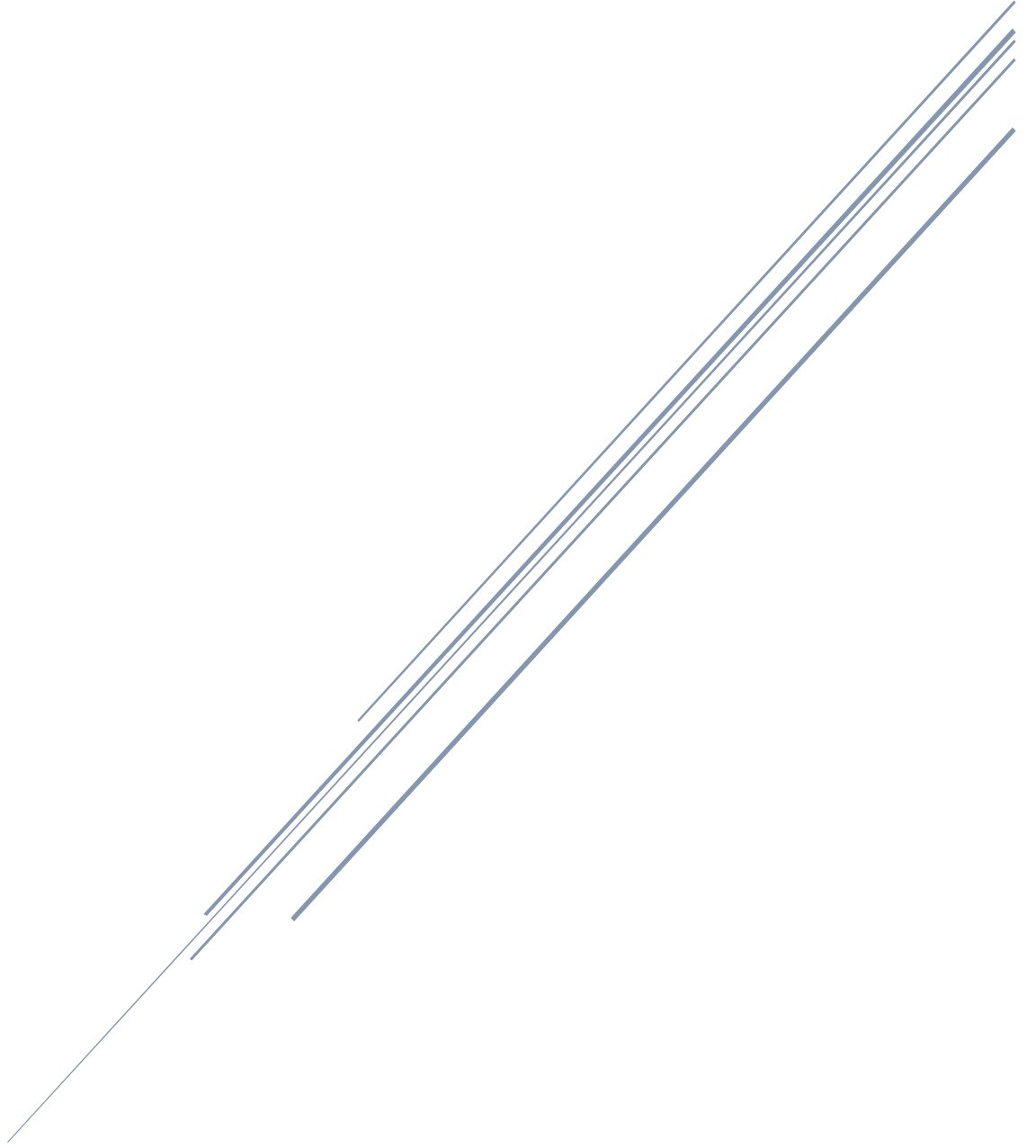


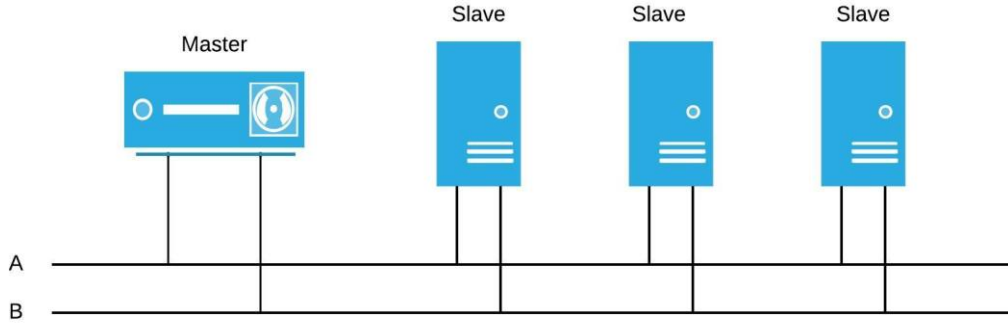
MODBUS HABERLEŐME ALIŐMA RAPORU



FERUDUN GÖKCEGÖZ
İSTANBUL 2020

MODBUS HABERLEŐME PROTOKOLÜ

Modbus protokolü master/slave mimarisine dayanan endüstriyel cihazlar arasında sıklıkla kullanılan yazılımsal bir haberleşme protokolüdür. 1979 yılında sunulmuştur. Zaman içerisinde endüstriyel cihazlarda kullanımı yaygınlaşıp bir endüstri standardı haline gelmiştir. Detaylı bilgi için *PI-MBUS-300 Rev. J* dokümanı inceleyebilir.



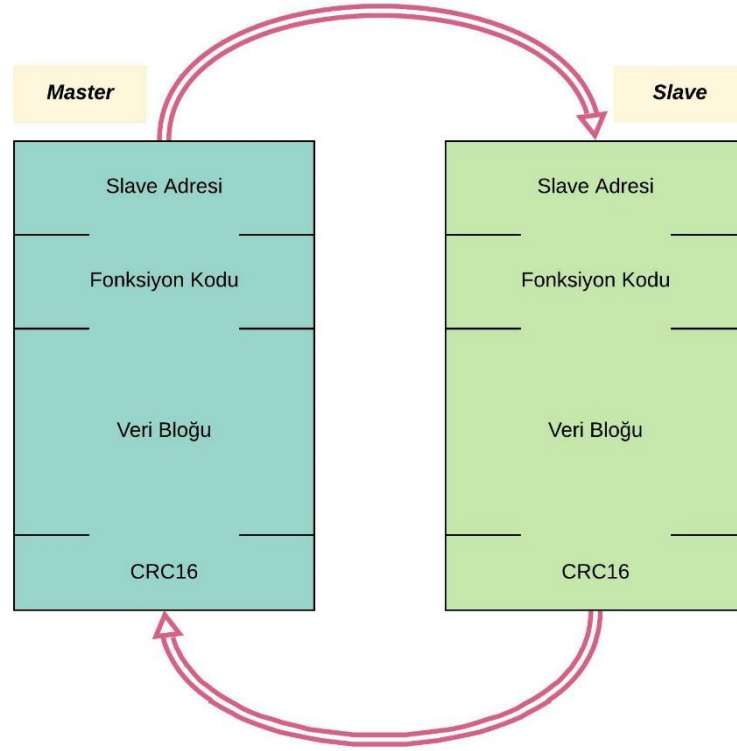
Modbus Master/Slave Mimarisi

Örnek bir modbus haberleşmeli cihazda haberleşme formatı aşağıdaki şekilde olmaktadır.

Fiziksel Arabirim	RS485
Veri Uzunluğu	8 Bit
Parite	Yok
Stop Biti	1
Haberleşme Formatı	RTU
Hata Kontrolü	CRC16
Baudrate (bps)	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200

MODBUS RTU HABERLEŐME YAPISI

Bir modbus ağında bir adet master cihaz ve birden fazla slave cihaz bulunabilmektedir. Master cihaz tarafından gönderilen sorgu mesajları tüm slave cihazlar tarafından dinlenir. Fakat yalnızca adres bilgisi eşleşen cihaz tarafından cevap mesajı gönderilir. Bu şekilde master ve slave cihazlar arasında sorgu ve cevap mesajları alınıp verilerek haberleşme sağlanır.



Bir modbus rtu mesajı aşağıdaki şekilde görüldüğü üzere, ilk byte slave adres bilgisini içeren kısım, ikinci byte fonksiyon bilgisini içeren kısım, ardından yapılması gereken fonksiyona ilişkin verileri içeren kısım ve son olarak CRC16 hata kontrolüne ilişkin kısım olmak üzere 4 parçadan oluşmaktadır.

Slave Adresi (1 byte)	Fonksiyon Kodu (1 byte)	Veri (n byte)	CRC (2 byte)
--------------------------	----------------------------	------------------	-----------------

Modbus RTU Mesaj Yapısı

Slave cihazların adres bilgileri 1 - 247 arasında değer alabilmektedir. Fonksiyon kodu ise yapılmak istenen işleme göre (Holding Register Okuma/Yazma, Input Register Okuma vs.) protokol ile belirlenen değerleri almaktadır. Genel itibariyle modbus haberleşmede 4 tip parametre tipi bulunmaktadır.

<i>Holding Register</i>	<i>16 bit</i>	<i>Okunabilir/Yazılabilir</i>
<i>Input Register</i>	<i>16 bit</i>	<i>Sadece okunabilir</i>
<i>Discrete Input</i>	<i>1 bit</i>	<i>Sadece okunabilir</i>
<i>Coil</i>	<i>1 bit</i>	<i>Okunabilir/Yazılabilir</i>

MODBUS HABERLEŞME FONKSİYONLARI

Modbus master mesajları ile slave cihazlara yaptırılmak istenen fonksiyonlar modbus haberleşme standardında tanımlanmıştır. En çok kullanılan fonksiyonlar sırası ile aşağıdaki gibidir.

(0x01) Read Coil Status, 1 bitlik okunabilir ve yazılabilir parametreleri okumada kullanılır.

(0x02) Read Input Status, 1 bitlik sadece okunabilir parametreleri okumada kullanılır.

(0x03) Read Holding Register, 16 bitlik okunabilir ve yazılabilir parametreleri okumada kullanılır.

(0x04) Read Input Register, 16 bitlik sadece okunabilir parametreleri okumada kullanılır.

(0x05) Force Single Coil, 1 bitlik okunabilir ve yazılabilir parametrelere yazmada kullanılır.

(0x06) Preset Single Register, 16 bitlik okunabilir ve yazılabilir parametrelere yazmada kullanılır.

(0x0F) Force Multiple Coil, 1 bitlik okunabilir ve yazılabilir parametrelere çoklu yazmada kullanılır.

(0x10) Preset Multiple Coil, 16 bitlik okunabilir ve yazılabilir parametrelere çoklu yazmada kullanılır.

SORGU MESAJI

CEVAP MESAJI

	(Hex)		(Hex)
Slave Address	11	Slave Address	11
Function	03	Function	03
Starting Address Hi	00	Byte Count	06
Starting Address Lo	6B	Data Hi (Register 40108)	02
No. of Points Hi	00	Data Lo (Register 40108)	2B
No. of Points Lo	03	Data Hi (Register 40109)	00
Error Check (LRC or CRC)	—	Data Lo (Register 40109)	00
		Data Hi (Register 40110)	00
		Data Lo (Register 40110)	64
		Error Check (LRC or CRC)	—

Read Holding Register Fonksiyonuna İlişkin Sorgu ve Cevap Mesaj Yapıları

MODBUS HABERLEŞME DURUMLARI

Yazılım içerisinde modbus haberleşme aşağıdaki durumlardan (state) birinde olabilir. Mevcut durum *GetModbusStatus()* fonksiyonu ile öğrenilebilir.

- RXTX_INIT
- RXTX_IDLE
- RXTX_START
- RXTX_DATABUF
- RXTX_RESPONSE

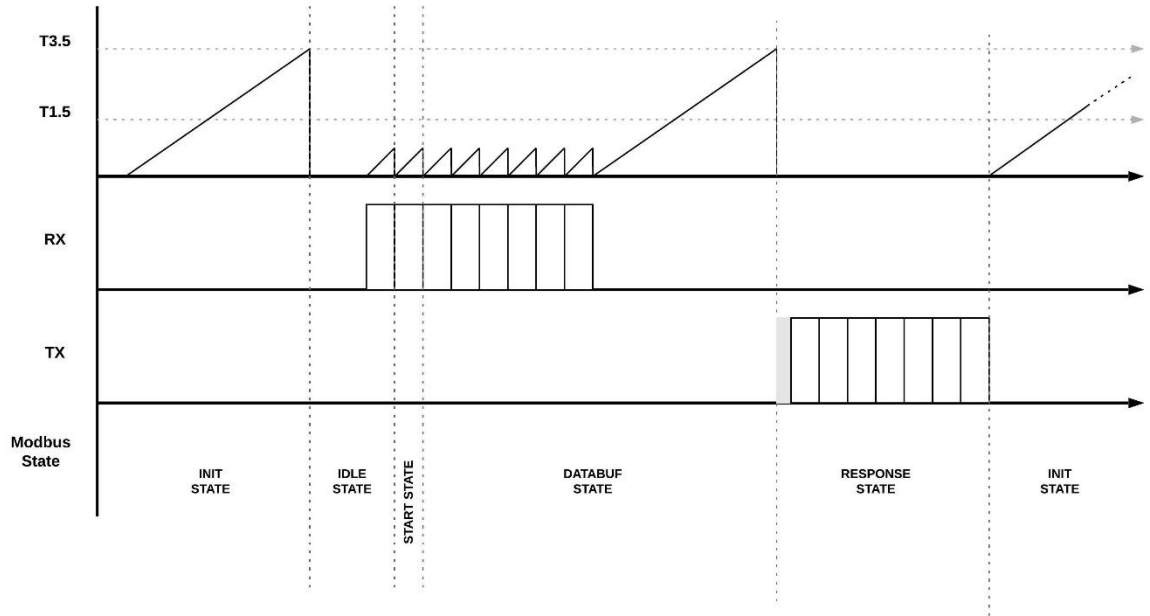
Modbus haberleşme ilk olarak *RXTX_INIT* durumunda başlar. Ve modbus için kullanılan donanımsal timer modülü çalışmaya başlayarak 3.5T ile belirlenen süre beklenmeye başlar. Süre dolduğunda alınan timer kesmesi ile durum değiştirilir ve *RXTX_IDLE* durumuna geçilir. Bu duruma geçilme ile birlikte usart kesmesi aktif hale getirilir.

RXTX_IDLE durumunda ise master cihazdan sorgu beklenir. Sorgu geldiğinde ise paketin ilk verisinin gelmesiyle alınan usart kesmesinde, *RXTX_IDLE* durumundan *RXTX_START* durumuna geçilir. Ve alınan ilk veri olan slave adres bilgisi ilgili hafıza alanına kaydedilir. Bu aşamadan sonra paketin byte ları arasında 1.5T süresinin kontrol edilmesi için timer resetlenip tekrardan çalışmaya başlatılır.

RXTX_START durumunda alınan yeni bir usart kesmesinde ise ilk olarak 1.5T süresi kontrol edilir. Eğer bu süre aşılmışsa modbus durum makinesi (state machine) *RXTX_INIT* durumuna geçirilerek yeniden 3.5T süresi yeniden yakalanmaya çalışılır. Eğer 1.5T süresi aşılmamışsa fonksiyon bilgisini içeren veri ilgili hafıza alanına kaydedilir ve timer resetlenerek *RXTX_DATABUF* durumuna geçilir.

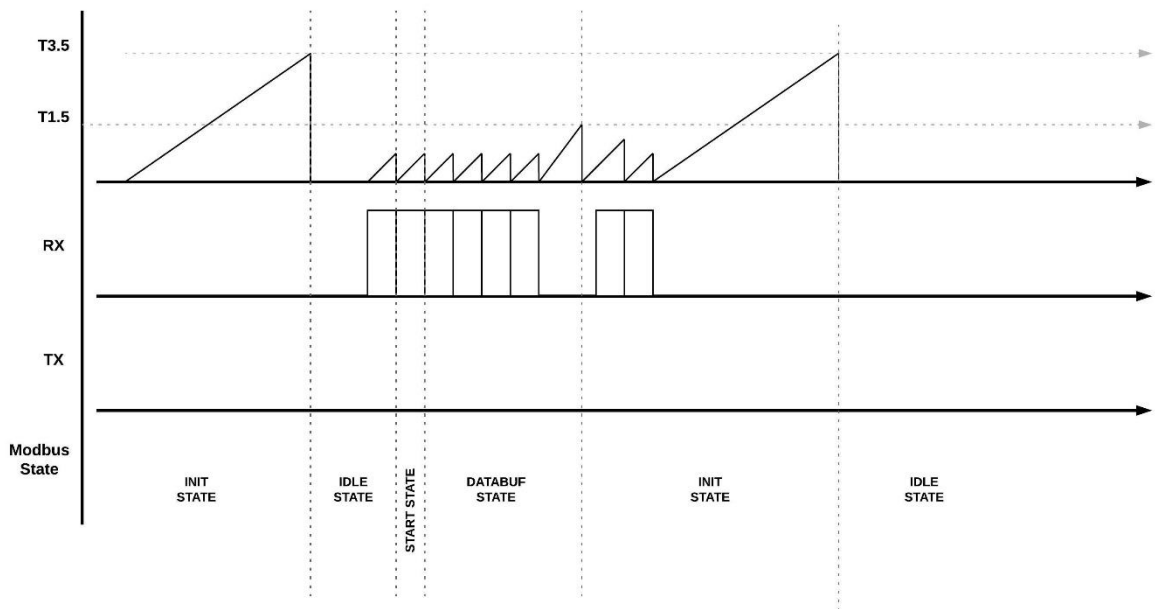
RXTX_DATABUF durumunda ise sıralı olarak usart kesmesi ile gelen paketin tüm verileri 1.5T süresi kontrol edilerek kaydedilir. Bu esnada timer sürekli çalışmaya devam ettiği için master tarafından gönderilen paket bittiğinde yeniden 3.5T süresi yakalanarak timer kesmesi içinde *RXTX_RESPONSE* durumuna geçilir.

RXTX_RESPONSE durumunda ise gelen paket incelemeye alınarak sırasıyla byte sayısı, slave adresi, fonksiyon kodu ve crc hata kontrolü yapılarak gelen paketin geçerliliği kontrol edilir. Gelen paket geçerli bir paket ise ilgili fonksiyon çağrılarak gönderilecek paket hazırlanıp, master cihaza gönderilir. Gönderim tamamlandıktan sonra ise tekrardan *RXTX_INIT* durumuna geçilerek yeni bir paket almaya hazırlanılır.



Haberleşme Esnasında Timer/Usart ve State Machine Durumları

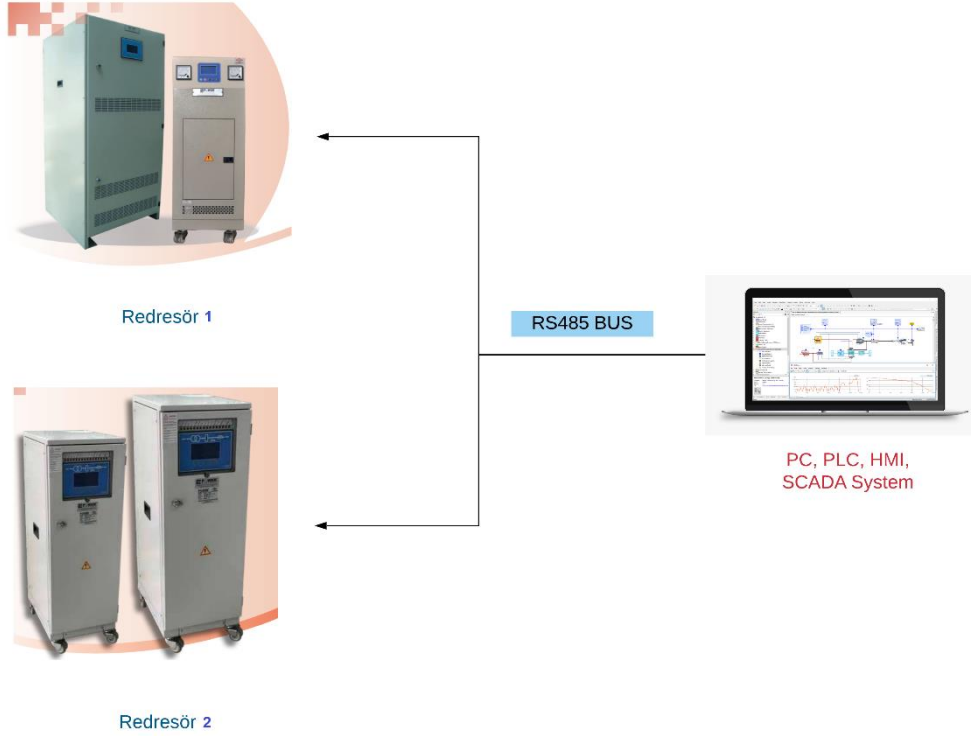
Aşağıdaki grafikte ise master cihazın gönderdiği paketin alımı esnasında byte lar arasında 1.5T süresinin aşılması durumu örnek olarak gösterilmiştir. Paket alımı başlamışken, ikinci byte dan itibaren her usart kesmesinde bu süre kontrol edilir. Eğer süre aşılmışsa *RXTX_INIT* durumuna geçilerek yeniden hatta 3.5T lik bir boşluk yakalanmaya çalışılır. Eğer bu aralıkta geç te olsa veriler gelmeye devam ediyorsa gelen veriler kaydedilmez ve sadece timer değeri resetlenir. Hatta 3.5T boşluğu yakalandığında ise *RXTX_IDLE* durumuna geçilerek master cihazdan gelecek olan paketleri dinleme modunda beklenir.



Haberleşme Esnasında 1.5T Süresinin Aşılması Durumu

ÖRNEK BİR HABERLEŞME BAĞLANTI ALTYAPISI

Örnek olarak Redresörlerin Modbus haberleşme altyapısı RS485 hattı üzerinden aşağıdaki şekilde kurulabilir. Master tarafta PC, PLC, HMI veya uygun bir scada altyapısı ile cihazın kullanıcı kitapçığında tanımlanmış tüm verilere, hata durumlarına ve durum bitlerine erişim mümkün olmaktadır.



MODBUS HATA MESAJLARI

- **ILLEGAL FUNCTION (Hata Kodu : 0x01)**
Cihazda tanımlanmamış bir fonksiyon sorgusu geldiğinde bu hata mesajı ile geri dönüş yapılır.
- **ILLEGAL ADRES (Hata Kodu : 0x02)**
Cihazda tanımlanmamış bir adres verisi sorgulandığında bu hata mesajı ile geri dönüş yapılır.
- **ILLEGAL VALUE (Hata Kodu : 0x03)**
Tanımlı bir adrese, sınırlar dahilinde bir veri yazılmadığında bu hata mesajı ile geri dönüş yapılır.



Ferudun GÖKCEGÖZ, 1987 İstanbul doğumludur. 2010 yılında Sakarya Üniversitesi, Elektrik Elektronik Mühendisliği bölümünden mezun olmuştur. Ardından Yıldız Teknik Üniversitesi, Elektrik Müh. A.B.D. Elektrik Mak. ve Güç Elektroniği programında yüksek lisans eğitimini tamamlamıştır. Şuan Yıldız Teknik Üniversitesi, Elektrik Müh. A.B.D. Elektrik Mak. ve Güç Elektroniği programında doktora eğitime devam etmektedir. 2010 Haziran – 2014 Kasım tarihleri arası Sisel Mühendislik, 2015 Mayıs – 2017 Mayıs tarihleri arası Grup Arge Enerji ve Kontrol Sistemleri, 2017 Mayıs – 2019 Ekim tarihleri arası Elartek Mühendislik firmasında arge departmanlarında görev almıştır. 2019 Ekim ayından itibaren de Power Elektronik firmasında arge mühendisi olarak çalışmaktadır. Gömülü Sistemler, Kontrol ve Güç Elektroniği alanında çalışmalarına devam etmektedir.